UNIVERSITY OF THE SACRED HEART

DEPARTMENT OF BUSINESS ADMINISTRATION
GRADUATE PROGRAM
MANAGEMENT INFORMATION SYSTEM
SANTURCE, PUERTO RICO

DIGITAL SIGNATURES: TENDENCY IN THE NEAR FUTURE IN THE

PHARMACEUTICAL INDUSTRY OF PUERTO RICO

JOSÉ MANUEL COPPLIND PALERMO

AUGUST, 2000

HOJA DE APROBACION DE TESIS

Certifico que he leído este estudio y que, en mi opinión, se ajusta a los cánones aceptables de disertación académica y es completamente adecuado en propósito y calidad, como Tesis/Proyecto para el grado de Maestría en Gerencia de Sistemas de Información.

Director

Asesor

Asesor

ACKNOWLEGMENTS

I'd like to dedicate this thesis to:

my mother Teresa,

my father José,

my sisters María and Anna,

my brother Carlos,

my grandmother Dora;

my aunt Anita,

my uncle José,

my cousin Giovanna,

To my teachers at the University of the Sacred Heart, specially to:

Lic. Carmen Cintrón,

Prof. Rafael Green, and

Prof. Ravelo;

To my friends at work and school, specially to:

Jaime Santana,

Ana and Tirso Bursian,

Sonia Sáez,

Javier Pérez,

Gisela Santiago,

Luis R. Rivera,

Sylvia Valentín,

César Calderón,

José Colón, and

Ana Gorbea.

SUMMARY

This thesis is related to the future tendencies of the Electronic / Digital Signatures.

Electronic / Digital signatures, as a solution for a paperless environment within a company, has it advantages and disadvantages. Within this research we analyze the existing alternatives available in the market to anticipate the future use of Electronic / Digital signatures in the work environment

Our objective is achieved through an evaluation of current technology and cost/benefits analysis of the implementation of these technologies, versus continuing in the paper-based environment.

The results obtained from this research anticipates that a very small -but incrementing- percent of companies will be using or will be evaluating alternatives in the use of Electronic / Digital signature technology for all their business activities.

TABLE OF CONTENTS

ACKNOWLEGMENTS SUMMARY LIST OF FIGURES LIST OF TABLES	. 3 . 6
CHAPTER I. INTRODUCTION	10 11
ELECTRONIC COMMERCE	16 27 34 35
Regulatory Acceptance:	36
Enforcement Integrity:	
Security:	37
Validation:	37
Standards:	38
Freedom of Information:	38
IMPACT OF THE FDA RULE (21 CFR PART 11)	40 43
SIGNATURES / ELECTRONIC RECORDS	47
ELECTRONIC RECORDS.)U
CHAPTER II METHODOLOGY. 5 PARTICIPANTS 5	
CHAPTER III ANALYSIS AND RESULTS	53

Approvelt software54	ŀ
TECHNOLOGY EVALUATION 58	}
CHAPTER IV CONCLUSION AND RECOMENDATIONS)
CHAPTER V FUTURE RESEARCH AND AREAS OF INTEREST 63	}
REFERENCES64	
APPENDIX A: Guideline Questions used in interview	5
APPENDIX B: Result Tabulation from Interviews	
APPENDIX C: List of Pharmaceuticals established in Puerto Rico	3
APPENDIX D: Federal register: 21 CFR Part 11)

LIST OF FIGURES

Figure	I.	Development Drug Life Cycle40.
Figure	II.	Typical process to obtain document signature approval44.

CHAPTER I. INTRODUCTION

Electronic storage of text, and the ability to edit and update it, and Federal Acts and Bills like the U.S. Government Paper Elimination Act (see Table 1) is reducing the need for paper in many businesses -and also the amount of trash produced-. It also reduces costs for the paper itself and its storage -including inventory, disposal and all associated handling costs-. Some observers (Baase, 1997) have pointed out that fax machines and laser printers make it so easy to print things on paper that we are in fact using more paper now than we did before.

More and more trees are being felled to satisfy our vast appetite for paper, in offices which were supposed by now to be all-electronic. In the US, paper consumption has rocketed 320 percent over the past 30 years (Erman et al., 1997). In absolute terms, this means that US consumers gobbled up 4 trillion pages of paper in 1996, compared with only 2.5 trillion in 1986 -about the time that word processors and personal computers were becoming really popular. The two most successful office products of recent times, the photocopier and the fax machine, are of course enormous users or generators of paper, while technologies which do not use paper, such as electronic mail and voice mail, have been slow to catch on. The overall market of office automation equipment is not as strong as it was in the 1980's, but sales of desktop laser printers are booming, and of course they also consume vast amounts of paper.

Electronic commerce is emerging as the future way of doing business. (Rasilainen, 2000) Trust is essential for the success and continued development of electronic commerce. Electronic signatures are an important and essential component to protect information and provide this trust in electronic commerce. This need for electronic signatures -and its associated technology- as a key issue for electronic commerce has been recognized in most countries.

This document analyses the need to implement electronic/digital signatures as a way to reduce costs within a company, especially the kind of company that are regulated by the Food and Drug Administration -FDA-: pharmaceuticals, food manufacturers, etc. Also to help the environment (through paperless environment), accelerate processing speed of transactions, etc., reflecting its gain in reduction costs for the company that wants to evaluate this technology and implement it.

JUSTIFICATION

Automated systems are being used more extensively in all industries. The use of such systems is also expanding into an emerging objective of the use of automation: implementation of paperless electronic records. Signatures are a key aspect of many records and the transition from paper records containing traditional handwritten signatures to paperless electronic records raises a set of issues relating to acceptance of alternatives for the government and any regulating agency (i.e. Food and Drug Administration -FDA-, etc.).

Signature alternatives for the classical "autographical ink signature" are being considered as appropriate equivalent to this autographical signature. Even though several concerns about the application of signature alternatives have arisen, some laws (see Table I) have been approved accepting the use of electronic signatures as an equivalent to the classical "autographical ink signature".

LITERATURE REVIEW

DEFINITION OF TERMS

- Algorithms: A set of ordered steps for solving a problem, such as mathematical formula or the instructions in a program (Tech Encyclopedia, www.techweb.com).
- Asymmetric System: A system in which major components or properties are different (Tech Encyclopedia, www.techweb.com).
- **Biometrics**: A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable (Glossary of PC and Internet Terminology).
- Cryptography: Conversion of data into a secret code for transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called ciphertext via an encryption algorithm. The ciphertext is decoded (decrypted) at the receiving end and turned back into plaintext (Tech Encyclopedia, www.techweb.com).
- **Data Encryption**: Process of converting data into "unreadable code" so that prying eyes cannot understand the content (Tech Encyclopedia, www.techweb.com).
- Electronic Commerce: Business which takes place between companies using services such as the Internet, Electronic Data Interchange or Electronic File Transfer, Two companies, one the supplier and the other the customer can transmit inquiries,

orders, invoices, payments, etc. Directly through their computer systems. (Tech Encyclopedia, www.techweb.com).

- Electronic Identification: Electronic identification is a means of identification which lacks an intrinsic biometric or behavioral link to the person being identified.

 Uniqueness of the identification is predicated upon a system of administrative controls. Examples of electronic identification include passwords/identification codes, bar codes, and personal identification codes (FDA Progress Report, 1992).
- Electronic Signature: An electronic signature is a non-handwritten unique means of identifying an individual, which has an intrinsic biometric or behavioral link to the individual which remains with the individual such that other persons cannot apply the electronic signature. Examples of electronic signatures include retinal scan systems, voice prints, and hand prints (FDA Progress Report, 1992).
- Signature: A signature is the name of an individual, handwritten in script by that individual. The act of signing with a writing or making instrument such as a pen, pencil, or stylus is preserved. However, the scripted name, while conventionally applied to paper, may also be applied to other devices which, like paper, capture the written name (signatures recorded electronically). The act of signing serves as an intrinsic behavioral link to the signer (FDA Progress Report, 1992).
- Digital Signature: Refer to Electronic Signature or to Table I.

ELECTRONIC COMMERCE

People are "surfing" the Internet for knowledge, amusement, and to make small purchases using secure browsers such as Netscape and Microsoft's Internet Explorer, which can encrypt credit card numbers (Tozer, 1999). Very soon, however, the Internet will be used to conduct serious commercial transactions where it is not enough to merely encrypt the message but to make sure that the message originates from an entity allegedly sending it and has not been altered or garbled in transit (Tozer, 1999). Baase, (1997) noted that the data transmitted by satellite can be "seen" by anyone with a satellite dish. E-mail that goes through several computers on its way to its destination may be read on any of those intermediary systems.

People engaging in Internet commerce will want to know that the message and the electronic "signature" attached to the message can both be verified and can be used in court to bind the "signer" to the deal (Tozer, 1999).

Business transactions, such as online bank-account transfers, are now secured from prying eyes through data encryption. However, without signatures, there is no guarantee that a person or organization on one end of a Web or E-mail transaction is who they say they are (Hancocks, 1999). That is why most banks have "non responsibility" agreements per electronic transactions.

Business owners with an interest in using the Internet for commercial transactions -which should include virtually every business- need a basic understanding of the process and the legal principles underlying such commerce (Tozer, 1999).

The need to maintain the security and secrecy of communications is increasing, and encryption is one of the tools for doing so (Baase, 1997).

Electronic signatures provide evidence in digital form that some commitment has been explicitly endorsed. The most common form of electronic signature today is the digital signature. Digital signatures are created and verified by means of cryptography mathematics (refer to section "How Digital Signature Technology Works"). They use a public key cryptography, which employs mathematical algorithms using two different but mathematically related keys: a private key for creating a digital signature and a public key for verifying it. It is computationally not feasible to derive the private key from the knowledge of the public key and thus to forge the digital signature. (Rasilainen, 2000).

Public key cryptosystems -as in the Secure Socket Layer (SSL) protocols- are based on the use of an associated key pair: a private key that is kept private, and a public key that can be published. The system allows secret messages to be sent over insecure channels like the Internet. By encrypting the messages using the intended recipient's openly available public key, the sender can be certain that only the intended recipient -the holder of the associated private key- will be able to decrypt the message (Tozer, 1999).

Today, many countries around the world, many states in the United States of America, and other jurisdictions are contemplating technology neutral, broad enabling legislation -generally known as "electronic signature" laws. Some jurisdictions are also enacting more specific legislation, such as digital signature laws, to deal with specific market activities, such as EDI -Electronic Data Interchange, an Internet commerce application- (www.silanis.com).

The explosive growth of electronic commerce and on-line business-to-business transactions has fueled the demand for a secure and legally binding electronic method for signing on-line documents. Networks have become so ubiquitous that organizations naturally want to use them to achieve the efficiencies of an entirely electronic process. However, businesses and governments require signatures to procure supplies, originate applications, service loans, negotiate contracts, submit government forms and handle most business-to-business transactions (www.PenOp.com).

Page 16

WHAT IS DIGITAL SIGNATURE?

If we take most of the enacted statutes that are currently being developed in the United States, we could find the following definitions for a digital signature (Zanger, 2000):

Table I. Definitions for Digital Signature.

Table I. Definitions for Digital Signature		
STATE	BILL / STATUTE	<u>DEFINITION OF</u> <u>DIGITAL SIGNATURE</u>
Arizona	1998 AZ HB 2518	A type of electronic signature that transforms a message through the use of an asymmetric cryptosystem.
Arkansas	The Information Network of Arkansas (1999 AR SB 378)	Term used but not defined.
California	California Civil Code (adding s. 1633)(1999 CA SB 1124).	"Digital Signature", for the purposes of this section, means an electronic identifier, created by a computer, that is intended by the party using it to have the same force and effect as a manual signature. The use of a digital signature shall have the same force or effects as a manual signature if it embodies all of the following attributes: 1. It is unique to the person using it. 2. It is capable of verification. 3. It is under the sole control of the person using it. 4. It is linked to data in a manner that if the data is changed the digital signature is invalidated.

Table I. Definitions for Digital Signature		
STATE	BILL / STATUTE	DEFINITION OF
	CA Government Code § 16.5	Uses the term "digital signatures" to refer to electronic signatures. "'Digital signature' means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature."
Colorado	Colorado revised statutes, adding 24-71-101, amending 24-30-1603, 24-30-1604(1) & (1)(b), 4-9-413, 4-9-401(1), 4-9-405(2), and 4-9-406 (1999) CO HB 1079).	As used in this article, 'Digital Signature' or 'Electronic Signature' means an electronic identifier, created by computer, intended by the party using it to have the same force as the use of a manual signature. In any written communication in which a signature is required or used, any party to the communication may affix a signature by use of an electronic or digital signature that complies with the requirements of this section. The use of an electronic or digital signature shall have the same force and effect as the use of a manual signature if: 1. It is unique to the person using it; 2. It is capable of verification; 3. It is under the sole control of the person using it; 4. It is linked to data in such manner that the electronic or digital signature is invalidated if any data is changed; 5. It conforms to rules promulgated by the Executive Director of the Department of Personnel

<u>Table I.</u> Definitions for Digital Signature		
STATE	BILL / STATUTE	<u>DEFINITION OF</u> <u>DIGITAL SIGNATURE</u>
		pursuant to Section 24-30-1604(1).
Florida	Electronic Signature Act of 1996 - Fla Stat. § 282.70 et. Seq. (1997), (1996 FL SB 942).	"'Digital signature' means a type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: 1. Whether the transformation was created using the private key that corresponds to the signer's public key; 2. Whether the initial message has been altered since the transformation was made."
Georgia	Amends Title 40. Motor Vehicle and Traffic of the Georgia Code (1997 GA HB 487).	Uses the term "digital signatures" to refer to electronic signatures. The term "Digital Signature" is defined as "a digital or electronic method executed or adopted by a party with the intent to be bound by or to authenticate a record, which is unique to the person using it, is capable of verification, is under the sole control of the person using it, and is linked to data in such a manner that if the data are changed the digital or electronic signature is invalidated."
Hawaii	Hawaii revised statutes annotated title 14 § 231-8.5 (1995 HI SB 2401).	Term not used.

<u>Table I.</u> Definitions for Digital Signature		
STATE	BILL / STATUTE	<u>DEFINITION OF</u> <u>DIGITAL SIGNATURE</u>
Illinois	Illinois Electronic Commerce Security Act - Public Act 90-759 (1997 IL HB 3180)	"Digital signature" means a type of an electronic signature created by transforming an electronic record using a message digest function, and encrypting the resulting transformation with an symmetric cryptosystem using the signer's private key such that any person having the initial untransformed electronic record, the encrypted transformation, and the signer's corresponding public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key; and whether the initial electronic record has been altered since the transformation was made. A digital signature is a security procedure.
	Financial Institutions Digital Sigantures Act - 205 ILCS 705/5 (1997 IL HB 597)	Uses the term "digital signatures" to refer to encrypted electronic signatures. The term "digital signature" is defines as "an encrypted electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature.
	State Comptroller Act - 15 ILCS 405/14.01 (1997 IL SB 516 and 1997 IL HB 276)	Uses the term "digital signatures" to refer to electronic signatures. "'Digital Signature' means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature".
Indiana	Electronic Digital Signature Act - West's Ann. Indiana Code Title 5,	"Digital Signature" means an electronic signature that transforms a message using an asymmetric

	Table I. Definitions for	Digital Signature
STATE	BILL / STATUTE	<u>DEFINITION OF</u> <u>DIGITAL SIGNATURE</u>
	Art. 24 (1997 IN SB 5a, 1997 IN HB 1945).	cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (1) the transformation was created using the signer's public key; and (2) the initial message has been altered since the transformation was made.
Iowa	Iowa Electronic Commerce Security Act (1999 Iowa HF 624).	"'Digital signature' means a type of an electronic consisting of a transformation of an electronic record using a message digest function that is encrypted with an asymmetric cryptosystem using the signer's private key in a manner providing that any person having the initial untransformed electronic record, the encrypted transformation, and the signer's public key may accurately determine all of the following: a. Whether the transformation was created using a private key that corresponds to the signer's public key. Whether the initial electronic record has been altered since the transformation was made. A digital signature is a security procedure."
Maryland	Maryland Digital Signature Pilot Program, 1998 Md. Laws 482; (1998 MD HB 523).	Uses the term "digital signatures" to refer to electronic signatures. "'Digital Signature' means an electronic identifier, created by a computer, that: (i) Is intended by the authorized signer to have the same force and effect as the use of a manual signature;

	Table I. Definitions for	Digital Signature
<u>STATE</u>	BILL / STATUTE	<u>DEFINITION OF</u> <u>DIGITAL SIGNATURE</u>
		 (ii) Is unique to the authorized signer; (iii) Is capable of verification; (iv) Is under the sole control of the authorized signer; (v) Is linked to data in such a manner that if the data are changed, the signature is invalidated; and (vi) Conforms to regulations adopted by the Secretary of State."
Minnesota	1997 MN SB 2068 (Amends Minnesota Electronic Authentication Act (Minn. Stat. Ann. § 325K)).	"'Digital Signature' or "digitally signed" means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made."
	Minnesota Electronic Authentication Act (Minn. Stat. Ann. § 325K).	"'Digital Signature' means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (1) whether the transformation was created using the private key that corresponds to the signer's public key; and (2) whether the initial message has been altered since the transformation was made.
Mississippi	Digital Signature Act of 1997, Miss. Code 1972 Ann. § 25-63-let. Seq.	"'Digital Signature' means a message or part of a message which has been transformed using a computer

Table I. Definitions for Digital Signature		
<u>STATE</u>	BILL / STATUTE	<u>DEFINITION OF</u> DIGITAL SIGNATURE
	(1997) (1997 MS HB 752).	program called a "private key" such that a person receiving the message can use a related computer program referred to as the signer's "public key" to determine whether the transformation was created using the private key that corresponds to the public key and whether the original message has been altered since the transformation was made."
Missouri	Missouri Digital Signature Act (1998 MO SB 680).	Digital Signature means "a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (a) The transformation was created using the private key that corresponds to the signer's public key; and (b) The message has been altered since the transformation was made."
	1998 MO SB 844	The term "digital signature" isused but not defined.
New Hampshire	1998 NH LAWS 22; (1997 NH HB 290).	"'Digital Signature' means a type of electronic manipulation that transforms a message using an asymmetric cryptosystem such that a person having the transformed message and the signer's public key can accurately determine: (a) Whether the transformation was created using the private key that corresponds to the signer's public key; and (b) Whether the initial message has been altered since the transformation was made."

Table I. Definitions for Digital Signature		
<u>STATE</u>	BILL / STATUTE	<u>DEFINITION OF</u> DIGITAL SIGNATURE
	New Hampshire Digital Signature Act - RSA 294- D:1 et. Seq.; (1997 NH SB 207).	"'Digital Signature' means an electronic identifier, created by computer, intended by the party using it to have the same force and effect as the use of a manual signature."
New Mexico	Electronic Authentication of Documents Act New Mexico Statutes Annotated §14-15-1 et. Seq. (1996 NM HB 516).	"'Electronic authentication' means the electronic signing of a document that establishes a verifiable link between the originator of a document and the document by means of a public key or private key system."
	1999 NM SB 146.	Term used but not defined.
New York	Chapter 57A of the Consolidated Laws: The State Technology Law (includes Article I: The Electronic Signatures and Records Act) (1999 NY SB 6113).	Included in definition of Electronic Signature.
North Carolina	1997 NC HB 1356	Term not used.
Oklahoma	1997 OK HB 3287	Term used but not defined.
Oregon	Electronic Signature Act, Oregon Revised Statutes §192.825 et. Seq. (1997 OR HB 3046).	"'Digital Signature' means a type of electronic signature that transforms a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (a) Whether the transformation was created using the private key that corresponds to the signer's public key; (b) Whether the initial message has

Table I. Definitions for Digital Signature		
STATE	BILL / STATUTE	<u>DEFINITION OF</u> DIGITAL SIGNATURE
		been altered since the transformation was made. A 'key pair' is a private key and its corresponding public key in an asymmetric cryptosystem, under which the public key verifies a digital signature the private key creates. An 'asymmetric cryptosystem' is an algorithn or series of algorithms which provide a secure key pair."
	Oregon Revised Statutes §709.335 (1997 OR SB 125).	As defined in Oregon's Electronic Signature Act (see above).
Pennsylvania	The Electronic Transactions Act (Pennsylvania Consolidated Statutes, Titles 12 & 18) (1999 PA SB 555).	Term not used or defined, however, Statute refers to :Security Procedures," defined as procedures employed for the purpose of verifying that an electronic signature, record or performance is that of a specific person or for detecting changes or errors in the information record. The term includes a procedure which requires the use of algorithms or other codes, identifying words or numbers, encryption or callback or other acknowledgment procedures.
T	1997 PA SB 1385	Term not used or defined.
Texas	Tex. Bus. & Com. Code §2.108 (1998 TX HB 984).	Uses the term "digital signature" to refer to electronic signatures. "'Digital Signature' means an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature."

<u>Table I.</u> Definitions for Digital Signature		
<u>STATE</u>	BILL / STATUTE	<u>DEFINITION OF</u> <u>DIGITAL SIGNATURE</u>
	Tex. Gov't Code §403.027 (1997 TX SB 645).	Uses the term "digital signature" to refer to electronic signatures. The term "Digital Signature" is not defined, but the Act presumable uses the term in same manner as 1998 TX HB 984 (which uses the term "digital signature" to mean electronic signature).
	Tex. Transp. Code §201.931 (1997 TX SB 370).	Uses the term "digital signature" to refer to electronic signatures. "'Digital Signature' means an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature."
Utah	Utah Digital Signature Act (Utah Code Ann. §46-3-101 et seq.).	"'Digital Signature' means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (a) the transformation was created using the private key that corresponds to the signer's public key; and (b) the message has been altered since the transformation was made.
	Utah Stat. Ann §46-1-16 (1998 UT SB 107).	As defined in the Utah Digital Signature Act.
	1996 Utah Senate Bill 73.	As defined in the Utah Digital Signature Act.
	1996 Utah Senate Bill 188.	As defined in the Utah Digital Signature Act.
	1998 Utah Senate Bill 1.	Term used but not defined.
Virginia	Va. Code Ann. §59.1-467	Uses the term "digital signatures" to

Table I. Definitions for Digital Signature			
STATE	BILL / STATUTE	<u>DEFINITION OF</u> <u>DIGITAL SIGNATURE</u>	
	to 469 (1997 VA SB 923).	refer to electronic signatures. "'Digital Signature' means an electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature."	
Washington	Washington Electronic Authentication Act (Chapter 19.34 RCW).	"'Digital Signature' means a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine: (a) Whether the transformation was created using the private key that corresponds to the signer's public key; and (b) Whether the initial message has been altered since the transformation was made."	

These acts/statutes/bills are a critical next step in establishing trust in electronic commerce. In a way or another, these acts specifically requires government agencies - and encourages private business- to adopt digital signature technology (Hancocks, 1999).

The combined effect of the pending federal legislation will be similar to the setting of national standards for road signs on interstate highways: it will promote consistency over local idiosyncracies (Wright, 1999).

HOW DIGITAL SIGNATURE TECHNOLOGY WORKS

As stated by the American Bar Association (ABA, 1999), Section of Science and Technology, Information Security Committee, digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as "public key cryptography," which employs an algorithm using two different but mathematically related "keys": one for creating a digital signature or transforming data into seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. Computer equipment and software utilizing two such keys are often collectively termed an "asymmetric cryptosystem".

The complementary key of an asymmetric cryptosystem for digital signatures are arbitrarily termed the private key, which is known only to the signer and used to create the digital signature, and the public key, which is ordinarily more widely known and is used by a relying party to verify the digital signature. If many people need to verify the signer's digital signature, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible (the question of data ownership arises: Rights and Privileges). Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely it is "computationally not feasible to derive the private key from

knowledge of the public key". Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge digital signatures. This is sometimes referred to as the principle of "irreversibility" (ABA, 1999).

Another fundamental process, termed a "hash function," is used in both creating and verifying a digital signature. A hash function is an algorithm which creates a digital representation or "fingerprint" in the form of a "hash value" or "hash result" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it. Any change to the message invariably produced a different hash result when the same hash function is used. In the case of a secure hash function, sometimes termed a "one-way hash function," it is computationally not feasible to derive the original message from knowledge of its hash value. Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed. The greatness of the hash function is that different keys can reference the same address, which means that different people can share access levels and privileges without sharing a key (ABA, 1999).

Thus, use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature (ABA, 1999):

- **Digital signature creation** uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

To sign a document or any other item of information, the signer first determines precisely the borders of what is to be signed. The delimited information to be signed is termed the "message", then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the message. The signer's software then transforms the hash result into a digital signature using the signer's private key. The resulting digital signature is thus unique to both the message and the private key used to create it (ABA, 1999).

Typically, a digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. However, it may also

be sent or stored as a separate data element, so as long as it maintains a reliable association with its message (ABA, 1999).

Verification of a digital signature (ABA, 1999) is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks:

- (1) whether the digital signature was created using the corresponding private key; and
- (2) whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process.

The verification software will confirm the digital signature as "verified" if:

- (1) the signer's private key was used to digitally sign the message, which is known to be the case if the signer's public key was used to verify the signature because the signer's public key will be verify only a digital signature created with the signer's private key; and
- (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital signature during the verification process.

Various asymmetric cryptosystems create and verify digital signatures using different algorithms and procedures, but share this overall operational pattern (ABA, 1999). The following example -writing and sending a check, steps 1.0 and 2.0- illustrates how digital signature technology works (ABA, 1999).

1.0 Digital Signature Creation.

- 1.1 Sign.
 - 1.1.1 To begin the process, a check must be created. In order to create a digital signature with the check, a process known as "hash function" must occur.
 - 1.1.2 The next step is to encrypt the check and signature.

 The sender's digital signature software transforms the hash result into a digital signature using the sender's private key. The resulting digital signature is thus unique to both the message and the private key used to create it.
 - 1.1.3 Typically, a digital signature is appended to its message and stored or transmitted with its message.However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital

signature is unique to its message, it is useless if wholly disassociated from its message.

1.2 Seal.

1.2.1 Since public key algorithms can be slow to transmit, the next step is to encrypt the information. The check is encrypted with a fast symmetric key (uniquely generated for this occasion) and then, the symmetric key is encrypted with the receiver's public key. Now only the private key of the receiver can recover the symmetric key, and thus decrypt the check. A digital version of the envelope has been created.

1.3 Deliver.

1.3.1 At this point, the digital envelope is electronically sent to the receiver and the verification process begins.

2.0 Digital Signature Verification.

2.1 Accept.

2.1.1 The encrypted digital envelope arrives at the destination.

2.2 Open.

2.2.1 The receiver of the check decrypts the one-time symmetric key by using the receiver's private key.Then the check is decrypted using the one-time symmetric key. Once this has been completed, the verification process begins.

2.3 Verify.

2.3.1 Verification of a digital signature is accomplished by computing a new hash result of the original message. Then, using the sender's public key and the new hash result, the verifier checks: 1) whether the digital signature was created using the corresponding private key; and 2) whether the newly computed hash result matches the original hash result. The software will confirm the digital signature as "verified" 1) the sender's private key was used to digitally sign the message and 2) the message was unaltered. If the verification cannot be made, the software will identify that verification has failed.

PRIMARY AREAS OF CONCERN:

Concerns about application of signature alternatives in documents that the regulated industry must maintain as part of day to day operations, documents that, for example, are subject to Food and Drug Administration -FDA- inspection.

There is the area of official records submitted by the regulated industry (e.g. pharmaceuticals, etc.) to FDA for review and approval, usually as part of research or marketing applications. Generally, signatures on this kind of documents provide certification of data or authentication of submitted records.

Any company/agency own internal documents, some administrative, some regulatory, which are increasingly being subject of automation. For example, sample collection reports and analytical work sheets represent regulatory documents that might contain signature alternatives instead of conventional signatures.

WHAT ARE THE ISSUES RELATED TO ELECTRONIC SIGNATURES?

The following are the key issues regarding the acceptance of signature alternatives (as expressed by the FDA progress report presented by the Electronic Identification/Signature Working Group, 1996):

Legal Acceptance

It is vital to conform to judicial acceptance and qualifications regarding signature alternatives. Any accepted alternative should be viewed by the courts as equivalent to conventional signatures. The alternatives should carry the same commitment, legal weight, and significance as conventional signatures. Furthermore, falsification of signature alternatives should be considered to be fraudulent to the same extent as is falsification of conventional signatures.

In reviewing these issues, it may be useful to consider how signature alternatives may conform to three primary functions of the conventional "autographical" signature:

• First, the signature identifies the signer and shows the authority of act. The signature alternatives defined above (electronic signatures and electronic identification) may meet this function where administrative controls link the signature alternative to an individual by (for example) cross-references.

- Second, the signature documents the terms of the action in a manner that is legally binding and cannot be repudiated. Author repudiation would be much more difficult for electronic signatures, than for electronic identification, as defined above. Although legal precedence has yet to be encountered, electronic signatures would likely be more legally binding, by virtue of their security and non-transferability, than electronic identification.
- Third, the signature created a record traceable during investigations and admissible in court. By administrative controls and cross-references, it is possible that signature alternatives would provide record traceability, although some complexity may hamper that effort.

Regulatory Acceptance:

Acceptance of signature alternatives, at least as a means of identifying individuals in records produced by the regulated industry, is not uniform in the various regulations managed by the different centers. For example, the Current Good Manufacturing Practices (cGMP) regulations for human and veterinary drugs contain some sections that explicitly require signatures or initials without actually using the words signature or initials. Likewise, various records submitted to agencies like the FDA are explicitly required to be signed; interestingly, 21 CFR 1005.25, regarding designation of a foreign manufacturer's U.S. agent, requires all signatures to "be in ink".

Enforcement Integrity:

The ability to obtain copies of electronic records. The importance and legal acceptance of any signature alternatives in those records must not dilute any agency's ability to document individual responsibility and affix that responsibility in court, as we have done historically with paper records and conventional signatures.

Security:

It is vital that signature alternatives be secure. Whereas the recognition that any system can be corrupted and defeated by those intent of falsification, substitutes for conventional signatures should nonetheless be at least as secure as conventional signatures. Considering the easy with which some electronic identification methods can be falsified without leaving an audit trail, some signature alternatives may be inherently less secure and therefore should not be accepted by any regulating agency.

Validation:

The reliability of signature alternatives must be validated. Inadequate or entirely lacking computer system validation could be detected. Thus, validation would have to be a significant factor in acceptance of any signature alternatives.

Standards:

The acceptance of signature alternatives would be facilitated if appropriate signature standards could be developed. The adoption and recognition of public standards should be consistent with the regulatory agency's approach, in order for the agency to endorse a specific product or set of products as approved products to apply electronic signatures to electronic records.

Freedom of Information:

Some agencies receive the vast majority of freedom of information (FOI) request in paper form, where paper documents in possession of the agency are furnished to requesters consistent with legal requirements. Agencies has very limited experience with requests that are submitted electronically, where documents at issue are in electronic form, or where documents in electronic form are requested to be furnished in electronic form.

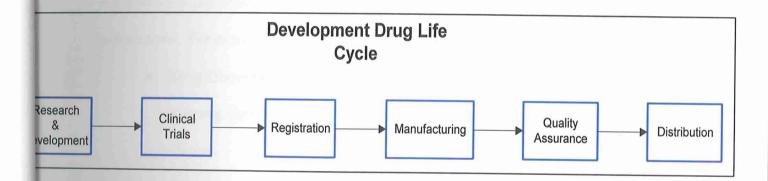
Several matters need to be addressed in this area. For example, administrative fees for researching, purging (as needed), and copying electronic records may need to be established, fees which reflect costs that differ from those involved in handling conventional paper forms (e.g. will requesters provide computer disks to capture the electronic documents, or the agency have to furnish the disks?).

The electronic form of documents may also permit some efficiencies. For instance, administrative overhead involved in processing individual FOI request for previously released electronic documents may be reduced if such documents are placed into an electronic database accessible by the general public; automation could, in theory, manage access fees and tracking.

IMPACT OF THE FDA RULE (21 CFR PART 11)

The significance of the FDA rule can not be over stressed. It is truly a Green Light to the industry, affecting business functions irrespective of where the Development Drug Life Cycle (DDLC) they reside (Barker, 1998). See appendix D for the Final FDA Rule.

Figure I. Development Drug Life Cycle



For many years Pharmaceutical companies have been investing in IT technology to support the DDLC -presented in figure I-, but with one significant limitation, the lack of acceptance for the electronic signature. The acceptance of electronic signature will have a significant impact on the pharmaceutical companies by allowing them to move to a single media stream and to avoid the unnecessary and costly use of paper. The removal of paper in processes such as New Drug Application (NDA) will benefit both the

Page 41

regulator and the regulated but only if the rule is understood and applied correctly (Barker, 1998).

By giving pharmaceutical companies the "green light" to use electronic records and electronic signatures (Barker, 1998), the rule represents a watershed by allowing major efficiency improvements in their business operations. This is intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. It is important to realize that the use of electronic signatures can dramatically drive down costs for all business processes, not just for FDA submissions. For example:

- Drug Discovery applications (e.g. MDL's Electronic Lab Notebook) rely upon
 a strong signature audit trail being in place to support a patent application or
 dispute.
- Signature heavy processes such as manufacturing are obvious beneficiaries.

Agencies such as the FDA are aware of the potential impact of the rule, especially regarding the need to accommodate and encourage new technologies while maintaining the agency's ability to carry out its mandate to protect public health (FDA, 1997). The agency is also aware that other Federal agencies share the same concerns and are addressing the same issues as FDA; the agency has held informal discussions with other Federal agencies and participated in several interagency groups on electronic records/electronic signatures and information technology issues.

Even though the present rules on electronic records/electronic signatures does not establish numerical standards for levels of security or validation -thus offering firms flexibility in determining what levels are appropriate for their situation-, when automated data processing is used for manufacturing or quality assurance purposes, adequate checks shall be designed and implemented to prevent inaccurate data output, input, and programming errors. Furthermore, while requiring operational checks, authority checks, and periodic testing of identifying devices, persons have the flexibility of conducting those controls by any suitable method, and also have the option of determining the frequency (FDA, 1997).

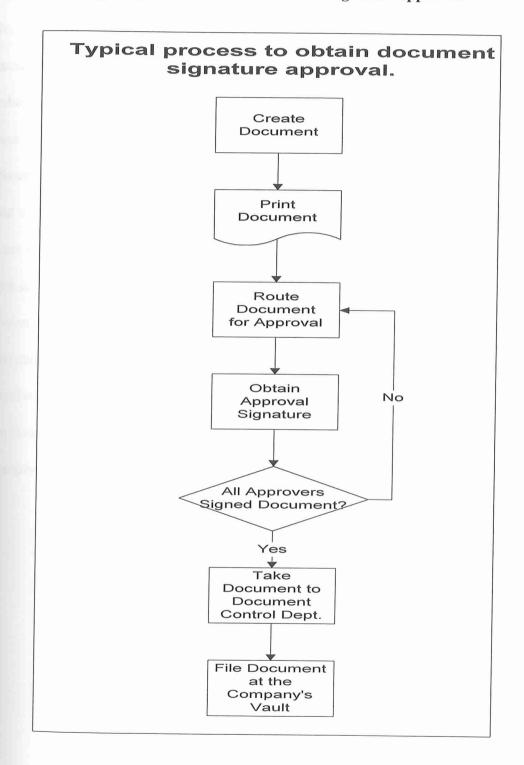
THE NEED FOR ELECTRONIC SIGNATURES/ELECTRONIC RECORDS.

In traditional paper-based processes, documents are created electronically, printed and physically routed from person to person to be signed. The greater the number of people to approve a document, the greater the physical distance between them, and the greater the revisions needed, the longer it takes to complete the approval process. Paper-based approval process is cumbersome, time-consuming and costly. These issues introduced the concept of electronic approval (FDA, 1996).

Electronic approval eliminates the need for pen and paper by allowing you to securely sign documents electronically. Electronic approval provides capabilities for the automatic management, and security of the entire business approval process. It drastically reduces the time and costs associated with traditional approval processes and allows for end to end electronic processes (FDA, 1996). A typical process for signature approval is presented in Figure II.

In August 1997, the FDA became the first federal agency to institute guidelines in their code of federal regulations regarding the use of electronic signatures. It introduced its 21 CFR Part 11 rule to allow the use of electronic documents and signatures in regulated processes. In compliance with the rule, FDA-regulated companies can now use electronic signatures to approve documents and subsequently submit these documents to them (the FDA).

Figure II. Typical process to obtain document signature approval.



Among documents submissions such as New Drug Applications (NDAs), Standard Operating Procedures (SOPs), manufacturing process controls, quality assurance and research and development, among others, pharmaceutical companies often submit as many as 500,000 pages of information to the FDA for their review. By law, in case of NDA applications, the FDA only has 180 days to review these submissions. However, the process is known to take an average of 1.5 to 3 years to complete! Time and costs associated with pushing large volumes of paper through the approval process were enormous. The FDA realized how inefficient these manual paper procedures were and acknowledged the potential benefits that could be gained by adopting an automated system. The FDA wanted to accommodate and encourage new technologies while maintaining its ability to quickly review documentation. It is therefore critical for FDA regulated businesses, wishing to utilize technology to increase efficiency, to find an application that will allow them to electronically approve and submit documents, while complying with FDA's rule on electronic signatures and records (FDA, 1997).

EXISTING REGULATIONS FOR ELECTRONIC SIGNATURES / ELECTRONIC RECORDS.

Table II.

Existing Regulations for Electronic Signatures / Electronic Records

21 CFR Part 11 for FDA-regulated industries.

U.S. Government Paper Elimination Act, which states that government agencies reduce paper and make electronic forms and documents available.

Specifications on digital signature use stipulated by General Accounting Office.

Secure Hash Algorithm standards set out by the National Institute of Standards and Technology (NIST).

Federal Information Processing Standards (FIPS) approved by US Department of Commerce

OTHER GUIDELINES

Table III.

Other Related Guidelines.

International Standards (ISO) families:

ISO 9000: good quality management practices, and

ISO 14000: environmental management systems.

The ISO 14000 family, of which the first standards were published in September and October 1996, addresses various aspects of environmental management. The very first two standards, ISO 14004 and ISO 14001, deal with environmental management systems. These are management tools to enable an organization of any size or type to control the impact of its activities, products or services on the environment. An environmental management system represents a structured approach to setting environmental objectives and targets, to achieving these and demonstrating that they have been achieved (ISO, 1997).

The standards do not specify levels of environmental performance - a fact which allows them to be implemented by a wide variety of organizations, whatever their current level of environmental maturity. However, a commitment to compliance with applicable

environmental legislation and regulations is required, along with commitment to continual improvements - for which the environmental management system provides the framework (ISO, 1997).

ISO 14004 provides guidelines on the elements of an environmental management system and its implementation, and discusses principal issues involved (ISO, 1997).

ISO 14001 specifies the requirements for such an environmental management system. Fulfilling these requirements demands objective evidence which can be audited to demonstrate that the environmental management system is operating effectively in conformance with the standard. ISO 14001 can thus be used for internal purposes (to provide assurance to the organization's management), and for external purposes (to provide assurance to interested parties). In the external context, conformance to ISO 14001 can be used to support what an organization claims about its own environmental policies and actions. It is suitable for both supplier's declarations of conformity by an independent certification body (ISO, 1997).

It is good to point out that all the ISO standards are voluntary, and many companies comply with it, even if they don't seek certification. ISO has no power to enforce their implementation. However, a certain percentage of its standards - mainly those concerned with health, safety or the environment - has been adopted in some

countries as part of their regulatory framework, or is referred to in legislation for which it serves as the technical basis (ISO, 1997).

ADVANTAGES OF ELECTRONIC SIGNATURES/ELECTRONIC RECORDS.

The industry and the Federal agencies can realize significant benefits by using electronic records and electronic signatures, such as (silanis, 2000):

- increasing the speed of information exchange,
- cost savings from the reduced need for storage space,
- reduced errors,
- data integration/trending,
- product improvement,
- manufacturing process streamlining,
- improved process control,
- reduced vulnerability of electronic signatures to fraud and abuse, and
- job creation in industries involved in electronic record and electronic signatures technologies.

Electronic signatures and electronic records have advantages over paper systems, advantages that include (silanis, 2000):

- 1. Having automated databases that enable more advanced searches of information, thus obviating the need for manual searches of paper records;
- 2. Permitting information to be viewed from multiple perspectives, as a date warehouse, etc.;

- 3. Permitting determination of trends, patterns, and behaviors, as in the Total Quality Management -TQM- approach, etc.;
- 4. Avoiding initial and subsequent document misfiling that may result from human error.

CHAPTER II METHODOLOGY

To identify the future of Electronic / Digital Signatures involves finding out if companies are using this technology. Also all decision factors associated with the implementation of this kind of system have to be considered.

The results obtained from this research are empirical, since no written information was found on the use of Electronic / Digital Signature technology in Puerto Rico. Only few companies from the regulated industry (pharmaceuticals) are evaluating the possibility to become 21 CFR Part 11 compliant. A total of 20 companies were interviewed out of a total population of 80 companies (refer to appendix C for a list of all companies in the Pharmaceutical Industry), and the results from their answers were averaged to evaluate the implementation of this type of technology.

PARTICIPANTS

System analysts from the different pharmaceuticals established in Puerto Rico, employing from 100 to 500 employees, were interviewed and asked general questions related to this topic (See appendix A, for a general guideline of the questions asked in the interviews).

CHAPTER III ANALYSIS AND RESULTS

The answers collected from the interviews performed, led us to evaluate the technology available in the market and perform a cost/benefit analysis for the use of the current technology available regarding electronic signatures.

TECHNOLOGY AVAILABLE IN THE MARKET.

PenOp ® Signature Series ™ software

PenOp ® Signature Series ™ software links people to documents by capturing all the details of a signing event and binding it to the electronic document. Verifiable electronic signature technology that works across the Internet, intranets, and extranets, lets you pick up a pen, sign and authenticate documents in the normal course of business without paper. PenOp software creates handwritten digital signatures to serve as legal and irrefutable audit trails of who signed what, when, where and why.

By introducing the electronic signature into e-commerce, PenOp enables costeffective end-to-end electronic document management while protecting the intent of the involved parties. PenOp's handwritten digital signature raises the standards for reliability

Digital Signatures.

Page 54

and accountability demanded in corporate and government settings, but arrives without the costs, delays, and potential for fraud that accompanies paper solutions.

Table IV.

Recommended system requirements for PenOp ® Signature Series TM software:

486 PC or better.

8 MB Ram for Windows 3.1x, 16 MB for Windows '95/'98/NT.

1MB Hard Disk space.

Mouse.

Super VGA Graphics Card.

DOS 5.0/Windows 3.1x, Windows 95 or Windows 98 or Windows NT 3.51, 4.

PenOp is available for the following softwares: Acrobat Exchange, Word 95/97, Internet Explorer, Netscape, AutoVue, JetForm, and Lotus Notes.

Approvelt software

Silanis Technology's ApproveIt software (www.Silanis.com, 1999) encrypts and embeds electronic signatures within signed documents for secure storage and uniform transmission with the document. Additionally, the software's Intelligent Signature technology ensures compliance with legal, commercial and government standards for

electronic signatures. As a result, major companies in the industries of insurance, pharmaceutical, biotechnology, medical device manufacturing, government and DOD, and manufacturing currently use ApproveIt in document management, workflow, e-mail and inter/tranet systems. ApproveIt automates, manages, and secures any business approval process so as to ensure enterprise wide utilization regardless of the size of the company or the complexity of the signing process.

ApproveIt is being widely adopted in various industries. Market applications of ApproveIt's technology include:

- FDA Regulated company, Signature Pharmaceuticals, passed a FDA audit while using ApproveIt for the automation of forms including Validation Protocol drafts, GMP drafts, SOP's and Certificate of Analysis reports.
- The joint Chiefs of Staff in the U.S. Department of Defense are using ApproveIt in conjunction with their automated workflow system to allow senior-level officials to electronically sign a variety of documents and route them via their established workflow application for additional signatures or final processing.
- At Nationwide Insurance, 500 agents are using ApproveIt in the company's Electronic Account Processing system. The application enables representatives to capture customer account information to the home office.

Digital Signatures.

Page 56

- Telecommunications company, Williams Communications, has an electronic forms program which is an intranet solution that allows all sales employees to quickly access the appropriate forms/documentation. They are using ApproveIt to sign, and route the forms electronically for additional approvals.
- At Teal Electronics, ApproveIt's verification and file auditing capabilities have speed-up approval cycles and created a centralized electronic document control system. As a result, employees are provided with immediate access to approved procedures and engineering documents on-line.

Table V.

Recommended system requirements for ApproveIt Desktop Software:

486 PC or better.

8 MB Ram for Windows 3.1x, 16 MB for Windows '95/'98/NT.

4MB Hard Disk space.

Mouse.

Super VGA Graphics Card.

DOS 5.0/Windows 3.1x, Windows 95 or Windows 98 or Windows NT 3.51, 4.

ApproveIt is available for MS-Office (Word, Excel, Outlook) v '97,'98,2000, Adobe Acrobat v 3.0/4.0, JetForm FormFlow v. 2.x & 99, and CAD R12 & R13.

TECHNOLOGY EVALUATION.

From the participants interviewed, most companies fit within the following paper need distribution:

Table VI. Yearly paper demand in manufactu (averaged).	ıring / pharmaceutic	al industry
PAPER TYPE	PRICE	AMOUNT
• 400 boxes of letter paper (8½ x 11)	\$ 40.00	\$ 16,000.00
• 50 boxes of legal paper (8½ x 14)	50.00	2,500.00
• 120 boxes of computer paper (11 x		
17)	35.00	4,200.00
• 15 boxes of official paper (8½ x 11)	260.00	3,900.00
Total		\$26,600.00

This amount of paper gives us a total of \$26,600.00 yearly.

Also, the general average of managers, supervisors, etc., that might be needing the Electronic / Digital Signature Technology software are, on average, 80 people.

- Price for ApproveIt Software is \$149.00 per license. *1
- Price of PenOp Software depends on quantity, for the average indicated above, the price would be \$165.00 per license. *2

Table VII. Software vs Pape	r Cost Analysis	
Cost of Paper (Yearly)	ApproveIt Cost (80 licenses)	PenOp Cos (80 licenses)
\$ 26,600.00	\$ 11,920.00	\$ 13,200.00

Assuming that most of the companies participating within this research have computerized systems/networks/intranet/internet installed as part of their daily business activities, the only costs reflected are the paper cost versus the software costs. This simplifies a great deal our analysis and it is evident the benefit of implementing Electronic / Digital Signatures technology in any industry. We understand that, for example in the regulated industry, some processes have to be modified to implement this technology as part of the manufacturing processes (which involves more costs for personnel reviewing their Standard Operating Procedures, etc.). Also, costs for buying paper, storage and handling are not included.

^{*1} Price for ApproveIt software obtained from Web Site www.silanis.com
*2 Price for PenOp Software obtained from sales representative as a result of an inquiry at their web site www.penop.com.

CHAPTER IV CONCLUSION AND RECOMENDATIONS

Open networks such as the Internet are of increasing importance for world-wide communication. They offer the possibility of interactive communication between parties who may not have pre-established relationships. They offer new business opportunities by creating tools to strenghtn productivity and reduce costs, as well as new methods of reaching customers. Networks are being exploited by companies that wish to take advantage of new ways of doing business and new means of working, such as telework and shared virtual environments. Government departments are also using these networks in their interactions with companies and with citizens.

When we sign a document, we become accountable. Our signature indicates our agreement, acceptance and authorization to act and move forward. Our business processes rely on the signatures of customers, managers, suppliers and business partners to keep work flowing. Patients sign consent forms, judges approve warrants, mortgage lenders need a signature for a loan, engineers stamp drawings, insurance providers cannot proceed without a signature on an application. These acts of signing are critical to an organization's operation and success.

Even though governments or any regulating agency has accepted any technology, they are aware of a variety of signature alternative technologies and will consider their acceptance according to their performance characteristics and the level of security they

provide. The level of performance and security would be commensurate with the regulatory significance of the electronic record.

From E-mail to cellular communications, from secure Web access to digital cash, cryptography is an essential part of today's information systems in the form of digital signatures. Cryptography in digital signatures helps provide accountability, fairness, accuracy, and confidentiality. It can prevent fraud in electronic commerce and assure the validity of financial transactions. It can prove your identity or protect your anonymity. It can keep from reading your confidential documents.

Several different methods exist to sign documents electronically varying from very simple methods (e.g. inserting a scanned image of a hand-written signature in a word processing documents) to very advanced methods (e.g. digital signatures using "public-key cryptography"). The term "Electronic Signature" is currently being used, but there is currently no agreed definition for it. It is thus very likely that different interpretations may exist behind this wording.

Digital signature technology stems from the need to sign computer-based documents such as electronic mail messages, or documents within e-mails messages. Signing an electronic document directly, in its electronic form, eliminates the need to put the document on paper in order to sign it.

Electronic approval eliminates the need for pen and paper by allowing you to securely sign documents electronically. Electronic approval provides capabilities for the automatic management, and security of the entire business approval process. It drastically reduces the time and costs associated with traditional approval processes and allows for end to end electronic processes.

It is our recommendation to any company or institution that would like to implement this type of technology to evaluate its impact within their business and within their clients and suppliers. Keeping technology updated within any industry is a competitive advantage that most companies use to gain more clients/markets. Electronic / Digital signatures is no exception. As time passes, more and more companies will be adopting this type of technology into their business processes. We strongly recommend governments to continue to support technology through regulations of use for any technology that has legal impact to the society.

CHAPTER V FUTURE RESEARCH AND AREAS OF INTEREST

The field of Electronic / Digital Signature is, as most of the computer software related fields, a constant evolution. New areas and techniques are going to be introduced into this field. Some issues as security (especially for the federal government of the United States of America) and standards are clear areas of future research on the Electronic / Digital Signature field, especially after the approval of electronic signature laws.

Research companies and software developer companies will feel more confident to incorporate new technology that will comply with the governments requirements pertaining the use of electronic records and electronic / digital signatures. These companies are willing to obtain governments approval on their software to handle the electronic signature process. It is all a matter of time. We'll see.

REFERENCES

American Bar Association, Section of Science and Technology. <u>Digital Signature</u> <u>Guidelines Tutorial</u>. <u>www.abanet.org</u> 1999.

Baase Sara. <u>A Gift of Fire. Social, Legal, and Ethical Issues in Computing</u>. Prentice Hall, 1997.

Barker, Tim; Bamforth, Paul (1998). <u>The Electronic Signature: Implications for the European Industry.</u> Erman et al, 1997

Glossary of PC and Internet Terminology.

http://homepages.enterprise.net/jenko/Glossary/G.htm

Hancocks, John. <u>Digital John Hancocks</u>. Wired news and report <u>www.wired.com</u> 1999.

Interlink Electronics. Epad Technology. www.interlinkelec.com
International Organization for Standardization (ISO). ISO 9000 and ISO 14000 in Plain Language. www.iso.com 1997.

PenOp Software. PenOp Corporation. www.PenOp.com 1999.

Puerto Rico Chamber of Commerce. Puerto Rico Business Register. 2000.

Rasilainen, Harry. <u>ETSI Standards on Electronic Signatures to secure electronic commerce.</u> <u>www.etsi.org.</u> 2000.

Silanis Tecnology. <u>ApproveIt Software</u>. <u>Electronic Approval Overview</u>. <u>www.silanis.com</u>. 2000

Tech Encyclopedia. www.techweb.com/encyclopedia/defineterm

Tozer, Chris. <u>ABA section creates First Digital Signature Guidelines to Aid in security of the Internet</u>. 1999

U.S. Department of Health and Human Services. Food and Drug Administration (1997).

21 CFR Part 11. Electronic Records; Electronic Signatures; Final Rule. Electronic Submissions; Establishment of Public Docket; Notice.

U.S. Department of Health and Human Services. Food and Drug Administration. Electronic Identification/Signature Working Group. (1992, 1996). <u>Progress Report.</u>

Wright, Benjamin. Congress set to finalize latest e-signature law. What does really means? www.PenOp.com 1999.

Zanger, Larry. <u>Definitions of the term "Digital Signature" in Enacted Legislation</u>. <u>www.mbc.com</u> 2000.

APPENDIX A: Guideline Questions used in interview.

Name:			Date:	_
Title:				
	Manufac			
	Pharmac	ceutical		
	Other.			
How many employees	the company	or branch has	3?	
Ooes the company use	s any technolo	ogy for Electr	onic / Digital signatu	ure?
f not, is the company		f planning to	use any of the availa	able technology for
low much money do	es the compa	ny spend on	naner (vearly on any	w kind: conject fav
omputer, etc.).		my spend on	paper (yearry on any	with copies, tax,
ny other comment ompany/branch?	s related to	electronic	Signature/Records	applied to your
-				

APPENDIX B: Result Tabulation from Interviews.

The next table contains all information related to paper demand in the manufacturing/pharmaceutical companies interviewed. Company names are not shown due to confidentiality agreement from most of the companies.

Table	VIII.			grand and
Paper	Demand for Mar	nufacturing/Pha	armaceutical Indus	try (Yearly)
	Letter	Legal	Computer	Official
	Paper	Paper	Paper	Paper
	300	20	100	25
	500	40	275	35
	320	80	150	15
	450	75	180	20
	460	55	130	18
	340	40	100	9
	350	45	80	10
	400	30	130	18
	250	40	145	5
	550	70	95	32
	520	25	90	27
	425	45	75	15
	450	80	50	15
	375	90	100	16
	360	60	140	12
	350	70	100	8
	450	40	150	14
	420	35	170	12
	430	40	90	10
TO LOVE SOUT	300	20	50	_4
TOTAL	400	50	120	15

APPENDIX C: List of Pharmaceuticals established in Puerto Rico.

ASANOFI PHARMACEUTICAL po Box 70322 San Juan, OR 00936-8322 edif Royal Bank Ste 285 Hato Rev. PR 00917 Tel. (787) 758-1033 Fax (787) 753-1263 General Manager losé Méndez nistribution of Pharmaceutical sales Volume: \$10M Plus - \$50M mployment Bracket: 26 - 50 AUPJOHN INTER-AMERICAN Area Indl Higuillar Pueblo Viejo. PR 00920 Tel. (787) 792-6667 undicinal & Botanical Products WYETH - AYERST LABORATORIES (PR) INC PO Box 362917 San Juan, PR 00936-2917 Tel. (787) 782-3838 Pharmaceutical Product Distributors 1003851 Anhthalmic Goods ACENTROVISION - CLINICA DE OPTOMETRIA 70 Box 2825 Hato Rey, PR 00919 Tel. (787) 764-4848 Hictor Alfonso Ostometry Clinic **ACLINICA VISUAL MORALES** WETTE DRA & ASSOC 10 Box 34210 San Juan, PR 00926 H (787) 758-2275 **Potometrist** AESSILOR INDUSTRIES abanetas Ind Park, Mercedita Ponce, R 00715 H (787) 848-4130 nance & Administrator Vice-Pres. Mbeida Irizarry ans Manufacturer **MENTOR CARIBE** 0. Box 1358 El Jibaro Ind'I. Park dra, PR 00739 (787) 739-8418 int Manager Juel Soler ^{leo}cular Lens Manufacturer The Business Register, where business

finds business.

```
▲ OCULAR SCIENCES PUERTO RICO INC
```

P O Box 2801 Santa Isabel.
PR 00757
Repto Ind. La Playa Rd. 538
Santa Isabel. PR 00757
Tel. (787) 845-2113
Fax (787) 845-3236
Manager
Fernando Vázquez
Manufacturers & Distributors of Contact Lens
Sales Volume: S5M Plus - \$10M
Employment Bracket: 450

▲ OPTI-FACTORY

El Centro Bldg. Marginal 14–8 M. Rivera Ave Hato Rey. PR 00918 Tel. (787) 758–7878 Vice–President Luis C. Colón Optical Lab and Vision Center. Optometry Services. Sale and Repair of Eye Glasses and Security Lenses.

▲ PEARLE VISION CENTER OF PRINC

1122 Ponce de Leon Río Piedras. PR 00925 Tel. (787) 765–0088 Managing Director Caribbean Donald Johndrow Vision Test. Contact Lenses. Frames and other Ophthalmic Goods

▲ PROFESSIONAL OPTICAL SERVICES INC

P. O. Box 2636 Bayamon Sta Bayamón, PR 00960-2636 Tel. (787) 785-1862 Owner Anthony Mark Lens Manufacturers. Open Monday to Friday from 8:00 AM to 4:00 PM

▲SOUTHERN OPTICAL COMPANY

Sunny Isle Professional Bldg. St Croix, USVI 00820 Tel. (340) 778–6565 Manager Margaret Rennie Eye Glasses. Contact Lenses and everything for the Eyes.

002834 ____ Pharmaceutical Preparations

▲ A J BART
P. O. Box 1360 Gurabo, PR 00778
Tel. (787) 737–8445
Owner
Alberto S. Baltolomei

Products.

Distributors of Pharmaceutical

▲ABBOTT PUERTO RICO OPERATIONS

P O Box 278 Barceloneta, PR 00617 Tel. (787) 846–6900 VP. Gen. Mgr. Abbott P R Operation José L. Rodríguez Manufacturers of Health Care Products

▲ ACCUPHARMA RESEARCH AND SCIENTIFIC CONSULTING INC P O Box 1340 Gurabo.

PR 00778–1340
Tel. (787) 850–4215
President
José F Colón Reyes
Generic Medicaments, Research &
Development, Microbiology
Pharmaceutical Test, Sample Testings,

ALCON (PUERTO RICO) INC

P. O. Box 3000 Humacao, PR 00792 Tel. (787) 852-3080 General Manager Milton Barley *Pharmaceutical Products Manufacturer*

▲ ALLERGAN AMERICA

P. O. Box 60 Hormigueros. PR 00660 Tel. (787) 849-3895 General Manager José Luis Díaz Pharmaceutical Preparations Manufacturer

AMGEN MANUFACTURING INC



P 0 Box 4060 Juncos,
PR 00777-4060
Road 31 Km. 24.6 Juncos, PR 00777
Tel. (787) 734-2000
Tel. (787) 734-6161
Director/Gen Manager
James Sanabria
Operations Manager
Miguel Nazario
Plant Controller
Jaime Arraya
Manager Human Resources
Axel Lluch

▲AYERST-WYETH PHARMACEUTICALS INC

Biotechmology

P. 0. Box 10001 Guayama, PR 00785 Tel (787) 864-4010 Vice-President & General Manager Mariano Martinez Mora Pharmaceutical Products Manufacturer

BASF PHARMACEUTICALS

BASF Pharmaceuticals A Unit of BASF

P O Box 795 Jayuya, PR 00664-0795

Road 144 Km 2.6 Jayuya, PR 00664

Tel. (787) 828–0990
Fax (787) 828–6440
Vice President & General Manager
Carlos R León
Buyer
Victor Arcelay
Pharmaceutical Products Manufacture
Parent/Affiliates/Branches

• BASF Pharmaceuticals

New Jersey



The Business Register

is the most complete

and up-to-date

Business to Business

Directory

R

TI

F;

H

AI PI Bi

1.1

PI

0.

IV

Pl

 P_{I}

in Puerto Rico.

MAXTER CARIBE INC



20 Box 1290 Guayama. 28 00785-1290 Roule 3 Km 142.5 Guayama, 28 00784 [el. (787) 864-5050 fax (787) 866-2714 General Manager idol Ghigliotty P.E. Unterial Director ator M. Guzman, Esq. shoulacturing of Anesthetics mimaceutical Products Division PHENL/Affiliates/Branches 180 C Health Care Inc 1107938 roducts & Services Koffurane USP, Enflurane USP. ukthoxyflurane ,Deflurane U S P Indemarks & Brandnames inrane, Forane, Suprane ales Volume: 150-200 Employment Bracket: 101 - 150







ABAXTER HEALTH CARE CORP OF PR

70 Box 518 Jayuya, PR 00664 M (787) 828-3700 ant Manager Edio Alvarez

henterals Solutions and Medical wices

NOTECH GROUP FENWAL MOISIN



10 Box 832 Maricao, PR 00606 1357 Km 0.8 Maricao, PR 00606 1. (787) 838-3000 11(787) 838-2110 man Resources Manager gie Lugo Manager . amin Padilla Director (Fenyzal del Caribe) Van Heems A Manager sse Betancourt maceutical Products Manufacturer

Mucts to Collect, Store and

Muster Blood and its Components

Parent/Affiliates/Branches · Baxter Healthcare Corp.

Chicago, Deerfield ILL 00615 Products & Services Systems for the Collection. Separation, Preservation, Manipulation, and Transfusion of Blood and Blood

Components. Trademarks & Brandnames

Fenwal, Baxter



▲ BIOTECH GROUP FENWAL DIVISION

P O Box 832 Maricao, PR 00606 Rd. 357 Km 0.8 Maricao, PR 00606 Tel. (787) 838-3000 Fax (787) 838-2110 Human Resources Manager Angie Lugo Pharmaceutical Products Manufacturer, Products to Collect, Store and Administer Blood and its Components.

▲ BIOVAIL LABORATORIES INC

P O Box 3468 Carolina. PR 00984-3468 Sabana Abajo Ind'I Park 34 Calle B Iturregui Ave Carolina, PR 00983 Tel. (787) 750-5350 Fax (787) 750-5360 General Manager Carmen M Reves Reves Manufacturing Research & Development Employment Bracket: 51-103

BRISTOL LABORATORIES CORPORATION BRISTOL CARIBBEAN INC



Bristol Laboratories → Corporation Bristol Caribbean, Inc. Mayaguez Operations

P 0 Box 897 Mayaguez, PR 00681 Trade Zone 7 Rd. 114 Foreign Mayaguez, PR 00680 Tel. (787) 834-0185 Fax (787) 834-4182 Vice-President & General Manager Theodore Iliopoulos Human Resources Director Rosa Beatriz Sanabria Oncologic Business Unit Leader Jean F Schneider Liquid & Question Business Unit Leader Javier Santana Comptroller Edgardo Gratacós CPA Materials Control Director Javier Santana

Director of Engineering

José M Maldonado

Engages in the Production of Non-Beta Lactam Oral Dosage Pharmaceutical Products and Oncological Drugs.

Parent/Affiliates/Branches

 Bristol-Myers Squibb Company 345 Park Ave. New York NY 10154 Products & Services Analgesic & Anti-Cancer Trademarks & Brandnames Bristol-Myers Squibb Co.



▲BRISTOL LABORATORIES CORPORATION BRISTOL CARIBBEAN INC

P O Box 897 Mayaguez, PR 00681 Trade Zone 7 Rd. 114 Foreign Mayaguez, PR 00680 Tel. (787) 834-0185 Fax (787) 265-4111 Vice-President & General Manager Theodore Iliopoulos Engages in the Production of Non-Beta Lactam Oral Dosage Pharmaceutical Products and Oncological Drugs

BRISTOL-MYERS BARCELONETA INC



BRISTOL-MYERS BARCELONFTA, INC.

P O Box 657 Barceloneta, PR 00617 Rd. 2 Km. 56.4 Barceloneta. PR 00617 Tel. (787) 846-3800 Fax (787) 846-7845 Administrative Assistant Elizabeth Padılla Antibiotic Manufacturer Parent/Affiliates/Branches

. Bristol Myers Squibb Company 345 Park Ave. New York NY 10154-0037 Products & Services

Amoxicillin Manufacturer for the Local and International Market

Trademarks & Brandnames

Polycillin, Buspar, Polymox, Beta Pen, Dicloxcil, Prostaphlin, Duricef, Naful, Staphcillin, Dyna Pen, Ultraceph, Pen V, Prostaphlin, Duricef. Natul, Staphcillin, Dyna Penn. Ultraceph, Pen V Sales Volume: Over \$50M Employment Bracket: 600 Plus





▲CHIRON BETA CORPORATION

P O Box 1624 Canóvanas, PR 00729 Tel. (787) 876-1400 Secretary Administrative Marta Ortiz Pharmaceutical Products

▲COCHARON WHOLESALE P 0 Box 8567 Humacao, PR 00792 Tel. (787) 852-4325 Manager Rafael Mangual Pharmaceutical Preparations

▲COLON DE JIMÉNEZ ANA L P 0 Box 22678 U P R Sta. San Juan, PR 00931 Tel. (787) 763-1454 Owner Ana Colón Dermatologist

▲ DADE DIAGNOSTIC OF PR INC

P 0 Box 865 Aguada, PR 00602 Tel. (787) 868-5500 Manufacturing Manager Randy Howe Manufacturing of Reagents and Laboratory Controls

▲ DANBURY PHARMACAL P.R. INC.

P 0 Box 886 Humacao, PR 00792

Road 3 Km. 76.9 Humacao Ind'l. Park Humacao, PR 00792 Tel. (787) 852-5151 Fax (787) 852-5974 General Manager Blanca Meléndez Pharmaceutical Manufacturing Sales Volume: \$5M Plus - \$10M Employment Bracket: 151 - 200

▲ DEL MAR PHARMACY SERVICE INC

P O Box 233 Mercedita Ponce, PR 00715-0043 Tel. (787) 842-6263 Pharmaceuticals & Related Products Distribution

▲ DENVER CHEMICAL (PR) INC

HC-04 Box 4012 Humacao, PR 00791-9502 Tel. (787) 852-3240 Manufacturing Manager Juan R. Suarez Pharmaceutical Products Manufacturer

It pays to register

in the Business Register

DORASOL LABORATORIES

p0 3906 San Juan, PR 00936 Tel. (787) 753-6549 Agustín Rodríguez Kissell Manufacturers of Pharmaceutical

products

ADROGUERIA GONZÁLEZ INC PO Box 350 Ponce, PR 00733

Tel. (787) 724-1078 pharmaceutical Preparations

▲DROGUERIA RIO PIEDRAS

590 De Diego Ave. Río Piedras, PR 00924 Tel. (787) 751-5030 President Raúl González Wholesale and Distribution of Medicines.

DUPONT MERCK PHARMA

PO Box 301000 Manatí. PR 00674-3000 Tel. (787) 854-1030 President William Henández Pharmaceutical Products

AEATON LABORATORIES

P 0 Box 1055 Manatí, PR 00674 Tel. (787) 854-1520 Vice-President General Manager Ramón Sepulveda Pharmaceutical Products Manufacturer

▲ENGRAPH LEHIGH PRESS PUERTO RICO

P O Box 1469 Juncos, PR 00777 Mamey Ind'l Center Road 189 Km 12.4 Juncos, PR 00777 Tel. (787) 734-1000 Fax (787) 734-1004 President Luis Herrera Insert and Outsert for Pharmaceutical Industries Office Hours, Mon - Fri from 8:00 AM to 5:00 PM Sales Volume: \$5M Plus - \$10M Employment Bracket: 101 - 150

▲ENVIRONMENT PRO-TEK

P O Box 38053 Airport Station San Juan, PR 00937-1053 Tel. (787) 749-9534 Consultant René Santiago Air & Water Purificator, Oxygen Generator. Sediment Remover. Biodegtable Products. Insulation For Boiler.

Looking for a Fax number? Get it fast in the Fax Section. ▲EX-LAX INC

H C - 01 Box 16629 Humacao. PR 00791-9731 Tel. (787) 852-3190 Executive Vice Pres. & General Mgr Santos Troche Laxative and Antiflatulex Manufacturers

▲ FAULDING PUERTO RICO INC

P O Box 250471 Ramey Branch Aquadilla PR 00604-0471 Tel. (787) 890-3000 General Manager Juan Miguel Gomez Pharmaceutical Products

▲ GENERICS OF PUERTO RICO INC

P O Box 11533 Fdez Juncos Sta Santurce, PR 00910 Monte Rey Urb. 3 Calle Acacia Pueblo Viejo, PR 00920 Tel. (787) 792-2430 Fax (787) 782-0990 President Carlos A. Fraga Pharmaceutical Products Distributors Sales Volume: \$1M Plus - \$5M Employment Bracket: 26 - 50

▲GLAXO WELCOME

P 0 Box 363461 San Juan. PR 00936-3461 Tel. (787) 250-7580 Finance Director Luis Cintrón Pharmaceuticals Wholesaler

▲HOECHST MARION ROUSSEL PUERTO RICO INC

P O Box 2120 San Juan. PR 00922-2120 Tel. (787) 782-1900 General Manager Francisco Nordelo Pharmaceutical Products

JANSSEN ORTHO LLC

JANSSEN PRODUCTS

HC - 02 Box 19250 Gurabo. PR 00778-9629 Bo. Mamey II Road 933 Km. 0.1 Gurabo. PR 00778-9250 Tel. (787) 789-5000 Fax (787) 272-7644 Fax (787) 272-7602 VP Manufacturing & General Manager William B Nelson

Director of Logistic & Materials Mgnt Margarita Hernández Finance Director Tony Perez Human Resource Manager Fernando Plaud OA/QC Director Eric Olivieri Director of Engineering Maintenance/Environmental & Safety Nallagounder Kuppusamy Pharmaceutical Products Parent/Affiliates/Branches Johnson & Johnson Corporate Worldwide Headquarters One Johnson & Johnson Plaza New Brunswick NJ 08933

Products & Services

1125 Harbourton Road Titusville

Propulsid, Prisperdal, Sporanox. Nizoral, Vermox, Hismanal Sales Volume: Over \$50M Employment Bracket: 401 - 450

· Janssen Pharmaceutical

NJ 08560-0200



Employment Bracket: 500 Plus

Manufacturer of Pharmaceutical

Sales Volume: \$5M Plus - \$10M

-LILLY DEL CARIBE INC.

P O Box 1198 Carolina.

P.B. Ind'l Park Km 12.6 65th Inf Ave

PR 00986-1198

Carolina, PR 00985

Tel. (787) 257-5555

Tel. (787) 257-5333

Fax (787) 257-5544

Fax (787) 257-5988

Paul Ahern

Iliana Rivera

Products

Evelyn Rodriguez

President & General Manager

Director Human Resources

Director Quality Control

▲ JANSSEN PRODUCTS

HC - 02 Box 19250 Gurabo, PR 00778-9629 Bo. Mamey II Road 933 Km. 0.1 Gurabo, PR 00778-9250 Tel. (787) 789-5000 Fax (787) 272-7644 VP. Manufacturing Tomás Ramírez Pharmaceutical Products Sales Volume: Over \$50M Employment Bracket: 401 - 450

▲ LEDERLE PARENTERALS INC

P O Box A C Pueblo Sta. Carolina. PR 00984-4904 65 Infantry Ave. Km. 9.7 Carolina, PR 00979 Tel. (787) 752-7474 Fax (787) 762-3395 President & Gen. Manager Alfredo R Nadal Pharmaceutical Products Sales Volume: \$5M Plus - \$10M Employment Bracket: 500 Plus

▲LIFESCAN (PR) INC

P O Box 5001 Cabo Rojo, PR 00623 Bo Pedernales Road 308 Km 0.8 Cabo Rojo. PR 00623 Tel. (787) 255-7700 Fax (787) 255-7713 Finance Manager Max Roldán Reagent Strips for Glucose Monitoring. Open Monday to Friday from 8:00 AM - 5:00 PM Employment Bracket: 251 - 300

The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

CAS - INSERTCO



aRox 377 San Germán, PR 00683 entro Indl Park Rd. 102 Km 33.2 væl San Germán, PR 00683

(787) 892-1268 (1/87) 892-4112

salzano Manager Ufret Ufret

Soluction Coordinator

Cruz Manager stred Centeno

masing Agents unida Mora

domer Service Morales

munt Executive Sevilla

outs Outserts & Labels for amaceutical and Electronic stries. Starch Displacement & Sess Pharmaceutical Preparation.

Volume: \$5M Plus - \$10M doyment Bracket: 90 - 100



MARION & COMPANY 180x 3009 Manati, PR 00674 (787) 854-3005

legial Manager asio Rivera

maceutical Products

MCGAW OF PUERTO RICO

180x 729 Sabana Grande,

(787) 873-4600 eral Manager Ranfit

dal Devices Manufacturing

Looking for

an internet address?

Get it fast

In the internet Section.

MCNEIL CONSUMER PRODUCTS A DIV OF J & J CONSUMER CO P R INC



PR 00771-2009 Bo. Montones Road 183 Km 19.8 Las Piedras, PR 00771 Tel. (787) 733-1000 Tel. (787) 782-7030 Fax (787) 733-6616 General Manager Edgardo J. Fabregas Over the Counter Propietary Products Parent/Affiliates/Branches • McNeil Consumer Products Inc.

P 0 Box 2009 Las Piedras,

Camp Hill Road 19034

Trademarks & Brandnames Tylenol Employment Bracket: 351 - 400



▲MCNEIL PHARMACEUTICAL A DIV OF OMJ PHARMACEUTICAL INC

P. O. Box 710 Dorado, PR 00646-0710 Tel. (787) 796-1540 General Manager Krenly Cruz Manufacturer of Capsules. Tablets. Caplets and Liquid of Ethical Pharmaceutical Products

▲ MEDISEARCH P R INC

P O Box 2460 Guayama. PR 00785-2460 Tel. (787) 864-0684 President John K. Whitney Manufacturer of Therapeutic Pads. Heat Therapy Pads, Pressure Ulcer Relief, Thrombo Cuff.

MERCK SHARP & DOHME QUIMICA DE PRINC ARECIBO OPERATIONS



MERCK SHARP & DOHME

P O Box 1011 Sabana Hoyos Barceloneta, PR 00688 Road 2 Km. 60.3 Sabana Hoyos. PR 00688 Tel. (787) 846-1600

Fax (787) 846-5580 Director of PR Operations Richard S. Bowles Senior Director Mfg Services Luis Couto General Manager Iván Lugo Director of Public Affairs Rafael Robert Purchasing Manager PR Operations Luis Archilla **Financial Director** Carlos Gomez LS Operation Head for PR. Luis E. Ortiz

Pharmaceutical Manufacturing Parent/Affiliates/Branches

- Merck and Company Inc Whitehouse Station NY • MSD Quimica de PR. Caguas Operations
- Caguas PR 00725 • MSD Quimica de PR Barceloneta
- Operations P O Box 601 Barceloneta PR 00617 Trademarks & Brandnames

Prilosec, Fosamax, Proscar Sales Volume: Over \$50M Employment Bracket: 500 Plus



▲MOVA PHARMACEUTICAL CORPORATION

P O Box 8639 Caguas, PR 00726 Villa Blanca Ind'l Park Rd 1 Km 34.1 Caguas, PR 00726 Tel. (787) 746-8500 Fax (787) 743-7669 President & CEO Joaquín Viso Pharmaceutical Products Employment Bracket: 500 Plus

▲ NESSAN LABORATORIES INC

P. O. Box 1941 Carolina, PR 00984 Tel. (787) 769-5053 President Nellie E. Sánchez Pharmaceutical Products

O M J PHARMACEUTICAL INC

OMJ Pharmaceuticals, Inc.

P 0 Box 367 San German, PR 00683 Rd. 362 Km. 0.5 San Germán, PR 00683 Tel. (787) 892-2245 Fax (787) 892-2095 General Manager Felix Morales Lye Care Products Manufacturers

Parent/Affiliates/Branches

Ortho Biotech Inc. U.S. Route 202 P O Box 670 Raritan 00869-0602 Products & Services

Ophthalmics Products, Medical Devices Employment Bracket: 201 - 250

▲ ORTHO PHARMACEUTICAL/A DIV OF J & J PHARM CO

(PR) INC P. O. Box 463 Manatí, PR 00674 Tel. (787) 854-1800 General Manager Krenly Cruz Contraceptives and Semi-Solids.

▲P C R DE PUERTO RICO

P O Box 960 Punta Santiago PR 00741 Road 3 Km. 76.9 Humacao. PR 00791 Tel. (787) 852-4520 Fax (787) 852-4284 Plant Manager Santiago Hernández Reyes Organic Chemicals for Cancer Treatment Employment Bracket: 0 - 25

The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

PACO PUERTO RICO INC

PO Box 1661 Canóvanas, PR 00729 San Isidro Ind Park Road 188 Km 0.5 Canóvanas, PR 00729 Tel. (787) 876-6362 Tel. (787) 876-6258 Fax (787) 876-0165 Fax (787) 876-5099 Plant Manager Rubén Aguayo Human Resources Manager Frances Guzmán Finance Director Brian Fichthorn Account Executive Miguel Parada Material Manager Antonio Rivera

complete Manufacturing and Packaging Services for the

Pharmaceutical and Health Care Industries.

Parent/Affiliates/Branches

• Paco Pharmaceutical Services Inc New Jersey NJ Employment Bracket: 100-225

PFIZER PHARMACEUTICALS



PO Box 628 Barceloneta, PR 00617 Cruce Dávila Rd. 2 Km 58.2 Barceloneta, PR 00617 Tel. (787) 846-4300 Fax (787) 846-7022 Fax (787) 846-5077 General Manager Anthony Maddaluna Director, H R and Public Affairs Héctor Corretjer Pharmaceutical Products Manufacturing. Parent/Affiliates/Branches •Pfizer Inc. 235 E. 42 St. New York City NY 10017 Trademarks & Brandnames feldene, Procardia, Procardia XL,

Sales Volume: Over \$50M Employment Bracket: 1000 Plus

Minipress / Minizide, Sinequan,

Zythromax. Cardura, Zoloft

Glucotrol, Diflucan, Antivert / Bonine,

It pays to register in the Business Register **▲**PROCTER & GAMBLE PHARMACEUTICAL PUERTO RICO INC

P O Box 1055 Manatí. PR 00674 Tel. (787) 854-1520 Vice Pres. & Gen. Manager Ramón Sepúlveda Pharmaceutical Products Manufacturer

REEDCO & DENTCO INC



Faulding Puerto Rico, Inc.

H C - 04 Box 4013 Humacao. PR 00791 Humacao Ind'l Park Rd 3 Km 76.4 Humacao, PR 00791 Tel. (787) 852-3400 Tel. (787) 724-6756 Fax (787) 850-2300 Fax (787) 852-7870 General Manager Luis R. Acevedo Production Manager Lizzette Pérez Quality Service Manager Reynaldo Velázquez Maintenance Facility Manager Victor Marrero Traffic & Warehouse Manager Angel Rodríguez Human Resources Manager Mildred Sein Administration Manager Eduardo Clemente Plant Engineer & Regulatory Affairs Ivan Santiago Inventory Control Manager Juan C Aponte Traffic Supervisor Miguel A. López Pharmaceutical Products Manufacturer Parent/Affiliates/Branches • Block Drug Co Inc 257 Cornelison Ave NJ 07302 Products & Services Dental Product. Shampoo's, Pharmaceutical, Dermatologic Trademarks & Brandnames Tegrin, Sensodyne-F, Poligrip, Super Poligrip, Dentu-Creme, Sensodyne, R & C, B C Tablet. Nytol, Tegrin L T. Balmex, Durascreen



Sales Volume: \$5M Plus - \$10M

▲ REEDCO & DENTCO INC

H C - 04 Box 4013 Humacao, PR 00791 Humacao Ind'l. Park Rd. 3 Km. 76.4 Humacao. PR 00791 Tel. (787) 852-3400

Fax (787) 850-2300 General Manager Luis R. Acevedo Pharmaceutical Products Manufacturer Sales Volume: \$5M Plus - \$10M Employment Bracket: 301 - 350

RHONE-POULENC RORER CARIBBEAN



P O Box 364824 San Juan, PR 00936-4824 De La Cruz Plaza Suite 100 Metro Office Park Guaynabo, 00968-1705 Tel. (787) 783-6868 Fax (787) 783-4845 Fax (787) 783-4346 Finance Director Angel B. Méndez General Manager & Vice President Isidro J Ferrer Marketing & Sales Director Nelson De Jesus Sales Director Ana L Del Rio Sales & Marketing of Pharmaceutical Preparations Products & Services Lozol, Tussar, SLO-BID, Nasacort,



Penetrex, Nitrolingual Zagam Trademarks & Brandnames Sales Volume: \$5M Plus - \$10M Employment Bracket: 51 - 100



RHONE POULENC RORER PR

P O Box 345 Manatí, PR 00674-0345 604 Road Bo San José Manatí, PR 00674 Tel. (787) 854-1058 Fax (787) 854-3100 VP & General Manager Carlos Santiago Comptroller Jaime L. Sanabria Operations Director Franco Negrón Human Resource Director Victor Osuna Quality Control Director Jorge Cotto Materials Management Director

Dolores Fernández

Pharmaceutical Preparations

Manufacturer of Tablets, Capsules,

Creams & Inhaled Therapy Products.

Project Engineer José R. Osorio

Parent/Affiliates/Branches

•Rhone Poulenc Rorer, Inc. 500 Arcola Rd, P O Box 1200 Collegeville 19426-0107

· Rhone Poulenc Rorer Caribbean Corp

De La Cruz Plaza S-100 Metro Office Park Guaynabo PR 00968-1705

Products & Services Trademarks & Brandnames

Nasacort, Lozol, Azmacort, Slo-bid, Hygroton, Vytone, Benzamycin, Benzagel, Sulfacet, Rilutek, Nicobid. Hytone, Penetrex, Masacort AQ Employment Bracket: 351 - 400



RIMACO INC

P O Box 8895 Fdez. Juncos Station Santurce, PR 00910 Villa Caparra Ext. Calle Marginal Buchanan Guaynabo, PR 00966 Tel. (787) 792-9512 Fax (787) 782-8310 President Ricardo Mayo Alvarez Marketing Manager Daniel Torres Torres Treasurer/Vice President Ricardo Mayo Alvarez Jr. **Executive Secretary** Ramona Orozco Pharmaceutical Products Distributor. Sales Volume: \$5M Plus - \$10M Employment Bracket: 0 - 25

▲ SANOFI PHARMACEUTICAL INC

P O Box 70322 San Juan, PR 00936-8322 Tel. (787) 758-1033 General Manager José Méndez Distribution of Pharmaceutical Products.

Contact us

at our internet site

www.pbrb.com.

SCHERING-PLOUGH RADUCTS INC



1804 1779 Las Piedras. Jco ind'l Park Rd 183 Piedras, PR 00771 [4] (787) 733-2323 (a) (787) 783-3333 ar(787) 733-3229 (187) 733-2333 ariai Manager Rodriguez eration Director an Ciena aptroller antiago nan Resources Manager sse Cordoves senals Director an Aldarondo uneering Manager mes Kregloh My Control Director ando Santiago umaceutical Manufacturer of Bulk inshed Dosage Form, Specializing Sustained Release Technologies tract Manufacturing Services hent/Affiliates/Branches weing Plough Corporation halda Farms P O Box 1000

Mson NJ 07940-1000 ducts & Services atin. Unidur, Normodyne, Theo-Dur क्षेड, K-Dur Tablet... Eulexin

SVolume: \$5M Fars - \$10M doyment Bracket '51 - 300



SCHMID PRODUCTS CORP

48ox 4016 Humai ao, 00791-9502 1787) 852-2476 ident & General for lager A. Marrero

loms for Natural ling and

Wivity Manufactu s

EARLE CARIBBEAN

🕅 367189 San Juan, 0936-7189

(787) 258-6474

Grieco Maceutical and Consumer VIs. Sales and Distribution SEARLE, LTD



Food · Health · Hope P O Box 11247 Barceloneta, PR 00617-1247 Rd 140 Km 64.4 Barceloneta, PR 00617 Tel. (787) 846-5000 Fax (787) 846-6595 Fax (787) 846-2640 General Manager Hector Jové Comptroller Iván Marcano Quality Control Director Rosaura Ortiz Materials Director Vivian Molinari Human Resource Director José L. Narváez **Engineering Director** Felipe Sánchez Pharmaceutical Products



Manufacturing. Exclusive Distributor of

Visipaque, Omniscan, Omnipaque, And

Nycomed Products (Omnipaque):

Picker International del Caribe Inc.

Trademarks & Brandnames

Third Party Manufacturing

▲ SEIN MÉNDEZ LABORATORIES INC

P O Box 10757 San Juan, PR 00922-0757 Tel. (787) 793-2700 General Manager Francisco Santos Manufacturer & Distributors of Pharmaceutical O T C Products

SMITHKLINE BEECHAM INTERAMERICAN

Pharmaceuticals

P 0 Box 2160 San Juan. PR 00922-2160 Calle Diana #29 Amelia Ind'l Park Guaynabo, PR 00922 General Manager

Finance Manager Armando Rodríguez Sales of Ethical Products. Trademarks & Brandnames S B-I A C Puerto Rico

Sales Volume: \$10M Plus - \$50M Employment Bracket: 51 - 100



SQUIBB MANUFACTURING INC

. The Residence W. L. S.

SMITHKLINE BEECHAM

PHARMACEUTICALS

SmithKline Beecham Pharmaceuticals

P O Box 11975 Cidra. PR 00739-1975 Bo. Certeneias Rd 172 Km 9.1 Cidra. Tel. (787) 766-4000 Tel. (787) 739-8401 Fax (787) 250-3710 President-General Manager José Luis Rosado Vice-President Finance Raúl Cermeño **Business Development Director** Joan Cruz Pharmaceutic Manufacturing Director Betsy Rodriguez Vice-President Human Resources Sonia Berrios Vice Pres. Public Relations Jorge González VP Quality Assurance Adalberto Ramirez **Enginering Director** Ismael Guzmán Pharmaceutical Products Parent/Affiliates/Branches

· Smithkline Beecham

Smithkline Interamerican

P O Box 2160 San Juan

PR 00922-2160

Brand

Paxil

PR 00731

PR 00731

Tel (787) 8-12-0313

S B House Great West Road London

• Smithkline Beecham Consumer

P O Box 9597 Hato Rey PR 00919

Tagamet, Ecotrin, Feosol, Stelazine,

Relafen, Dyazide, Bactroban, Compazin

Trademarks & Brandnames

Sales Volume: Over \$50M

Employment Bracket: 500 Plus

▲ SPECIALTIES CHEMICAL

Playa Ponce 46 Calle Mirasol Ponce.

DBA PONCE PHARMA

P O Box 277 Playa Sta. Ponce.





Tel. (787) 774-8000 Fax (787) 774-0302

José Vargas

P 0 Box 609 Humacao, PR 00792 Road 3 Km. 77.5 Humacao. PR 00791 Tel. (787) 852-1255

Fax (787) 852-3800 VP & General Manager Francisco Gutierrez Financial Site Leader Tina Fiumenero Human Resources Site Leader Grisel Castro

Director of Quality Control Luis O. Rodriguez

Director of Manufacturing Bernie Morales

Director of Maintenance Israel Diaz Chemical Products Manufacturers

Parent/Affiliates/Branches · Bristol Myers Squibb Company 345 Park Avenue 10154 Sales Volume: \$5M Plus - \$10M Employment Bracket: 500 Plus



▲ SQUIBB MANUFACTURING INC

P 0 Box 609 Humacao, PR 00792 Road 3 Km. 77.5 Humacao, PR 00791 Tel. (787) 852-1255 Fax (787) 852-3800 General Manager Francisco Gutierrez Chemical Products Manufacturers Sales Volume: \$5M Plus - \$10M Employment Bracket: 500 Plus

Looking for

an internet address?

Get it fast in

the Internet Section.

SONOCO OF PRINC



SONOCO P O Box 399 Yabucoa, PR 00767 Tel. (787) 893-2675 Tel. (787) 893-2600 Fax (787) 893-2200 General Manager José Zayas Plant Superintendent

Octavio Divison Sales Representative Jackie Rosado Paper Products & Fiber Composite

Cans and Spiral Tubes Parent/Affiliates/Branches

 Sonoco Products Co. Hartsville SC

Trademarks & Brandnames Sonotubes, Sonovoids, Sonomolds Employment Bracket: 26 - 50







▲SUNRISE PAPER CORP P O Box 9702 Carolina. PR 00988-9702 Tel. (787) 748-1595 President Mateo Labov

> Looking for a Fax Number?

Get It fast in the Fax Section

The Business Register. where business

▲ PUERTO RICO CONTAINER

CORP P 0 Box 3587 San Juan, PR 00936 Tel. (787) 785-8080 General Manager Tomas Davis Manufacturing of Corrugated

003229 Pressed and Blown Glass and Glassware, n.e.c.

▲WARNER LAMBERT INC

P O Box 786 Vega Baja, PR 00694 Tel. (787) 858-2323 President Robert Janosky

▲TU FARMACIA Y MÁS

Tel. (787) 852-0785

Manuel Mediavilla Jr.

Owner

Pharmacy

P O Box 638 Humação, PR 00792

Pharmaceutical Products Manufacturer

ZENITH LABORATORIES CARIBE INC



ASTERLING PRODUCTS

INTERNATIONAL INC

Sales. Marketing & Distribution of

ASTRYKER PUERTO RICO

goad 3 Km 130.2 Arroyo. PR 00714

PO Box 329 Arroyo, PR 00714

Sales Volume: \$5M Plus - \$10M

Employment Bracket: 451 - 500

Syntex Humacan Operations

p 0. Box 364567 San Juan.

consumer Health Products

PR 00936-4567

General Manager

Anthony Leber

Tel. (787) 758-0985

Tel. (787) 839-7688

Fax (787) 839-0282

Francis Pagán

Medical Devices

Senior Facilities Engineer

SYNTEX (F P) INC

HC-01 Box 16625 Humacao.

Bo Mariana Road 909 Km 1.1

Pharmaceutical Products Manufacturer

PR 00791-9731

Humacao. PR 00791

Tel. (787) 852-0909

Tel. (787) 852-0919

Tel. (787) 852-0219

Fax (787) 852-9641

Parent/Affiliates/Branches

• Hoffman - La Roche; LTD 340 Kingsland Street 07110

268 Muñoz Rivera Ave. Suite 1005

• Syntex Puerto Rico Inc

Hato Rev PR 00918

ATHE UPJOHN

Tel. (787) 846-4900

Redgy L. Coucke

PR 00617

MANUFACTURING CO

Gen. Manager (Manufacturing)

Pharmaceutical Manufacturers

La Cruz Azul de Puerto Rico, Inc.

LA NUEVA CRUZ AZUL

Un Concesionario Independiente de

la Blue Cross and Blue Shield Association.

PO Box 11307 Barceloneta,

General Manager

Frankie Santana

P 0 Box 11979 Cidra, PR 00739 Cidra Ind'I Park Calle A Lote 8 Cidra. PR 00739 Tel. (787) 739-8421 Fax (787) 739-4321

Fax (787) 739-9405 VP-General Manager Nelson R. Rodríguez Finance Director

Jesús R. Santiago Human Resources Manager Ruth Camacho

Generic Drug Manufacturing

•IVAX Corporation



▲ZENITH LABORATORIES CARIBE INC

Tel. (787) 739-8421 Fax (787) 739-4321 VP-General Manager Nelson R. Rodríguez Generic Drug Manufacturing Employment Bracket: 150-200

an internet address?

Get it fast in

the Internet Section.

OWENS-ILLINOIS DE

PUERTO RICO P 0 Box 387 Vega Alta, PR 00692 Bo. Sabana Hoyos Rd. 690 Km. 1.1 Vega Alta, PR 00692 Tel. (787) 883-5800 Tel. (787) 882-5710 Tel. (787) 725-5800 Fax (787) 883-1177

General Manager Dee J. Hillberry Administrative Manager Luis A. Pagán

Sales Manager Cayo Boada Materials Manager

Salvador Muriel Human Resources Manager Héctor Negrón Production Manager David Rosa

> Quality & Assurance Manager Félix Román

> Glass Containers Manufacturers **Products & Services**

Glass Containers Trademarks & Brandnames Sales Volume: \$10M Plus - \$50M

PLASTIC & MILLS

Converted Paper and

ALIANCA FOLDING BOX INC

P 0 Box 5068 Carolina, PR 00984

Calle Varcacel Carolina, PR 00979

Fomento Bldg. Sabana Abajo

Tel. (787) 750-1810

Fax (787) 757-8045

Antonio Castillo González

Folding Box Manufacturing

President

Cardhoard

PRODUCTS

Paperboard

Products, n.e.c.

002649

Employment Bracket: 301 - 350

Parent/Affiliates/Branches

8800 Northwest 36th St. Miami 33178-2404

Employment Bracket: 150-200

P O Box 11979 Cidra, PR 00739 Cidra Ind'l Park Cidra, PR 00739

Looking for

www.pbrp.com.

Napkins Manufacturers

finds business

an our internet site

Contact us

SANOFI PHARMACEUTICAL INC p 0 Box 70322 San Juan, pR 00936–8322

Edif Royal Bank Ste 285 Hato Rev.

PR 00917

Tel. (787) 758–1033
Fax (787) 753–1263
General Manager
José Méndez
Distribution of Pharmaceutical
Products.
Sales Volume: \$10M Plus – \$50M
Employment Bracket: 26 – 50

AUPJOHN INTER-AMERICAN CORP

Area Indl Higuillar Pueblo Viejo, PR 00920 Tel. (787) 792-6667 Medicinal & Botanical Products

WYETH - AYERST LABORATORIES (PR) INC

P 0 Box 362917 San Juan, PR 00936–2917 Tel. (787) 782–3838 Pharmaceutical Product Distributors

003851 ____ Ophthalmic Goods

ACENTROVISION - CLINICA DE OPTOMETRIA

PO Box 2825 Hato Rey, PR 00919
Id. (787) 764-4848
Owner
Histor Alfonso
Oplometry Clinic

ACLINICA VISUAL MORALES IVETTE DRA & ASSOC

^{†0} Box 34210 San Juan, PR 00926 M. (787) 758–2275 Mometrist

AESSILOR INDUSTRIES

Monetas Ind Park, Mercedita Ponce, 78 00715 (8 (787) 848–4130 (Mance & Administrator Vice–Pres.)
Meida Irizarry (Manufacturer)

AMENTOR CARIBE

O. Box 1358 El Jibaro Ind'I. Park da PR 00739 d (787) 739–8418 an Manager Juel Soler Geocular Lens Manufacturer

(The Business Register, where business finds business.

▲ OCULAR SCIENCES PUERTO RICO INC

P O Box 2801 Santa Isabel.
PR 00757
Repto Ind. La Playa Rd. 538
Santa Isabel. PR 00757
Tel. (787) 845–2113
Fax (787) 845–3236
Manager
Fernando Vázquez
Manufacturers & Distributors of Contact Lens
Sales Volume: S5M Plus – \$10M
Employment Bracket: 450

▲OPTI-FACTORY

El Centro Bldg. Marginal 14–B M. Rivera Ave Hato Rey. PR 00918 Tel. (787) 758–7878 Vice–President Luis C. Colón Optical Lab and Vision Center. Optometry Services. Sale and Repair of Eye Glasses and Security Lenses.

▲ PEARLE VISION CENTER OF PRINC

1122 Ponce de Leon Río Piedras, PR 00925 Tel. (787) 765-0088 Managing Director Caribbean Donald Johndrow Vision Test. Contact Lenses. Frames and other Ophthalmic Goods

▲ PROFESSIONAL OPTICAL SERVICES INC

P. O. Box 2636 Bayamon Sta Bayamón, PR 00960-2636 Tel. (787) 785-1862 Owner Anthony Mark Lens Manufacturers. Open Monday to Friday from 8:00 AM to 4:00 PM

▲SOUTHERN OPTICAL COMPANY

Sunny Isle Professional Bldg. St Croix, USVI 00820 Tel. (340) 778–6565 Manager Margaret Rennie Eye Glasses. Contact Lenses and everything for the Eyes.

002834 ____ Pharmaceutical Preparations

A J BART
P. O. Box 1360 Gurabo, PR 00778
Tel. (787) 737–8445
Owner
Alberto S. Baltolomei
Distributors of Pharmaceutical

Products.

▲ABBOTT PUERTO RICO OPERATIONS

P 0 Box 278 Barceloneta, PR 00617 Tel. (787) 846–6900 VP. Gen. Mgr. Abbott P R Operation José L. Rodríguez Manufacturers of Health Care Products

ACCUPHARMA RESEARCH AND SCIENTIFIC CONSULTING INC P 0 Box 1340 Gurabo.

PR 00778–1340
Tel. (787) 850–4215
President
José F Colón Reyes
Generic Medicaments. Research &
Development. Microbiology
Pharmaceutical Test. Sample Testings.

ALCON (PUERTO RICO) INC P. O. Box 3000 Humacao, PR 00792

Tel. (787) 852–3080 General Manager Milton Barley Pharmaceutical Products Manufacturer

▲ALLERGAN AMERICA

P. O. Box 60 Hormigueros, PR 00660 Tel. (787) 849-3895 General Manager José Luis Diaz Pharmaceutical Preparations Manufacturer

AMGEN MANUFACTURING INC



P O Box 4060 Juncos,
PR 00777-4060
Road 31 Km. 24.6 Juncos, PR 00777
Tel. (787) 734-2000
Tel. (787) 731-2000
Fax (787) 734-6161
Director/Gen Manager
James Sanabria
Operations Manager
Miguel Nazario
Plant Controller
Jaime Arraya
Manager Human Resources
Axel Lluch
Biotechmology

▲AYERST-WYETH PHARMACEUTICALS INC

P. O. Box 10001 Guayama, PR 00785 Tel (787) 864-4010 Vice-President & General Manager Mariano Martinez Mora Pharmaceutical Products Manufacturer

-BASE PHARMACEUTICALS

BASF Pharmaceuticals A Unit of BASF

P O Box 795 Jayuya, PR 00664-0795 Road 144 Km 2.6 Jayuya, PR 00661 Tel. (787) 828-0990 Fax (787) 828-6440 Vice President & General Manager Carlos R León Buyer Victor Arcelay

Pharmaceutical Products Manufacture
Parent/Affiliates/Branches

BASE Pharmaceuticals

New Jersey
Employment Bracket: 101 – 150



The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

MAXTER CARIBE INC

Baxter

n Box 1290 Guayama, R 00785-1290 anule 3 Km 142.5 Guayama, 22 00784 [el. (787) 864-5050 fax (787) 866-2714 eneral Manager and Ghigliotty P.E. unerial Director alor M. Guzman, Esq. Unutacturing of Anesthetics amaceutical Products Division Pagent/Affiliates/Branches 180 C Health Care Inc U07938 mducts & Services saflurane USP, Enflurane USP. Mhoxyflurane, Deflurane USP Indemarks & Brandnames inrane, Forane, Suprane iles Volume: 150-200 Employment Bracket: 101 - 150







ABAXTER HEALTH CARE CORP OF PR 10 Box 518 Jayuya, PR 00664 1 (787) 828-3700 Rent Manager ladio Alvarez benterals Solutions and Medical

MOTECH GROUP FENWAL MOISIN



Box 832 Maricao, PR 00606 1357 Km 0.8 Maricao, PR 00606 (787) 838-3000 (787) 838-2110 man Resources Manager Je Lugo Manager Manager amin Padilla Director (Fenyval del Caribe) Van Heems Manager sse Betancourt maceutical Products Manufacturer. littles to Collect. Store and

Muster Blood and its Components

Parent/Affiliates/Branches · Baxter Healthcare Corp.

Chicago, Deerfield ILL 00615 Products & Services Systems for the Collection. Separation, Preservation, Manipulation, and Transfusion of Blood and Blood Components. Trademarks & Brandnames

Fenwal, Baxter



▲ BIOTECH GROUP FENWAL DIVISION

P 0 Box 832 Maricao, PR 00606 Rd. 357 Km 0.8 Maricao, PR 00606 Tel. (787) 838-3000 Fax (787) 838-2110 Human Resources Manager Angie Lugo Pharmaceutical Products Manufacturer, Products to Collect, Store and Administer Blood and its Components.

▲ BIOVAIL LABORATORIES INC

P O Box 3468 Carolina, PR 00984-3468 Sabana Abaio Ind'I Park 34 Calle B Iturregui Ave Carolina, PR 00983 Tel. (787) 750-5350 Fax (787) 750-5360 General Manager Carmen M Reyes Reyes Manufacturing Research & Development Employment Bracket: 51-103

BRISTOL LABORATORIES CORPORATION BRISTOL CARIBBEAN INC



Bristol Laboratories 2 Corporation Bristol Caribbean, Inc. Mayaguez Operations

P O Box 897 Mayaguez, PR 00681 Trade Zone 7 Rd. 114 Foreign Mayaguez, PR 00680 Tel. (787) 834-0185 Fax (787) 834-4182 Vice-President & General Manager Theodore Iliopoulos Human Resources Director Rosa Beatriz Sanabria Oncologic Business Unit Leader Jean F Schneider Liquid & Question Business Unit Leader Javier Santana Comptroller Edgardo Gratacós CPA Materials Control Director Javier Santana Director of Engineering José M Maldonado

Engages in the Production of Non-Beta Lactam Oral Dosage Pharmaceutical Products and Oncological Drugs.

Parent/Affiliates/Branches

· Bristol-Myers Squibb Company 345 Park Ave. New York NY 10154 Products & Services Analgesic & Anti-Cancer Trademarks & Brandnames Bristol-Myers Squibb Co



▲ BRISTOL LABORATORIES CORPORATION BRISTOL CARIBBEAN INC

P O Box 897 Mayaquez, PR 00681 Trade Zone 7 Rd. 114 Foreign Mayaguez, PR 00680 Tel. (787) 834-0185 Fax (787) 265-4111 Vice-President & General Manager Theodore Iliopoulos Engages in the Production of Non-Beta Lactam Oral Dosage Pharmaceutical Products and Oncological Drugs

BRISTOL-MYERS BARCELONETA INC



BRISTOL-MYERS BARCELONFTA, INC.

P O Box 657 Barceloneta, PR 00617 Rd. 2 Km. 56.4 Barceloneta PR 00617

Tel. (787) 846-3800 Fax (787) 846-7845 Administrative Assistant

Elizabeth Padılla Antibiotic Manufacturer Parent/Affiliates/Branches Bristol Myers Squibb Company 345 Park Ave. New York

NY 10154-0037 **Products & Services**

Amoxicillin Manufacturer for the Local and International Market

Trademarks & Brandnames

1

Polycillin, Buspar, Polymox, Beta Pen, Dicloxcil, Prostaphlin, Duricef. Naful, Staphcillin, Dyna Pen, Ultraceph. Pen V, Prostaphlin, Duricef, Naful, Staphcillin, Dyna Penn. Ultraceph, Pen V Sales Volume. Over \$50M Employment Bracket, 600 Plus





▲CHIRON BETA CORPORATION

P O Box 1624 Canóvanas, PR 00729 Tel. (787) 876-1400 Secretary Administrative Marta Ortiz Pharmaceutical Products

▲COCHARON WHOLESALE P O Box 8567 Humacao, PR 00792 Tel. (787) 852-4325 Manager Rafael Mangual

▲COLON DE JIMÉNEZ ANA L P 0 Box 22678 U P R Sta

San Juan, PR 00931 Tel. (787) 763-1454 Owner Ana Colón Dermatologist

Pharmaceutical Preparations

▲ DADE DIAGNOSTIC OF PR INC

P 0 Box 865 Aguada, PR 00602 Tel. (787) 868-5500 Manufacturing Manager Randy Howe Manufacturing of Reagents and Laboratory Controls

▲ DANBURY PHARMACAL P.R. INC.

Road 3 Km. 76.9 Humacao Ind'I. Park Humacao, PR 00792 Tel. (787) 852-5151 Fax (787) 852-5974 General Manager Blanca Meléndez Pharmaceutical Manufacturing Sales Volume: \$5M Plus - \$10M Employment Bracket: 151 - 200

P 0 Box 886 Humacao, PR 00792

▲ DEL MAR PHARMACY SERVICE INC

P O Box 233 Mercedita Ponce. PR 00715-0043 Tel. (787) 842-6263 Pharmaceuticals & Related Products Distribution

▲ DENVER CHEMICAL (PR) INC

HC-04 Box 4012 Humacao, PR 00791-9502 Tel. (787) 852-3240 Manufacturing Manager Juan R. Suarez Pharmaceutical Products Manufacturer

It pays to register

in the Business Register

ADORASOL LABORATORIES _{p0} 3906 San Juan, PR 00936 Tel. (787) 753-6549 Agustín Rodríguez Kissell Manufacturers of Pharmaceutical products

ADROGUERIA GONZÁLEZ INC PO Box 350 Ponce, PR 00733 rel (787) 724-1078 pharmaceutical Preparations

ADROGUERIA RIO PIEDRAS 590 De Diego Ave. Río Piedras, PR 00924 Tel. (787) 751-5030 president Raúl González Wholesale and Distribution of Medicines.

ADUPONT MERCK PHARMA PO Box 301000 Manati. PR 00674-3000 Tel. (787) 854-1030 President William Henández Pharmaceutical Products

AEATON L'ABORATORIES PO Box 1055 Manatí, PR 00674 Tel. (787) 854-1520 Vice-President General Manager Ramón Sepulveda Pharmaceutical Products Manufacturer

AENGRAPH LEHIGH PRESS PUERTO RICO

P 0 Box 1469 Juncos, PR 00777 Mamey Ind'l Center Road 189 Km 12.4 Juncos, PR 00777 Tel. (787) 734-1000 fax (787) 734-1004 President Luis Herrera Insert and Outsert for Pharmaceutical Industries Office Hours. Mon - Fri from 8:00 AM to 5:00 PM Sales Volume: \$5M Plus - \$10M Employment Bracket: 101 – 150

▲ENVIRONMENT PRO-TEK

P O Box 38053 Airport Station San Juan, PR 00937-1053 Tel. (787) 749-9534 Consultant René Santiago Air & Water Purificator, Oxygen Generator. Sediment Remover. Biodegtable Products. Insulation For

Looking for a Fax number? Get it fast in the Fax Section.

▲ FX-LAX INC H.C. - 01 Box 16629 Humacao. PR 00791-9731 Tel. (787) 852-3190 Executive Vice Pres. & General Mgr Santos Troche Laxative and Antiflatulex Manufacturers

▲FAULDING PUERTO RICO INC

P O Box 250471 Ramey Branch Aguadilla. PR 00604-0471 Tel. (787) 890-3000 General Manager Juan Miguel Gomez Pharmaceutical Products

▲ GENERICS OF PUERTO RICO INC

P O Box 11533 Fdez Juncos Sta Santurce, PR 00910 Monte Rey Urb. 3 Calle Acacia Pueblo Viejo, PR 00920 Tel. (787) 792-2430 Fax (787) 782-0990 President Carlos A. Fraga Pharmaceutical Products Distributors Sales Volume: \$1M Plus - \$5M Employment Bracket: 26 - 50

▲GLAXO WELCOME

▲ HOECHST MARION INC

P O Box 2120 San Juan PR 00922-2120 Tel. (787) 782-1900 General Manager Francisco Nordelo Pharmaceutical Products

JANSSEN PRODUCTS

HC - 02 Box 19250 Gurabo. PR 00778-9629 Bo. Mamey II Road 933 Km. 0.1 Gurabo, PR 00778-9250 Tel. (787) 789-5000 Fax (787) 272-7644 Fax (787) 272-7602 VP Manufacturing & General Manager William B Nelson

Director of Logistic & Materials Mgnt Margarita Hernández Finance Director Tony Perez Human Resource Manager Fernando Plaud OA'QC Director Eric Olivieri Director of Engineering Maintenance/Environmental & Safety Nallagounder Kuppusamy Pharmaceutical Products Parent/Affiliates/Branches

 Johnson & Johnson Corporate Worldwide Headquarters One Johnson & Johnson Plaza New Brunswick NJ 08933

 Janssen Pharmaceutical 1125 Harbourton Road Titusville NJ 08560-0200

▲ JANSSEN PRODUCTS

Bo. Mamey II Road 933 Km. 0.1

HC - 02 Box 19250 Gurabo.

Gurabo, PR 00778-9250

Pharmaceutical Products

Sales Volume: Over \$50M Employment Bracket: 401 – 450

▲ LEDERLE PARENTERALS

P O Box A C Pueblo Sta. Carolina.

65 Infantry Ave. Km. 9.7 Carolina,

Tel. (787) 789-5000

Fax (787) 272-7644

VP. Manufacturing

Tomás Ramírez

INC

PR 00979

PR 00984-4904

Tel. (787) 752-7474

President & Gen. Manager

Pharmaceutical Products

▲LIFESCAN (PR) INC

Cabo Rojo, PR 00623

Tel. (787) 255-7700

Fax (787) 255-7713

Reagent Strips for Glucose

from 8:00 AM - 5:00 PM

Finance Manager

Max Roldán

P 0 Box 5001 Cabo Rojo, PR 00623

Monitoring Open Monday to Friday

Employment Bracket: 251 - 300

Bo Pedernales Road 308 Km 0.8

Sales Volume: \$5M Plus - \$10M Employment Bracket: 500 Plus

Fax (787) 762-3395

Alfredo R Nadal

PR 00778-9629

Products & Services Propulsid, Prisperdal, Sporanox,

Nizoral, Vermox, Hismanal Sales Volume: Over \$50M Employment Bracket: 401 - 450

P 0 Box 363461 San Juan, PR 00936-3461 Tel. (787) 250-7580 Finance Director Luis Cintrón Pharmaceuticals Wholesaler

ROUSSEL PUERTO RICO

JANSSEN ORTHO LLC

LILLY DEL CARIBE INC.

P O Box 1198 Carolina. PR 00986-1198 P.R. Ind'l Park Km 12.6 65th Inf Ave. Carolina, PR 00985 Tel. (787) 257-5555 Tel. (787) 257-5333 Fax (787) 257-5544 Fax (787) 257-5988 President & General Manager Paul Ahern Director Human Resources Iliana Rivera Director Quality Control Evelyn Rodriguez Manufacturer of Pharmaceutical Products Sales Volume: \$5M Plus - \$10M Employment Bracket: 500 Plus

The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

IICAS - INSERTCO



ngox 377 San Germán, PR 00683 Relifo Indl Park Rd. 102 Km 33.2 street San Germán, PR 00683 (787) 892-1268

(787) 892-4112 Salzano Manager Manager

om Ufret

aduction Coordinator

Cruz Manager

Myred Centeno archasing Agents

unida Mora Momer Service

and Morales wount Executive

Sevilla gits, Outserts & Labels for wmaceutical and Electronic stries, Starch Displacement & wess Pharmaceutical Preparation. S Volume: \$5M Plus - \$10M cloyment Bracket: 90 - 100



MARION & COMPANY 180x 3009 Manati, PR 00674 1(787) 854-3005 lenal Manager aasio Rivera maceutical Products

MCGAW OF PUERTO RICO

Box 729 Sabana Grande, (787) 873-4600 leral Manager

Ranfit deal Devices Manufacturing

Looking for

an internet address?

Get it fast

In the internet Section.

MCNEIL CONSUMER PRODUCTS A DIV OF J & J CONSUMER CO PRINC



Las Piedras, PR 00771 Tel. (787) 733-1000 Tel. (787) 782-7030 Fax (787) 733-6616 General Manager Edgardo J. Fabregas Over the Counter Propietary Products Parent/Affiliates/Branches • McNeil Consumer Products Inc. Camp Hill Road 19034 Trademarks & Brandnames Tylenol Employment Bracket: 351 - 400

P O Box 2009 Las Piedras,

Bo. Montones Road 183 Km 19.8

PR 00771-2009



▲ MCNEIL PHARMACEUTICAL A DIV OF OMJ PHARMACEUTICAL INC

P. O. Box 710 Dorado, PR 00646-0710 Tel. (787) 796-1540 General Manager Krenly Cruz Manufacturer of Capsules, Tablets, Caplets and Liquid of Ethical Pharmaceutical Products

▲ MEDISEARCH P R INC

P O Box 2460 Guayama. PR 00785-2460 Tel. (787) 864-0684 President John K. Whitney Manufacturer of Therapeutic Pads. Heat Therapy Pads, Pressure Ulcer Relief. Thrombo Cuff.

MERCK SHARP & DOHME QUIMICA DE P B INC ARECIBO OPERATIONS



MERCK SHARP & DOHME

P O Box 1011 Sabana Hoyos Barceloneta, PR 00688 Road 2 Km. 60.3 Sabana Hoyos. PR 00688 Tel. (787) 846-1600

Director of PR Operations Richard S. Bowles Senior Director Mfg Services Luis Couto General Manager Iván Lugo Director of Public Affairs Rafael Robert Purchasing Manager PR Operations Luis Archilla

Fax (787) 846-5580

Financial Director Carlos Gómez IS Operation Head for PR. Luis E. Ortiz

Pharmaceutical Manufacturing Parent/Affiliates/Branches

 Merck and Company Inc. Whitehouse Station NY

• MSD Quimica de PR. Caguas Operations

Caguas PR 00725 • MSD Quimica de PR Barceloneta Operations

P O Box 601 Barceloneta PR 00617 Trademarks & Brandnames Prilosec, Fosamax, Proscar Sales Volume: Over \$50M

Employment Bracket: 500 Plus



P O Box 8639 Caguas, PR 00726 Villa Blanca Ind'l Park Rd 1 Km 34.1 Caguas, PR 00726 Tel. (787) 746-8500 Fax (787) 743-7669 President & CEO Joaquín Viso Pharmaceutical Products Employment Bracket: 500 Plus

▲ NESSAN LABORATORIES INC

P. O. Box 1941 Carolina, PR 00984 Tel. (787) 769-5053 President Nellie E. Sanchez Pharmaceutical Products

O M J PHARMACEUTICAL INC

OMJ Pharmaceuticals, Inc.

P O Box 367 San German, PR 00683 Rd. 362 Km. 0.5 San Germán, PR 00683 Tel. (787) 892-2245 Fax (787) 892-2095 General Manager Felix Morales Lye Care Products Manufacturers

Parent/Affiliates/Branches

Ortho Biotech Inc. U.S. Route 202 P O Box 670 Raritan 00869-0602 Products & Services Ophthalmics Products, Medical Devices Employment Bracket: 201 - 250

▲ ORTHO PHARMACEUTICAL/A DIV OF J & J PHARM CO (PR) INC

P. O. Box 463 Manatí, PR 00674 Tel. (787) 854-1800 General Manager Krenly Cruz Contraceptives and Semi-Solids.

▲ P C R DE PUERTO RICO INC

P O Box 960 Punta Santiago PR 00741 Road 3 Km. 76.9 Humacao, PR 00791 Tel. (787) 852-4520 Fax (787) 852-4284 Plant Manager Santiago Hernández Reves Organic Chemicals for Cancer Treatment Employment Bracket: 0 - 25

The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

Pharmaceutical and Health Care Industries. Parent/Affiliates/Branches • Paco Pharmaceutical Services Inc New Jersey NJ Employment Bracket: 100-225

complete Manufacturing and

Packaging Services for the

PACO PUERTO RICO INC

PO Box 1661 Canóvanas, PR 00729

san Isidro Ind Park Road 188 Km

n5 Canóvanas, PR 00729

Human Resources Manager

Tel. (787) 876-6362

Tel. (787) 876-6258

Fax (787) 876-0165

Fax (787) 876-5099

Plant Manager

Rubén Aguayo

Frances Guzmán

Finance Director

Brian Fichthorn

Miguel Parada Material Manager

Antonio Rivera

Account Executive

PFIZER PHARMACEUTICALS



PO Box 628 Barceloneta, PR 00617 Cruce Dávila Rd. 2 Km 58.2 Barceloneta, PR 00617 Tel. (787) 846-4300 Fax (787) 846-7022 Fax (787) 846-5077 General Manager Anthony Maddaluna Director, H R and Public Affairs Héctor Corretier Pharmaceutical Products Manufacturing. Parent/Affiliates/Branches •Pfizer Inc 235 E. 42 St. New York City NY 10017 Trademarks & Brandnames Feldene, Procardia, Procardia XL, Glucotrol, Diflucan, Antivert / Bonine,

Employment Bracket: 1000 Plus

Minipress / Minizide, Sinequan,

Zythromax. Cardura, Zoloft

Sales Volume: Over \$50M

It pays to register ⁱⁿ the Business Register **▲**PROCTER & GAMBLE PHARMACEUTICAL PUERTO RICO INC

P O Box 1055 Manatí, PR 00674 Tel. (787) 854-1520 Vice Pres. & Gen. Manager Ramón Sepúlveda Pharmaceutical Products Manufacturer

REEDCO & DENTCO INC



Faulding Puerto Rico, Inc.

H C - 04 Box 4013 Humacao. PR 00791 Humacao Ind'l Park Rd 3 Km 76.4 Humacao, PR 00791 Tel. (787) 852-3400 Tel. (787) 724-6756 Fax (787) 850-2300 Fax (787) 852-7870 General Manager Luis R. Acevedo Production Manager Lizzette Pérez Quality Service Manager Reynaldo Velázquez Maintenance Facility Manager Victor Marrero Traffic & Warehouse Manager Angel Rodríguez Human Resources Manager Mildred Sein Administration Manager Eduardo Clemente Plant Engineer & Regulatory Affairs Ivan Santiago Inventory Control Manager Juan C Aponte Traffic Supervisor Miguel A. López Pharmaceutical Products Manufacturer Parent/Affiliates/Branches • Block Drug Co Inc 257 Cornelison Ave NJ 07302 Products & Services Dental Product. Shampoo's, Pharmaceutical, Dermatologic



Trademarks & Brandnames

Balmex, Durascreen

Tegrin, Sensodyne-F, Poligrip, Super

Poligrip. Dentu-Creme, Sensodyne, R

& C, B C Tablet, Nytol, Tegrin L T.

Sales Volume: \$5M Plus - \$10M

▲ REEDCO & DENTCO INC

H C - 04 Box 4013 Humacao. PR 00791 Humacao Ind'l. Park Rd. 3 Km. 76.4 Humacao. PR 00791 Tel. (787) 852-3400

Fax (787) 850 2300 General Manager Luis R. Acevedo Pharmaceutical Products Manufacturer Sales Volume: \$5M Plus - \$10M Employment Bracket: 301 - 350

RHONE-POULENC RORER CARIBBEAN

Rhone-Poulenc Rorer Caribbean



P O Box 364824 San Juan. PR 00936-4824 De La Cruz Plaza Suite 100 Metro Office Park Guavnabo, 00968-1705 Tel. (787) 783-6868 Fax (787) 783-4845 Fax (787) 783-4346 Finance Director Angel B. Méndez General Manager & Vice President Isidro J Ferrer Marketing & Sales Director Nelson De Jesus Sales Director Ana L Del Rio Sales & Marketing of Pharmaceutical Preparations Products & Services Lozol, Tussar, SLO-BID, Nasacort, Asmacort, Dilacox, Calcimar, DDAVP. Penetrex, Nitrolingual Zagam Trademarks & Brandnames Sales Volume: \$5M Plus - \$10M Employment Bracket: 51 - 100



RHONE POULENC RORER PR

INC P O Box 345 Manati, PR 00674-0345 604 Road Bo San José Manatí PR 00674 Tel. (787) 854-1058 Fax (787) 854-3100 VP & General Manager Carlos Santiago Comptroller Jaime L. Sanabria Operations Director Franco Negrón Human Resource Director Victor Osuna Quality Control Director Jorge Cotto

Materials Management Director

Pharmaceutical Preparations

Manufacturer of Tablets, Capsules,

Creams & Inhaled Therapy Products.

Dolores Fernández

Project Engineer

José R. Osorio

Parent/Affiliates/Branches •Rhone Poulenc Rorer Inc. 500 Arcola Rd. P O Box 1200

Collegeville 19426-0107 • Rhone Poulenc Rorer Caribbean Corp

De La Cruz Plaza S-100 Metro Office Park Guaynabo PR 00968-1705

Products & Services Trademarks & Brandnames

Nasacort, Lozol, Azmacort, Slo-bid. Hygroton, Vytone. Benzamycin. Benzagel, Sulfacet, Rilutek, Nicobid. Hytone. Penetrex, Masacort AQ Employment Bracket: 351 - 400





RIMACO INC

P O Box 8895 Fdez. Juncos Station Santurce, PR 00910 Villa Caparra Ext. Calle Marginal Buchanan Guaynabo, PR 00966 Tel. (787) 792-9512 Fax (787) 782-8310 President Ricardo Mayo Alvarez Marketing Manager Daniel Torres Torres Treasurer/Vice President Ricardo Mayo Alvarez Jr. **Executive Secretary** Ramona Orozco Pharmaceutical Products Distributor. Sales Volume: \$5M Plus - \$10M Employment Bracket: 0 - 25

▲SANOFI PHARMACEUTICAL INC

P O Box 70322 San Juan, PR 00936-8322 Tel. (787) 758-1033 General Manager José Méndez Distribution of Pharmaceutical Products.

Contact us

at our internet site

www.pbrb.com.

HERING-PLOUGH ONLICTS INC



1779 Las Piedras. aco Ind'l Park Rd 183 Predias. PR 00771 (187) 733-2323 (187) 783-3333 (1787) 733-3229 (m(187) 733-2333 eiai Manager Rodriguez and Director ao Ciena aptroller and Santiago nun Resources Manager .kse Cordoves senals Director an Aldarondo aneering Manager nes Kregloh My Control Director ando Santiago wmaceutical Manufacturer of Bulk inished Dosage Form, Specializing Sustained Release Technologies Muct Manufacturing Services

hent/Affiliates/Branches mering Plough Corporation

Gralda Farms P O Box 1000 Mison NJ 07940-1000

aducts & Services

antin, Unidur, Normodyne, Theo-Dur iels, K-Dur Tablet... Eulexin

Volume: \$5M Fais - \$10M ployment Bracket 51 - 300



ISCHMID PRODUCTS CORP 0-04 Box 4016 Human ao. 800791-9502 1(787) 852-2476 sident & General formager dio A. Marrero Indoms for Natural ling and asitivity Manufacto s

ISEARLE CARIBBEAN Box 367189 San Juan.

00936-7189 (787) 258-6474 ector

no Grieco lmaceutical and Consumer Jucts Sales and Distribution SEARLE, LTD



MONSANTO 3 Food · Health · Hope

P 0 Box 11247 Barceloneta, PR 00617-1247 Rd 140 Km 64.4 Barceloneta, PR 00617 Tel. (787) 846-5000 Fax (787) 846-6595 Fax (787) 846-2640 General Manager

Hector Jové Comptroller Iván Marcano Quality Control Director Rosaura Ortíz Materials Director Vivian Molinari Human Resource Director José L. Narváez Engineering Director Felipe Sánchez Pharmaceutical Products

Nycomed Products (Omnipaque): Picker International del Caribe Inc. Trademarks & Brandnames Visipaque, Omniscan, Omnipaque, And

Third Party Manufacturing Employment Bracket: 500 Plus

Manufacturing. Exclusive Distributor of





▲ SEIN MÉNDEZ LABORATORIES INC

P O Box 10757 San Juan. PR 00922-0757 Tel. (787) 793-2700 General Manager Francisco Santos Manufacturer & Distributors of Pharmaceutical O T C Products

SMITHKLINE BEECHAM INTERAMERICAN CORPORATION



P O Box 2160 San Juan. PR 00922-2160 Calle Diana #29 Amelia Ind'i Park Guaynabo, PR 00922 Tel. (787) 774-8000 Fax (787) 774-0302 General Manager José Vargas

Finance Manager Armando Rodriguez Sales of Ethical Products Trademarks & Brandnames S B-I A C Puerto Rico Sales Volume: \$10M Plus - \$50M Employment Bracket: 51 - 100

SMITHKLINE BEECHAM

PHARMACEUTICALS



Fax (787) 842-0313 Owner José Rivera Manufacturing & Sale of OTC Products, Veterinary Products and Private Labels. Sales Volume: \$0 - \$500K Employment Bracket: 0 - 25

SQUIBB MANUFACTURING INC

P O Box 609 Humacao, PR 00792

Road 3 Km. 77.5 Humacao,

Human Resources Site Leader

Director of Quality Control

Director of Manufacturing

Director of Maintenance

Parent/Affiliates/Branches

345 Park Avenue 10154

Chemical Products Manufacturers

· Bristol Myers Squibb Company

Sales Volume: \$5M Plus - \$10M

Employment Bracket: 500 Plus

Tel. (787) 852-1255

Fax (787) 852-3800

Francisco Gutierrez

Financial Site Leader

Tina Fiumenero

Luis O. Rodriguez

Bernie Morales

Israel Díaz

Grisel Castro

VP & General Manager

PR 00791

palat kandida ka a B. i

SmithKline Beecham Pharmaceuticals

P 0 Box 11975 Cidra. PR 00739-1975 Bo. Certenejas Rd 172 Km 9.1 Cidra. PR 00739 Tel. (787) 766-4000 Tel. (787) 739-8401 Fax (787) 250-3710 President-General Manager José Luis Rosado Vice-President Finance Raul Cermeño **Business Development Director** Joan Cruz Pharmaceutic Manufacturing Director Betsy Rodriguez Vice-President Human Resources Sonia Berrios Vice Pres. Public Relations Jorge González VP Quality Assurance Adalberto Ramirez Enginering Director

Ismael Guzmán

Pharmaceutical Products

· Smithkline Beecham

Parent/Affiliates/Branches

Smithkline Interamerican

P O Box 2160 San Juan

PR 00922-2160

Brand

.Paxil

S B House Great West Road London

Smithkline Beecham Consumer

P 0 Box 9597 Hato Rey PR 00919

Tagamet, Ecotrin, Feosol, Stelazine,

Relafen, Dyazide, Bactroban, Compazin

Trademarks & Brandnames

Sales Volume: Over \$50M



▲ SQUIBB MANUFACTURING

INC P 0 Box 609 Humacao, PR 00792 Road 3 Km. 77.5 Humacao, PR 00791 Tel. (787) 852-1255 Fax (787) 852-3800 General Manager Francisco Gutierrez Chemical Products Manufacturers Sales Volume: \$5M Plus - \$10M

Employment Bracket: 500 Plus



▲ SPECIALTIES CHEMICAL DBA PONCE PHARMA

P O Box 277 Playa Sta. Ponce. PR 00731 Playa Ponce 46 Calle Mirasol Ponce. PR 00731 Tel (787) 842-0313

Looking for

an internet address?

Get it fast in

the Internet Section.

SONOCO P O Box 399 Yabucoa, PR 00767 Tel. (787) 893-2675 Tel. (787) 893-2600 Fax (787) 893-2200 General Manager José Zayas

Plant Superintendent Octavio Divison Sales Representative Jackie Rosado Paper Products & Fiber Composite Cans and Spiral Tubes

Parent/Affiliates/Branches

· Sonoco Products Co Hartsville SC

Trademarks & Brandnames Sonotubes, Sonovoids, Sonomolds









▲SUNRISE PAPER CORP P O Box 9702 Carolina. PR 00988-9702 Tel. (787) 748-1595 President Mateo Laboy

Napkins Manufacturers

Looking for a

Fax Number? Get It fast in the

Fax Section

The Business Register where business

finds business

Contact us an our internet site www.pbrp.com.

▲TU FARMACIA Y MÁS

ASTERLING PRODUCTS

INTERNATIONAL INC.

sales. Marketing & Distribution of consumer Health Products

ASTRYKER PUERTO RICO

goad 3 Km 130.2 Arroyo, PR 00714

P 0 Box 329 Arroyo, PR 00714

sales Volume: \$5M Plus - \$10M

Employment Bracket: 451 - 500

Syntex Humacan Operations

A Proto Group Compan.

ρ O. Box 364567 San Juan.

PR 00936-4567

General Manager

Anthony Leber

Tel (787) 758-0985

Tel. (787) 839-7688

Fax (787) 839-0282

SYNTEX (F P) INC

HC-01 Box 16625 Humacao,

Bo Mariana Road 909 Km 1.1

Pharmaceutical Products Manufacturer

PR 00791-9731

Humacao, PR 00791

Tel. (787) 852-0909

Tel. (787) 852-0919

Tel. (787) 852-0219

Fax (787) 852-9641

Parent/Affiliates/Branches

·Hoffman - La Roche: LTD

340 Kingsland Street 07110 Syntex Puerto Rico Inc

Hato Rev PR 00918

ATHE UPJOHN

Tel. (787) 846-4900

Redgy L. Coucke

PR 00617

MANUFACTURING CO

Gen. Manager (Manufacturing)

La Nueva Cruz Azul

PO Box 11307 Barceloneta.

268 Muñoz Rivera Ave. Suite 1005

General Manager

Frankie Santana

Francis Pagán

Medical Devices

Senior Facilities Engineer

▲WARNER LAMBERT INC

P O Box 786 Vega Baja, PR 00694 Tel. (787) 858-2323 President Robert Janosky Pharmaceutical Products Manufacturer

ZENITH LABORATORIES CARIBE INC



Zenith Laboratories Caribe, Inc.

P 0 Box 11979 Cidra, PR 00739 Cidra Ind'l Park Calle A Lote 8 Cidra. PR 00739 Tel. (787) 739-8421 Fax (787) 739-4321 Fax (787) 739-9405 VP-General Manager Nelson R. Rodríguez Finance Director Jesús R. Santiago Human Resources Manager Ruth Camacho Generic Drug Manufacturing Parent/Affiliates/Branches •IVAX Corporation 8800 Northwest 36th St. Miami 33178-2404

Employment Bracket: 150-200

▲ ZENITH LABORATORIES CARIBE INC

P O Box 11979 Cidra, PR 00739 Cidra Ind'l Park Cidra, PR 00739 Tel. (787) 739-8421 Fax (787) 739-4321 VP-General Manager Nelson R. Rodríguez Generic Drug Manufacturing Employment Bracket: 150-200

Looking for

an internet address?

de Puerto Rico, Inc.

Un Concesionario Independiente de a Blue Cross and Blue Shield Association.

Pharmaceutical Manufacturers La Cruz Azul

Get it fast in

the Internet Section.

PUERTO RICO P O Box 387 Vega Alta, PR 00692 Bo. Sabana Hoyos Rd. 690 Km. 1.1 Vega Alta, PR 00692 Tel. (787) 883-5800 Tel. (787) 882-5710 Tel. (787) 725-5800 Fax (787) 883-1177

General Manager Dee J. Hillherry Administrative Manager Luis A. Pagán Sales Manager Cayo Boada

Materials Manager Salvador Muriel Human Resources Manager Héctor Negrón Production Manager

David Rosa Quality & Assurance Manager Félix Román

Products & Services

Trademarks & Brandnames Sales Volume: \$10M Plus - \$50M

002649 Converted Paper and Paperboard Products, n.e.c.

P O Box 5068 Carolina, PR 00984 Fomento Bldg. Sabana Abajo Calle Varcacel Carolina, PR 00979 Tel. (787) 750-1810 Fax (787) 757-8045 President Antonio Castillo González Folding Box Manufacturing

P O Box 3587 San Juan, PR 00936 Tel. (787) 785-8080 General Manager Tomas Davis Cardboard

003229 P 0 Box 638 Humacao, PR 00792 Pressed and Blown Tel. (787) 852-0785 Glass and Owner Manuel Mediavilla Jr. Glassware, n.e.c. Pharmacy

OWENS-ILLINOIS DE

Glass Containers Manufacturers

Glass Containers

Employment Bracket: 301 - 350

PLASTIC & WILLS PRODUCTS

▲ LIANCA FOLDING BOX INC

▲ PUERTO RICO CONTAINER CORP

Manufacturing of Corrugated

PR 00917 insé Méndez products. CORP PR 00920 003851 Mector Alfonso Otometry Clinic ***ptometrist** abanetas Ind Park, Mercedita Ponce, obeida Irizarry ira, PR 00739 ant Manager Juel Soler

SANOFI PHARMACEUTICAL

n Box 70322 San Juan, R 00936-8322 dif Royal Bank Ste 285 Hato Rev. Tel. (787) 758-1033 Fax (787) 753-1263 General Manager nistribution of Pharmaceutical sales Volume: \$10M Plus - \$50M Employment Bracket: 26 - 50

AUPJOHN INTER-AMERICAN

Area Indl Higuillar Pueblo Viejo, Tel. (787) 792-6667 Medicinal & Botanical Products

AWYETH - AYERST LABORATORIES (PR) INC

PO Box 362917 San Juan. PR 00936-2917 Tel. (787) 782-3838 Pharmaceutical Product Distributors

Ophthalmic Goods

ACENTROVISION - CLINICA DE OPTOMETRIA

10 Box 2825 Hato Rey, PR 00919 Tel. (787) 764-4848

ACLINICA VISUAL MORALES IVETTE DRA & ASSOC O Box 34210 San Juan, PR 00926

(787) 758-2275

LESSILOR INDUSTRIES

1 (787) 848-4130 hance & Administrator Vice-Pres. ens Manufacturer

MENTOR CARIBE

0. Box 1358 El Jibaro Ind'l. Park (787) 739-8418 reocular Lens Manufacturer

The Business Register, where business finds business.

▲ OCULAR SCIENCES PUERTO RICO INC

P O Box 2801 Santa Isabel. PR 00757 Repto Ind. La Playa Rd. 538 Santa Isabel, PR 00757 Tel. (787) 845-2113 Fax (787) 845-3236 Manager Fernando Vázquez Manufacturers & Distributors of Contact Lens Sales Volume: \$5M Plus - \$10M Employment Bracket: 450

▲OPTI-FACTORY

El Centro Bldg. Marginal 14-B M. Rivera Ave Hato Rey. PR 00918 Tel. (787) 758-7878 Vice-President Luis C. Colón Optical Lab and Vision Center. Optometry Services. Sale and Repair of Eye Glasses and Security Lenses.

▲ PEARLE VISION CENTER OF PRINC

1122 Ponce de Leon Río Piedras. PR 00925 Tel. (787) 765-0088 Managing Director Caribbean Donald Johndrow Vision Test. Contact Lenses. Frames and other Ophthalmic Goods

▲ PROFESSIONAL OPTICAL SERVICES INC

P. O. Box 2636 Bayamon Sta Bayamón, PR 00960-2636 Tel. (787) 785-1862 Owner Anthony Mark Lens Manufacturers. Open Monday to Friday from 8:00 AM to 4:00 PM

▲SOUTHERN OPTICAL COMPANY

Sunny Isle Professional Bldg. St Croix, USVI 00820 Tel. (340) 778-6565 Manager Margaret Rennie Eye Glasses. Contact Lenses and everything for the Eyes.

002834 Pharmaceutical Preparations

▲A J BART P. O. Box 1360 Gurabo, PR 00778 Tel. (787) 737-8445 Owner

Alberto S. Baltolomei Distributors of Pharmaceutical Products.

▲ABBOTT PUERTO RICO **OPERATIONS**

P O Box 278 Barceloneta, PR 00617 Tel. (787) 846-6900 VP. Gen. Mgr. Abbott P R Operation José L. Rodriguez Manufacturers of Health Care Products

▲ACCUPHARMA RESEARCH AND SCIENTIFIC CONSULTING INC.

P O Box 1340 Gurabo PR 00778-1340 Tel. (787) 850-4215 President José F Colón Reyes Generic Medicaments, Research & Development. Microbiology Pharmaceutical Test. Sample Testings.

▲ALCON (PUERTO RICO) INC

P. O. Box 3000 Humacao, PR 00792 Tel. (787) 852-3080 General Manager Milton Barley Pharmaceutical Products Manufacturer

▲ ALLERGAN AMERICA

P. O. Box 60 Hormigueros, PR 00660 Tel. (787) 849-3895 General Manager José Luis Diaz Pharmaceutical Preparations Manufacturer

AMGEN MANUFACTURING INC



P O Box 4060 Juncos, PR 00777-4060 Road 31 Km. 24.6 Juncos, PR 00777 Tel. (787) 734-2000 Tel. (787) 731-2000 Fax (787) 734-6161 Director/Gen Manager James Sanabria Operations Manager Miguel Nazario Plant Controller Jaime Arraya Manager Human Resources

▲AYERST-WYETH PHARMACEUTICALS INC

Axel Lluch

Biotechmology

P. O. Box 10001 Guayama. PR 00785 Tel (787) 864-4010 Vice-President & General Manager Mariano Martinez Mora Pharmaceutical Products Manufacturer

BASE PHARMACEUTICALS

BASF BASF Pharmaceuticals A Unit of BASE

P O Box 795 Jayuya. PR 00664-0795 Road 144 Km 2.6 Jayuya, PR 0066-1 Tel. (787) 828-0990 Fax (787) 828-6440 Vice President & General Manager Carlos R León Buyer Victor Arcelay Pharmaceutical Products Manufacturer Parent/Affiliates/Branches

 BASF Pharmaceuticals New Jersey Employment Bracket: 101 - 150



The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

C

14

MAXTER CARIBE INC



10 Box 1290 Guayama, R00785-1290 anule 3 Km 142.5 Guayama, :R 00784 [el. (787) 864-5050 fax (787) 866-2714 taneral Manager Edol Ghigliotty P.E. userial Director orlor M. Guzman, Esq. Unulacturing of Anesthetics maceutical Products Division Parent/Affiliates/Branches 180 C Health Care Inc W07938 moducts & Services offurane USP, Enflurane USP. Ushoxyflurane ,Deflurane USP Indemarks & Brandnames Mrane, Forane, Suprane iles Volume: 150-200 Engloyment Bracket: 101 - 150







BAXTER HEALTH CARE CORP OF PR 10Box 518 Jayuya, PR 00664 1 (787) 828-3700 ant Manager adio Alvarez benterals Solutions and Medical

MITECH GROUP FENWAL MISION



180x 832 Maricao, PR 00606 357 Km 0.8 Maricao, PR 00606 (787) 838-3000 4(787) 838-2110 man Resources Manager Je Lugo Manager Amin Padilla Director (Fenyval del Caribe) P Van Heems A Manager sse Betancourt Maceutical Products Manufacturer, lucts to Collect. Store and linster Blood and its Components

Parent/Affiliates/Branches

· Baxter Healthcare Corp. Chicago, Deerfield ILL 00615 Products & Services Systems for the Collection. Separation, Preservation, Manipulation, and Transfusion of Blood and Blood Components. Trademarks & Brandnames Fenwal, Baxter

▲ BIOTECH GROUP FENWAL DIVISION

P O Box 832 Maricao, PR 00606 Rd. 357 Km 0.8 Maricao, PR 00606 Tel. (787) 838-3000 Fax (787) 838-2110 Human Resources Manager Angie Lugo Pharmaceutical Products Manufacturer. Products to Collect, Store and Administer Blood and its Components.

▲ BIOVAIL LABORATORIES INC

P O Box 3468 Carolina. PR 00984-3468 Sabana Abajo Ind'l Park 34 Calle B Iturregui Ave Carolina, PR 00983 Tel. (787) 750-5350 Fax (787) 750-5360 General Manager Carmen M Reyes Reyes Manufacturing Research & Development Employment Bracket: 51-103

BRISTOL LABORATORIES CORPORATION BRISTOL CARIBBEAN INC



Bristol Laboratories ⇒ Corporation Bristol Caribbean, Inc. Mayaguez Operations

P O Box 897 Mayaguez, PR 00681 Trade Zone 7 Rd. 114 Foreign Mayaguez, PR 00680 Tel. (787) 834-0185 Fax (787) 834-4182 Vice-President & General Manager Theodore Iliopoulos Human Resources Director Rosa Beatriz Sanabria Oncologic Business Unit Leader Jean F Schneider Liquid & Question Business Unit Leader Javier Santana Comptroller Edgardo Gratacós CPA Materials Control Director Javier Santana Director of Engineering José M Maldonado

Engages in the Production of Non-Beta Lactam Oral Dosage Pharmaceutical Products and Oncological Drugs.

Parent/Affiliates/Branches

· Bristol-Myers Squibb Company 345 Park Ave. New York NY 10154 Products & Services Analgesic & Anti-Cancer Trademarks & Brandnames Bristol-Myers Squibb Co



▲BRISTOL LABORATORIES CORPORATION BRISTOL CARIBBEAN INC

P O Box 897 Mayaguez, PR 00681 Trade Zone 7 Rd. 114 Foreign Mayaguez, PR 00680 Tel. (787) 834-0185 Fax (787) 265-4111 Vice-President & General Manager Theodore Iliopoulos Engages in the Production of Non-Beta Lactam Oral Dosage Pharmaceutical Products and Oncological Drugs

BRISTOL-MYERS BARCELONETA INC



BRISTOL-MYERS BARCELONFTA, INC.

P O Box 657 Barceloneta, PR 00617 Rd. 2 Km. 56.4 Barceloneta. PR 00617 Tel. (787) 846-3800 Fax (787) 846-7845 Administrative Assistant Elizabeth Padılla

Antibiotic Manufacturer Parent/Affiliates/Branches Bristol Myers Squibb Company 345 Park Ave. New York NY 10154-0037

Products & Services

Amoxicillin Manufacturer for the Local and International Market

Trademarks & Brandnames

Polycillin, Buspar, Polymox, Beta Pen, Dicloxcil, Prostaphlin, Duricef. Naful, Staphcillin, Dyna Pen. Ultraceph. Pen V, Prostaphlin, Duricef. Naful, Staphcillin, Dyna Penn. Ultraceph, Pen V Sales Volume: Over \$50M Employment Bracket: 600 Plus





▲ CHIRON BETA CORPORATION

P O Box 1624 Canóvanas, PR 00729 Tel. (787) 876-1400 Secretary Administrative Marta Ortiz Pharmaceutical Products

▲COCHARON WHOLESALE P 0 Box 8567 Humacao, PR 00792 Tel. (787) 852-4325 Manager Rafael Mangual Pharmaceutical Preparations

▲COLON DE JIMÉNEZ ANA L P 0 Box 22678 U P R Sta. San Juan, PR 00931 Tel. (787) 763-1454 Owner Ana Colón Dermatologist

▲ DADE DIAGNOSTIC OF PR INC

P 0 Box 865 Aguada, PR 00602 Tel. (787) 868-5500 Manufacturing Manager Randy Howe Manufacturing of Reagents and Laboratory Controls

▲ DANBURY PHARMACAL P.R. INC.

P O Box 886 Humacao, PR 00792 Road 3 Km. 76.9 Humacao Ind'l. Park Humacao, PR 00792 Tel. (787) 852-5151 Fax (787) 852-5974 General Manager Blanca Meléndez Pharmaceutical Manufacturing Sales Volume: \$5M Plus - \$10M Employment Bracket: 151 - 200

▲ DEL MAR PHARMACY SERVICE INC

P O Box 233 Mercedita Ponce, PR 00715-0043 Tel. (787) 842-6263 Pharmaceuticals & Related Products Distribution

▲ DENVER CHEMICAL (PR) INC

HC-04 Box 4012 Humacao, PR 00791-9502 Tel. (787) 852-3240 Manufacturing Manager Juan R. Suarez Pharmaceutical Products Manufacturer

It pays to register

in the Business Register

DORASOL LABORATORIES
INC
P 0 3906 San Juan. PR 00936
Tel. (787) 753-6549
President

President Agustin Rodriguez Kissell Manufacturers of Pharmaceutical Agustis

DROGUERIA GONZÁLEZ INC PO BOX 350 Ponce. PR 00733 [el. (787) 724–1078 pharmaceutical Preparations

DROGUERIA RIO PIEDRAS INC 590 De Diego Ave. Río Piedras, PR 00924 1el. (787) 751–5030

president Raúl González Wholesale and Distribution of

Wholesale and Distribution Medicines.

ADUPONT MERCK PHARMA

PO Box 301000 Manatí. PR 00674-3000 Tel. (787) 854-1030 President William Henández Pharmaceutical Products

AEATON LABORATORIES

PO Box 1055 Manatí, PR 00674 Tel. (787) 854–1520 Vice-President General Manager Ramón Sepulveda Pharmaceutical Products Manufacturer

▲ENGRAPH LEHIGH PRESS PUERTO RICO

P O Box 1469 Juncos, PR 00777
Mamey Ind'l Center Road 189 Km
12.4 Juncos. PR 00777
Tel. (787) 734–1000
Fax (787) 734–1004
President
Luis Herrera
Insert and Outsert for Pharmaceutical
Industries Office Hours. Mon – Fri
from 8:00 AM to 5:00 PM
Sales Volume: \$5M Plus – \$10M
Employment Bracket: 101 – 150

▲ENVIRONMENT PRO-TEK

P O Box 38053 Airport Station San Juan, PR 00937-1053 Tel. (787) 749-9534 Consultant René Santiago Air & Water Purificator, Oxygen Generator. Sediment Remover, Biodegtable Products. Insulation For Boiler.

Looking for a Fax number?

Get it fast in the Fax Section.

▲EX-LAX INC

H C - 01 Box 16629 Humacao.
PR 00791-9731
Tel. (787) 852-3190
Executive Vice Pres. & General Mgr
Santos Troche
Laxative and Antiflatulex
Manufacturers

▲ FAULDING PUERTO RICO INC

P O Box 250471 Ramey Branch Aguadilla. PR 00604-0471 Tel. (787) 890-3000 General Manager Juan Miguel Gomez Pharmaceutical Products

▲ GENERICS OF PUERTO RICO INC

P O Box 11533 Fdez Juncos Sta Santurce, PR 00910 Monte Rey Urb. 3 Calle Acacia Pueblo Viejo, PR 00920 Tel. (787) 792–2430 Fax (787) 782–0990 President Carlos A. Fraga Pharmaceutical Products Distributors Sales Volume: S1M Plus – \$5M Employment Bracket: 26 – 50

▲GLAXO WELCOME

P 0 Box 363461 San Juan. PR 00936-3461 Tel. (787) 250-7580 Finance Director Luis Cintrón Pharmaceuticals Wholesaler

AHOECHST MARION
ROUSSEL PUERTO RICO
INC

P O Box 2120 San Juan. PR 00922-2120 Tel. (787) 782-1900 General Manager Francisco Nordelo Pharmaceutical Products

JANSSEN ORTHO LLC

JANSSEN PRODUCTS

HC - 02 Box 19250 Gurabo, PR 00778-9629 Bo. Mamey II Road 933 Km. 0.1 Gurabo, PR 00778-9250 Tel. (787) 789-5000 Fax (787) 272-7644 Fax (787) 272-7602 VP Manufacturing & General Manager William B Nelson Director of Logistic & Materials Mgut.
Margarita Hernández
Finance Director
Tony Perez
Human Resource Manager
Fernando Plaud
OA/OC Director
Eric Olivieri
Director of Engineering
Maintenance/Environmental & Safety
Nallagounder Kuppusamy
Pharmaceutical Products
Parent/Affiliates/Branches

• Johnson & Johnson Corporate
Worldwide Headquarters
One Johnson & Johnson Plaza

Janssen Pharmaceutical
 1125 Harbourton Road Titusville
 NJ 08560-0200

New Brunswick NJ 08933

Products & Services

Propulsid. Prisperdal, Sporanox. Nizoral. Vermox. Hismanal Sales Volume: Over \$50M Employment Bracket: 401 – 450



▲ JANSSEN PRODUCTS

HC - 02 Box 19250 Gurabo, PR 00778-9629 Bo. Mamey II Road 933 Km. 0.1 Gurabo, PR 00778-9250 Tel. (787) 789-5000 Fax (787) 272-7644 VP. Manufacturing Tomás Ramírez Pharmaceutical Products Sales Volume: Over \$50M Employment Bracket: 401 - 450

▲LEDERLE PARENTERALS INC

P O Box A C Pueblo Sta. Carolina. PR 00984–4904
65 Infantry Ave. Km. 9.7 Carolina. PR 00979
Tel. (787) 752–7474
Fax (787) 762–3395
President & Gen. Manager
Alfredo R Nadal
Pharmaceutical Products
Sales Volume: \$5M Plus – \$10M
Employment Bracket: 500 Plus

▲LIFESCAN (PR) INC

P O Box 5001 Cabo Rojo, PR 00623
Bo Pedernales Road 308 Km 0.8
Cabo Rojo, PR 00623
Tel. (787) 255-7700
Fax (787) 255-7713
Finance Manager
Max Roldán
Reagent Strips for Glucose
Monitoring Open Monday to Friday
from 8:00 AM - 5:00 PM
Employment Bracket: 251 - 300

LILLY DEL CARIBE INC.

Lilly

P O Box 1198 Carolina.
PR 00986-1198
P R Ind'l Park Km 12.6 65th Inf Ave Carolina. PR 00985
Tel. (787) 257-5555
Tel. (787) 257-5333
Fax (787) 257-5544
Fax (787) 257-5988
President & General Manager
Paul Ahern
Director Human Resources
Iliana Rivera
Director Quality Control

Manufacturer of Pharmaceutical

Sales Volume: \$5M Plus - \$10M

Employment Bracket: 500 Plus

Evelyn Rodriguez

Products

The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

MARION & COMPANY iox 3009 Manatí, PR 00674 787) 854-3005 Manager isio Rivera Maceutical Products

CGAW OF PUERTO RICO

ix 729 Sabana Grande 187) 873-4600 Manager | Devices Manufacturing

Looking for

an internet address?

Get it fast

The internet Section.

IUCAS ! INSERTCO PHARMACEUTICAL PRINTING CO

_{Rox} 377 San Germán, PR 00683 olifo Indl Park Rd. 102 Km 33.2 san Germán, PR 00683

(787) 892-1268 (787) 892-4112

CAS - INSERTCO

Salzano Manager diction Coordinator

Manager ted Centeno basing Agents

ada Mora omer Service Morales

Lunt Executive Sevilla

ds Outserts & Labels for maceutical and Electronic wies, Starch Displacement & ss Pharmaceutical Preparation. Volume: \$5M Plus - \$10M dyment Bracket: 90 - 100

A DIV OF OMJ PHARMACEUTICAL INC P. O. Box 710 Dorado. PR 00646-0710

▲MCNEIL PHARMACEUTICAL

Tel. (787) 796-1540 General Manager Krenly Cruz Manufacturer of Capsules, Tablets, Caplets and Liquid of Ethical Pharmaceutical Products

▲ MEDISEARCH P R INC

P O Box 2460 Guayama. PR 00785-2460 Tel. (787) 864-0684 President John K. Whitney Manufacturer of Therapeutic Pads. Heat Therapy Pads, Pressure Ulcer Relief. Thrombo Cuff.

MERCK SHARP & DOHME QUIMICA DE PRINC ARECIBO OPERATIONS



MERCK SHARP & DOHME .

P O Box 1011 Sabana Hoyos Barceloneta, PR 00688 Road 2 Km. 60.3 Sabana Hoyos. PR 00688 Tel. (787) 846-1600

MCNEIL CONSUMER PRODUCTS A DIV OF J & J CONSUMER CO PRINC



General Manager Iván Lugo Director of Public Affairs Rafael Robert Purchasing Manager PR Operations Luis Archilla Financial Director P O Box 2009 Las Piedras. Carlos Gomez PR 00771-2009 IS Operation Head for PR Bo. Montones Road 183 Km 19 8 Luis E. Ortiz Las Piedras, PR 00771 Pharmaceutical Manufacturing Tel. (787) 733-1000 Parent/Affiliates/Branches Tel. (787) 782-7030 . Merck and Company Inc. Whitehouse Station NY

Fax (787) 846-5580

Richard S. Bowles

Luis Couto

Operations

Operations

Caguas PR 00725

Director of PR Operations

Senior Director Mfg Services

Fax (787) 733-6616 General Manager Edgardo J. Fabregas Over the Counter Propietary Products Parent/Affiliates/Branches

• McNeil Consumer Products Inc Camp Hill Road 19034 Trademarks & Brandnames

Tylenol Employment Bracket: 351 - 400



▲ MOVA PHARMACEUTICAL CORPORATION

· MSD Quimica de PR. Caguas

• MSD Quimica de PR Barceloneta

P O Box 601 Barceloneta PR 00617

Trademarks & Brandnames

Employment Bracket: 500 Plus

Prilosec, Fosamax, Proscar

Sales Volume: Over \$50M

P O Box 8639 Caguas, PR 00726 Villa Blanca Ind'l Park Rd 1 Km 34.1 Caguas, PR 00726 Tel. (787) 746-8500 Fax (787) 743-7669 President & CEO Joaquín Viso Pharmaceutical Products Employment Bracket: 500 Plus

▲ NESSAN LABORATORIES INC

P. O. Box 1941 Carolina, PR 00984 Tel. (787) 769-5053 President Nellie E. Sánchez Pharmaceutical Products

O M J PHARMACEUTICAL INC

OMJ Pharmaceuticals, Inc.

P O Box 367 San German, PR 00683 Rd. 362 Km. 0.5 San Germán. PR 00683 Tel. (787) 892-2245 Fax (787) 892-2095 General Manager Felix Morales Lye Care Products Manufacturers

Parent/Affiliates/Branches

Devices

Ortho Biotech Inc. U.S. Route 202 P O Box 670 Raritan 00869-0602 Products & Services Ophthalmics Products, Medical

Employment Bracket: 201 - 250

▲ORTHO PHARMACEUTICAL/A DIV OF J & J PHARM CO (PR) INC

P. O. Box 463 Manatí, PR 00674 Tel. (787) 854-1800 General Manager Krenly Cruz Contraceptives and Semi-Solids

▲P C R DE PUERTO RICO INC

P O Box 960 Punta Santiago PR 00741 Road 3 Km. 76.9 Humacao. PR 00791 Tel. (787) 852-4520 Fax (787) 852-4284 Plant Manager Santiago Hernández Reyes Organic Chemicals for Cancer Treatment Employment Bracket: 0 - 25

The Business Register

is the most complete

and up-to-date

Business to Business

Directory

in Puerto Rico.

PACO PUERTO RICO INC

P 0 Box 1661 Canóvanas, PR 00729 san Isidro Ind Park Road 188 Km 0.5 Canóvanas, PR 00729

Tel. (787) 876-6362 Tel. (787) 876-6258

Fax (787) 876-0165

Fax (787) 876-5099

Plant Manager Rubén Aguayo Human Resources Manager Frances Guzmán Finance Director Brian Fichthorn Account Executive Miguel Parada Material Manager

Antonio Rivera Complete Manufacturing and Packaging Services for the Pharmaceutical and Health Care

Industries. Parent/Affiliates/Branches

• Paco Pharmaceutical Services Inc New Jersey NJ Employment Bracket: 100-225

PFIZER PHARMACEUTICALS



P 0 Box 628 Barceloneta, PR 00617 Cruce Dávila Rd. 2 Km 58.2 Barceloneta, PR 00617 Tel. (787) 846-4300 Fax (787) 846-7022 Fax (787) 846-5077 General Manager Anthony Maddaluna Director, H R and Public Affairs Héctor Corretier Pharmaceutical Products Manufacturing. Parent/Affiliates/Branches •Pfizer Inc 235 E. 42 St. New York City NY 10017 Trademarks & Brandnames

Feldene, Procardia, Procardia XL,

Glucotrol. Diflucan, Antivert / Bonine, Minipress / Minizide, Sinequan, Zythromax. Cardura, Zoloft Sales Volume: Over \$50M Employment Bracket: 1000 Plus

It pays to register in the Business Register **▲**PROCTER & GAMBLE PHARMACEUTICAL PUERTO RICO INC

P 0 Box 1055 Manati. PR 00674 Tel. (787) 854-1520 Vice Pres. & Gen. Manager Ramón Sepúlveda Pharmaceutical Products Manufacturer

REEDCO & DENTCO INC



H C - 04 Box 4013 Humacao,

PR 00791 Humacao Ind'l Park Rd 3 Km 76.4 Humacao, PR 00791 Tel. (787) 852-3400 Tel. (787) 724-6756 Fax (787) 850-2300 Fax (787) 852-7870 General Manager

Luis R. Acevedo Production Manager Lizzette Pérez Quality Service Manager Reynaldo Velázquez Maintenance Facility Manager Victor Marrero Traffic & Warehouse Manager Angel Rodriguez Human Resources Manager Mildred Sein Administration Manager Eduardo Clemente Plant Engineer & Regulatory Affairs Ivan Santiago Inventory Control Manager Juan C Aponte Traffic Supervisor Miquel A. López Pharmaceutical Products Manufacturer Parent/Affiliates/Branches • Block Drug Co Inc 257 Cornelison Ave NJ 07302

Products & Services Dental Product. Shampoo's, Pharmaceutical, Dermatologic Trademarks & Brandnames

Tegrin, Sensodyne-F, Poligrip, Super Poligrip, Dentu-Creme, Sensodyne, R & C, B C Tablet. Nytol, Tegrin L T. Balmex, Durascreen Sales Volume: \$5M Plus - \$10M

Employment Bracket: 301 - 350



H C - 04 Box 4013 Humacao, PR 00791 Humacao Ind'l. Park Rd. 3 Km. 76.4 Humacao. PR 00791 Tel. (787) 852-3400

Fax (787) 850-2300 General Manager Luis R. Acevedo Pharmaceutical Products Manufacturer Sales Volume: \$5M Plus - \$10M Employment Bracket: 301 - 350

RHONE-POULENC ROBER CARIBBEAN



P O Box 364824 San Juan, PR 00936-4824 De La Cruz Plaza Suite 100 Metro Office Park Guaynabo, 00968-1705 Tel. (787) 783-6868 Fax (787) 783-4845 Fax (787) 783-4346 Finance Director Angel B. Méndez General Manager & Vice President Isidro J Ferrer Marketing & Sales Director Nelson De Jesus Sales Director Ana L Del Rio Sales & Marketing of Pharmaceutical Preparations **Products & Services** Lozol, Tussar, SLO-BID, Nasacort, Asmacort, Dilacox, Calcimar, DDAVP. Penetrex, Nitrolingual Zagam



Trademarks & Brandnames

Sales Volume: \$5M Plus - \$10M

RHONE POULENC ROBER PR

INC P O Box 345 Manatí. PR 00674-0345 604 Road Bo San José Manati. PR 00674 Tel. (787) 854-1058 Fax (787) 854-3100 VP & General Manager Carlos Santiago Comptroller Jaime L. Sanabria Operations Director Franco Negrón Human Resource Director

Victor Osuna Quality Control Director Jorge Cotto Materials Management Director Dolores Fernández Project Engineer José R. Osorio

Pharmaceutical Preparations

Manufacturer of Tablets, Capsules,

Creams & Inhaled Therapy Products.

Ramona Orozco Pharmaceutical Products Distributor. Sales Volume: \$5M Plus - \$10M Employment Bracket: 0 - 25

Parent/Affiliates/Branches

•Rhone Poulenc Rorer, Inc.

Collegeville 19426-0107

Products & Services

RIMACO INC

Santurce, PR 00910

Tel. (787) 792-9512

Fax (787) 782-8310

Ricardo Mayo Alvarez

Marketing Manager

Daniel Torres Torres

Executive Secretary

Treasurer/Vice President

Ricardo Mayo Alvarez Jr.

President

Corp

500 Arcola Rd. P O Box 1200

Rhone Poulenc Rorer Caribbean

Park Guaynabo PR 00968-1705

Trademarks & Brandnames

Hygroton, Vytone, Benzamycin,

Hytone. Penetrex, Masacort AQ

Employment Bracket: 351 - 400

P O Box 8895 Fdez, Juncos Station

Villa Caparra Ext. Calle Marginal

Buchanan Guaynabo, PR 00966

De La Cruz Plaza S-100 Metro Office

Nasacort, Lozol, Azmacort, Slo-bid.

Benzagel, Sulfacet, Rilutek, Nicobid.

▲SANOFI PHARMACEUTICAL INC

P O Box 70322 San Juan, PR 00936-8322 Tel. (787) 758-1033 General Manager José Méndez Distribution of Pharmaceutical Products.

Contact us

at our internet site

www.pbrb.com.

ICHERING-PLOUGH RODUCTS INC



Box 1779 Las Piedras, Jo Ind'l Park Rd 183 Piedras. PR 00771 (4) (787) 733-2323 (187) 783-3333 far (787) 733-3229 m (787) 733-2333 aiai Manager Rodriguez eation Director oro Ciena (siptroller and Santiago nan Resources Manager asse Cordoves senals Director an Aldarondo aneering Manager nes Kregloh My Control Director ando Santiago maceutical Manufacturer of Bulk inished Dosage Form, Specializing Sustained Release Technologies Must Manufacturing Services hent/Affiliates/Branches weing Plough Corporation Salda Farms P O Box 1000 Mison NJ 07940-1400 which & Services

S Volume: \$5M Fais - \$10M oloyment Bracket '51 - 300

Min. Unidur, Normodyne, Theo-Dur

Mels, K-Dur Tablet... Eulexin

ISCHMID PRODUCTS CORP

4016 Humaicao, 00791-9502 1787) 852-2476 adent & General Namager A. Marrero doms for Natural ling and Mivity Manufactu s

MEARLE CARIBBEAN

Box 367189 San Juan, 10936-7189 (787) 258-6474

Grieco

Maceutical and Consumer ucts Sales and Distribution SEARLE, LTD



MONSANTO 🛂 Food · Health · Hope

P O Box 11247 Barceloneta. PR 00617-1247 Rd 140 Km 64.4 Barceloneta PR 00617 Tel. (787) 846-5000 Fax (787) 846-6595 Fax (787) 846-2640 General Manager Hector Jové Comptroller Iván Marcano Quality Control Director Rosaura Ortiz Materials Director Vivian Molinari Human Resource Director José L. Narváez **Engineering Director** Felipe Sánchez Pharmaceutical Products Manufacturing. Exclusive Distributor of Nycomed Products (Omnipaque): Picker International del Caribe Inc.



Visipaque, Omniscan, Omnipaque, And

Trademarks & Brandnames

Third Party Manufacturing



P O Box 10757 San Juan. PR 00922-0757 Tel. (787) 793-2700 General Manager Francisco Santos Manufacturer & Distributors of Pharmaceutical O T C Products

SMITHKLINE BEECHAM INTERAMERICAN CORPORATION



P O Box 2160 San Juan. PR 00922 2160 Calle Diana #29 Amelia Ind'i Park Guaynabo, PR 00922 Tel. (787) 774-8000 Fax (787) 774-0302 General Manager Jose Vargas

Finance Manager Armando Rodríguez Sales of Ethical Products Trademarks & Brandnames

S B-I A C Puerto Rico Sales Volume: \$10M Plus - \$50M Employment Bracket: 51 - 100



SQUIBB MANUFACTURING INC

Lat Resident Reineff, in

Fax (787) 842-0313

Manufacturing & Sale of OTC

Sales Volume: \$0 - \$500K

Employment Bracket: 0 - 25

Products, Veterinary Products and

Owner

José Rivera

Private Labels.

SMITHKLINE BEECHAM **PHARMACEUTICALS**



P 0 Box 11975 Cidra.

SmithKline Beecham Pharmaceuticals

PR 00739-1975 Bo. Certenejas Rd 172 Km 9.1 Cidra, PR 00739 Tel. (787) 766-4000 Tel. (787) 739-8401 Fax (787) 250-3710 President-General Manager José Luis Rosado Vice-President Finance Raúl Cermeño Business Development Director Joan Cruz Pharmaceutic Manufacturing Director Betsy Rodriquez Vice-President Human Resources Sonia Berrios Vice Pres. Public Relations Jorge González VP Quality Assurance Adalberto Ramirez **Enginering Director** Ismael Guzmán Pharmaceutical Products Parent/Affiliates/Branches

· Smithkline Beecham S B House Great West Road London

 Smithkline Interamerican P O Box 2160 San Juan PR 00922-2160

· Smithkline Beecham Consumer Brand P O Box 9597 Hato Rey PR 00919

Trademarks & Brandnames

Tagamet, Ecotrin, Feosol, Stelazine, Relafen, Dyazide, Bactroban, Compazin .Paxil Sales Volume: Over \$50M

Employment Bracket: 500 Plus

▲ SPECIALTIES CHEMICAL DBA PONCE PHARMA

P O Box 277 Playa Sta. Ponce. PR 00731 Playa Ponce 46 Calle Mirasol Ponce PR 00731 Tel (787) 842-0313

P 0 Box 609 Humacao, PR 00792 Road 3 Km. 77.5 Humacao. PR 00791 Tel. (787) 852-1255 Fax (787) 852-3800 VP & General Manager Francisco Gutierrez Financial Site Leader Tina Fiumenero Human Resources Site Leader Grisel Castro Director of Quality Control Luis O. Rodriguez Director of Manufacturing Bernie Morales Director of Maintenance Israel Díaz Chemical Products Manufacturers

Parent/Affiliates/Branches

 Bristol Myers Squibb Company 345 Park Avenue 10154 Sales Volume: \$5M Plus - \$10M Employment Bracket: 500 Plus



▲ SQUIBB MANUFACTURING INC

P 0 Box 609 Humacao, PR 00792 Road 3 Km. 77.5 Humação PR 00791 Tel. (787) 852-1255 Fax (787) 852-3800 General Manager Francisco Gutierrez Chemical Products Manufacturers Sales Volume: \$5M Plus - \$10M Employment Bracket: 500 Plus

Looking for

an internet address?

Get it fast in

the Internet Section.

▲TU FARMACIA Y MÁS

p O. Box 364567 San Juan. PR 00936-4567 Tel. (787) 758-0985 General Manager Anthony Leber sales. Marketing & Distribution of consumer Health Products

ASTERLING PRODUCTS

INTERNATIONAL INC

ASTRYKER PUERTO RICO

p 0 Box 329 Arroyo, PR 00714 Road 3 Km 130.2 Arroyo. PR 00714 Tel. (787) 839-7688 Fax (787) 839-0282 Senior Facilities Engineer Francis Pagán Medical Devices sales Volume: \$5M Plus - \$10M Employment Bracket: 451 - 500

SYNTEX (F P) INC



Syntex Humacan Operation A Realin Geoup Company

HC-01 Box 16625 Humacao, PR 00791-9731 80 Mariana Road 909 Km 1.1 Humacao, PR 00791 Tel. (787) 852-0909 Tel. (787) 852-0919 Tel. (787) 852-0219 fax (787) 852-9641 General Manager Frankie Santana Pharmaceutical Products Manufacturer Parent/Affiliates/Branches · Hoffman - La Roche: LTD 340 Kingsland Street 07110 Syntex Puerto Rico Inc. 268 Muñoz Rivera Ave. Suite 1005 Hato Rev PR 00918



ATHE UPJOHN MANUFACTURING CO PO Box 11307 Barceloneta. PR 00617 lel. (787) 846-4900 Gen. Manager (Manufacturing) Redgy L. Coucke Pharmaceutical Manufacturers



LA NUEVA CRUZ AZUL

Un Concesionario Independiente de la Blue Cross and Blue Shield Association.

P O Box 638 Humacao, PR 00792 Tel. (787) 852-0785 Owner Manuel Mediavilla Jr.

Pharmacy

▲WARNER LAMBERT INC

P O Box 786 Vega Baia, PR 00694 Tel. (787) 858-2323 President Robert Janosky Pharmaceutical Products Manufacturer

ZENITH LABORATORIES CARIBE INC



Zenith Laboratories Caribe, Inc.

P O Box 11979 Cidra, PR 00739 Cidra Ind'l Park Calle A Lote 8 Cidra. PR 00739 Tel. (787) 739-8421 Fax (787) 739-4321 Fax (787) 739-9405 VP-General Manager Nelson R. Rodríguez Finance Director Jesús R. Santiago Human Resources Manager Ruth Camacho Generic Drug Manufacturing Parent/Affiliates/Branches IVAX Corporation 8800 Northwest 36th St. Miami 33178-2404 Employment Bracket: 150-200



ZENITH LABORATORIES CARIBE INC

P O Box 11979 Cidra, PR 00739 Cidra Ind'l Park Cidra, PR 00739 Tel. (787) 739-8421 Fax (787) 739-4321 VP-General Manager Nelson R. Rodriguez Generic Drug Manufacturing Employment Bracket: 150-200

Looking for

an internet address?

Get it fast in

the Internet Section.

003229 Pressed and Blown Glass and Glassware, n.e.c.

OWENS-ILLINOIS DE

PUERTO RICO P 0 Box 387 Vega Alta, PR 00692 Bo. Sabana Hoyos Rd. 690 Km. 1.1 Vega Alta, PR 00692 Tel. (787) 883-5800 Tel. (787) 882-5710 Tel. (787) 725-5800 Fax (787) 883-1177 General Manager Dee J. Hillherry Administrative Manager Luis A. Pagán Sales Manager

Cayo Boada Materials Manager Salvador Muriel Human Resources Manager Héctor Negrón Production Manager David Rosa Quality & Assurance Manager Félix Román Glass Containers Manufacturers **Products & Services** Glass Containers Trademarks & Brandnames

Sales Volume: \$10M Plus - \$50M Employment Bracket: 301 - 350



PLASTIC & WILLS PRODUCTS

002649 Converted Paper and Paperboard Products, n.e.c.

▲ LIANCA FOLDING BOX INC

P O Box 5068 Carolina, PR 00984 Fomento Bldg. Sabana Abajo Calle Varcacel Carolina, PR 00979 Tel. (787) 750-1810 Fax (787) 757-8045 President Antonio Castillo González Folding Box Manufacturing

▲ PUERTO RICO CONTAINER CORP

P O Box 3587 San Juan, PR 00936 Tel. (787) 785-8080 General Manager Tomas Davis Manufacturing of Corrugated Cardboard

SONOCO OF PRINC



SONOCO

Tel. (787) 893-2675 Tel. (787) 893-2600 Fax (787) 893-2200 General Manager José Zayas Plant Superintendent Octavio Divison Sales Representative Jackie Rosado Paper Products & Fiber Composite Cans and Spiral Tubes Parent/Affiliates/Branches Sonoco Products Co. Hartsville SC Trademarks & Brandnames

Sonotubes, Sonovoids, Sonomolds

P 0 Box 399 Yabucoa, PR 00767







▲ SUNRISE PAPER CORP P O Box 9702 Carolina. PR 00988-9702 Tel. (787) 748-1595 President Mateo Laboy Napkins Manufacturers

> Looking for a Fax Number? Get It fast in the Fax Section

The Business Register. where business finds business

Contact us an our internet site www.pbrp.com.

APPENDIX D: Federal register: 21 CFR Part 11.



Thursday March 20, 1997

Part II

Department of Health and Human Services

Food and Drug Administration

21 CFR Part 11

Electronic Records; Electronic Signatures; Final Rule

Electronic Submissions; Establishment of Public Docket; Notice

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Food and Drug Administration

21 CFR Part 11

[Docket No. 92N-0251]

RIN 0910-AA29

Electronic Records; Electronic Signatures

AGENCY: Food and Drug Administration, HHS.

ACTION: Final rule.

SUMMARY: The Food and Drug Administration (FDA) is issuing regulations that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations, which apply to all FDA program areas, are intended to permit the widest possible use of electronic technology, compatible with FDA's responsibility to promote and protect public health. The use of electronic records as well as their submission to FDA is voluntary. Elsewhere in this issue of the Federal Register, FDA is publishing a document providing information concerning submissions that the agency is prepared to accept electronically

DATES: Effective August 20, 1997. Submit written comments on the information collection provisions of this final rule by May 19, 1997.

ADDRESSES: Submit written comments on the information collection provisions of this final rule to the Dockets Management Branch (HFA–305), Food and Drug Administration, 12420 Parklawn Dr., rm. 1–23, Rockville, MD 20857.

The final rule is also available electronically via Internet: http://www.fda.gov.

FOR FURTHER INFORMATION CONTACT:
Paul J. Motise, Center for Drug
Evaluation and Research (HFD–
325), Food and Drug
Administration, 7520 Standish Pl.,
Rockville, MD 20855, 301–594–
1089. E-mail address via Internet:
Motise@CDER.FDA.GOV, or

Tom M. Chin, Division of Compliance Policy (HFC–230), Food and Drug Administration, 5600 Fishers Lane, Rockville, MD 20857, 301–827– 0410. E-mail address via Internet: TChin@FDAEM.SSW.DHHS.GOV SUPPLEMENTARY INFORMATION: I. Background

In 1991, members of the pharmaceutical industry met with the agency to determine how they could accommodate paperless record systems under the current good manufacturing practice (CGMP) regulations in parts 210 and 211 (21 CFR parts 210 and 211). FDA created a Task Force on Electronic Identification/Signatures to develop a uniform approach by which the agency could accept electronic signatures and records in all program areas. In a February 24, 1992, report, a task force subgroup, the Electronic Identification/ Signature Working Group, recommended publication of an advance notice of proposed rulemaking (ANPRM) to obtain public comment on the issues involved.

In the Federal Register of July 21. 1992 (57 FR 32185), FDA published the ANPRM, which stated that the agency was considering the use of electronic identification/signatures, and requested comments on a number of related topics and concerns. FDA received 53 comments on the ANPRM. In the Federal Register of August 31, 1994 (59) FR 45160), the agency published a proposed rule that incorporated many of the comments to the ANPRM, and requested that comments on the proposed regulation be submitted by November 29, 1994. A complete discussion of the options considered by FDA and other background information on the agency's policy on electronic records and electronic signatures can be found in the ANPRM and the proposed

FDA received 49 comments on the proposed rule. The commenters represented a broad spectrum of interested parties: Human and veterinary pharmaceutical companies as well as biological products, medical device, and food interest groups, including 11 trade associations, 25 manufacturers, and 1 Federal agency.

II. Highlights of the Final Rule

The final rule provides criteria under which FDA will consider electronic records to be equivalent to paper records, and electronic signatures equivalent to traditional handwritten signatures. Part 11 (21 CFR part 11) applies to any paper records required by statute or agency regulations and supersedes any existing paper record requirements by providing that electronic records may be used in lieu of paper records. Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures, initials, and

other general signings required by agency regulations.

Section 11.2 provides that records may be maintained in electronic form and electronic signatures may be used in lieu of traditional signatures. Records and signatures submitted to the agency may be presented in an electronic form provided the requirements of part 11 are met and the records have been identified in a public docket as the type of submission the agency accepts in an electronic form. Unless records are identified in this docket as appropriate for electronic submission, only paper records will be regarded as official submissions.

Section 11.3 defines terms used in part 11, including the terms: Biometrics, closed system, open system, digital signature, electronic record, electronic signature, and handwritten signature.

Section 11.10 describes controls for closed systems, systems to which access is controlled by persons responsible for the content of electronic records on that system. These controls include measures designed to ensure the integrity of system operations and information stored in the system. Such measures include: (1) Validation; (2) the ability to generate accurate and complete copies of records; (3) archival protection of records; (4) use of computer-generated, time-stamped audit trails; (5) use of appropriate controls over systems documentation; and (6) a determination that persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks.

Section 11.10 also addresses the security of closed systems and requires that: (1) System access be limited to authorized individuals; (2) operational system checks be used to enforce permitted sequencing of steps and events as appropriate; (3) authority checks be used to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform operations; (4) device (e.g., terminal) checks be used to determine the validity of the source of data input or operation instruction; and (5) written policies be established and adhered to holding individuals accountable and responsible for actions initiated under their electronic signatures, so as to deter record and signature falsification.

requirements by providing that electronic records may be used in lieu of paper records. Electronic signatures which meet the requirements of the rule will be considered to be equivalent to full handwritten signatures, initials, and

to ensure record authenticity, integrity, and confidentiality.

Section 11.50 requires signature manifestations to contain information associated with the signing of electronic records. This information must include the printed name of the signer, the date and time when the signature was executed, and the meaning (such as review, approval, responsibility, and authorship) associated with the signature. In addition, this information is subject to the same controls as for electronic records and must be included in any human readable forms of the electronic record (such as electronic display or printout).

Under § 11.70, electronic signatures and handwritten signatures executed to electronic records must be linked to their respective records so that signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Under the general requirements for electronic signatures, at § 11.100, each electronic signature must be unique to one individual and must not be reused by, or reassigned to, anyone else. Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, the organization shall verify the identity of the individual.

Section 11.200 provides that electronic signatures not based on biometrics must employ at least two distinct identification components such as an identification code and password. In addition, when an individual executes a series of signings during a single period of controlled system access, the first signing must be executed using all electronic signature components and the subsequent signings must be executed using at least one component designed to be used only by that individual. When an individual executes one or more signings not performed during a single period of controlled system access, each signing must be executed using all of the electronic signature components.

Electronic signatures not based on biometrics are also required to be used only by their genuine owners and administered and executed to ensure that attempted use of an individual's electronic signature by anyone else requires the collaboration of two or more individuals. This would make it more difficult for anyone to forge an electronic signature. Electronic signatures based upon biometrics must be designed to ensure that such signatures cannot be used by anyone other than the genuine owners.

Under § 11.300, electronic signatures based upon use of identification codes

in combination with passwords must employ controls to ensure security and integrity. The controls must include the following provisions: (1) The uniqueness of each combined identification code and password must be maintained in such a way that no two general scope and effect of proposed individuals have the same combination of identification code and password; (2) persons using identification codes and/ or passwords must ensure that they are periodically recalled or revised; (3) loss management procedures must be followed to deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification codes or password information; (4) transaction safeguards must be used to prevent unauthorized use of passwords and/or identification codes, and to detect and report any attempt to misuse such codes; (5) devices that bear or generate identification codes or password information, such as tokens or cards. must be tested initially and periodically to ensure that they function properly and have not been altered in an unauthorized manner.

III. Comments on the Proposed Rule

A. General Comments

1. Many comments expressed general support for the proposed rule. Noting that the proposal's regulatory approach incorporated several suggestions submitted by industry in comments on the ANPRM, a number of comments stated that the proposal is a good example of agency and industry cooperation in resolving technical issues

Several comments also noted that both industry and the agency can realize share the same concerns and are significant benefits by using electronic records and electronic signatures, such as increasing the speed of information exchange, cost savings from the reduced need for storage space, reduced errors, data integration/trending, product improvement, manufacturing process streamlining, improved process control, reduced vulnerability of electronic signatures to fraud and abuse, and job creation in industries involved in electronic record and electronic signature technologies.

One comment noted that, when part 11 controls are satisfied, electronic signatures and electronic records have advantages over paper systems, advantages that include: (1) Having automated databases that enable more advanced searches of information, thus obviating the need for manual searches of paper records; (2) permitting information to be viewed from multiple

perspectives; (3) permitting determination of trends, patterns, and behaviors; and (4) avoiding initial and subsequent document misfiling that may result from human error.

There were several comments on the part 11. These comments noted that the final regulations will be viewed as a standard by other Government agencies. and may strongly influence the direction of electronic record and electronic signature technologies. One comment said that FDA's position on electronic signatures/electronic records is one of the most pressing issues for the pharmaceutical industry and has a significant impact on the industry's future competitiveness. Another comment said that the rule constitutes an important milestone along the Nation's information superhighway.

FDA believes that the extensive industry input and collaboration that went into formulating the final rule is representative of a productive partnership that will facilitate the use of advanced technologies. The agency acknowledges the potential benefits to be gained by electronic record/ electronic signature systems. The agency expects that the magnitude of these benefits should significantly outweigh the costs of making these systems, through compliance with part 11, reliable, trustworthy, and compatible with FDA's responsibility to promote and protect public health. The agency is aware of the potential impact of the rule, especially regarding the need to accommodate and encourage new technologies while maintaining the agency's ability to carry out its mandate to protect public health. The agency is also aware that other Federal agencies addressing the same issues as FDA; the agency has held informal discussions with other Federal agencies and participated in several interagency groups on electronic records/electronic signatures and information technology issues. FDA looks forward to exchanging information and experience with other agencies for mutual benefit and to promote a consistent Federal policy on electronic records and signatures. The agency also notes that benefits, such as the ones listed by the comments, will help to offset any system modification costs that persons may incur to achieve compliance with part 11.

B. Regulations Versus Guidelines

2. Several comments addressed whether the agency's policy on electronic signatures and electronic records should be issued as a regulation

or recommended in a guideline. Most comments supported a regulation, citing characteristics of an electronic signature the need for a practical and workable approach for criteria to ensure that records can be stored in electronic form and are reliable, trustworthy, secure, accurate, confidential, and authentic. One comment specifically supported a single regulation covering all FDAregulated products to ensure consistent requirements across all product lines. Two comments asserted that the agency should only issue guidelines or "make the regulations voluntary." One of these comments said that by issuing regulations, the agency is shifting from creating tools to enhance communication (technological quality) to creating tools for enforcement (compliance quality).

The agency remains convinced, as expressed in the preamble to the proposed rule (59 FR 45160 at 45165), that a policy statement, inspection guide, or other guidance would be an inappropriate means for enunciating a comprehensive policy on electronic signatures and records. FDA has concluded that regulations are necessary to establish uniform, enforceable, baseline standards for accepting electronic signatures and records. The agency believes, however, that supplemental guidance documents would be useful to address controls in greater detail than would be appropriate for regulations. Accordingly, the agency anticipates issuing supplemental guidance as needed and will afford all interested parties the opportunity to

comment on the guidance documents. The need for regulations is underscored by several opinions expressed in the comments. For example, one comment asserted that it should be acceptable for supervisors to remove the signatures of their subordinates from signed records and replace them with their own signatures. Although the agency does not object to the use of a supervisor's signature to endorse or confirm a subordinate's actions, removal of an original signature is an action the agency views as falsification. Several comments also argued that an electronic signature should consist of only a password, that passwords need not be unique, that it is acceptable for people to use passwords associated with their personal lives (like the names of their children or their pets), and that passwords need only be changed every 2 years. FDA believes that such procedures would greatly increase the possibility that a password could be compromised and the chance that any resulting impersonation and/or falsification would continue for a long time. Therefore, an enforceable

regulation describing the acceptable appears necessary.

C. Flexibility and Specificity

3. Several comments addressed the flexibility and specificity of the proposed rule. The comments contended that agency acceptance of electronic records systems should not be based on any particular technology, but rather on the adequacy of the system controls under which they are created and managed. Some comments claimed that the proposed rule was overly prescriptive and that it should not specify the mechanisms to be used, but rather only require owners/users to design appropriate safeguards and validate them to reasonably ensure electronic signature integrity and authenticity. One comment commended the agency for giving industry the freedom to choose from a variety of electronic signature technologies, while another urged that the final rule be more specific in detailing software requirements for electronic records and electronic notebooks in research and testing laboratories.

The agency believes that the provisions of the final rule afford firms considerable flexibility while providing a baseline level of confidence that records maintained in accordance with the rule will be of high integrity. For example, the regulation permits a wide variety of existing and emerging electronic signature technologies, from use of identification codes in conjunction with manually entered passwords to more sophisticated biometric systems that may necessitate additional hardware and software. While requiring electronic signatures to be linked to their respective electronic records, the final rule affords flexibility in achieving that link through use of any appropriate means, including use of digital signatures and secure relational database references. The final rule accepts a wide variety of electronic record technologies, including those based on optical storage devices. In addition, as discussed in comment 40 of this document, the final rule does not establish numerical standards for levels of security or validation, thus offering firms flexibility in determining what levels are appropriate for their situations. Furthermore, while requiring operational checks, authority checks. and periodic testing of identifying devices, persons have the flexibility of conducting those controls by any suitable method. When the final rule calls for a certain control, such as

persons have the option of determining the frequency.

D. Controls for Electronic Systems Compared with Paper Systems

4. Two comments stated that any controls that do not apply to paperbased document systems and handwritten signatures should not apply to electronic record and signature systems unless those controls are needed to address an identified unique risk associated with electronic record systems. One comment expressed concern that FDA was establishing a much higher standard for electronic signatures than necessary.

In attempting to establish minimum criteria to make electronic signatures and electronic records trustworthy and reliable and compatible with FDA's responsibility to promote and protect public health (e.g., by hastening the availability of new safe and effective medical products and ensuring the safety of foods), the agency has attempted to draw analogies to handwritten signatures and paper records wherever possible. In doing so, FDA has found that the analogy does not always hold because of the differences between paper and electronic systems. The agency believes some of those differences necessitate controls that will be unique to electronic technology and that must be addressed on their own merits and not evaluated on the basis of their equivalence to controls governing paper documents.

The agency found that some of the comments served to illustrate the differences between paper and electronic record technologies and the need to address controls that may not generally be found in paper record systems. For example, several comments pointed out that electronic records built upon information databases, unlike paper records, are actually transient views or representations of information that is dispersed in various parts of the database. (The agency notes that the databases themselves may be geographically dispersed but linked by networks.) The same software that generates representations of database information on a screen can also misrepresent that information, depending upon how the software is written (e.g., how a query is prepared). In addition, database elements can easily be changed at any time to misrepresent information, without evidence that a change was made, and in a manner that destroys the original information. Finally, more people have periodic testing of identification tokens, potential access to electronic record

systems than may have access to paper records.

Therefore, controls are needed to ensure that representations of database information have been generated in a manner that does not distort data or hide noncompliant or otherwise bad information, and that database elements themselves have not been altered so as to distort truth or falsify a record. Such controls include: (1) Using timestamped audit trails of information written to the database, where such audit trails are executed objectively and automatically rather than by the person entering the information, and (2) limiting access to the database search software. Absent effective controls, it is very easy to falsify electronic records to render them indistinguishable from original, true records.

The traditional paper record, in comparison, is generally a durable unitized representation that is fixed in time and space. Information is recorded directly in a manner that does not require an intermediate means of interpretation. When an incorrect entry is made, the customary method of correcting FDA-related records is to cross out the original entry in a manner that does not obscure the prior data. Although paper records may be falsified, it is relatively difficult (in comparison to falsification of electronic records) to do so in a nondetectable manner. In the case of paper records that have been falsified, a body of evidence exists that can help prove that the records had been changed; comparable methods to detect falsification of electronic records have yet to be fully developed.

In addition, there are significant technological differences between traditional handwritten signatures (recorded on paper) and electronic signatures that also require controls unique to electronic technologies. For example, the traditional handwritten signature cannot be readily compromised by being "loaned" or "lost," whereas an electronic signature based on a password in combination with an identification code can be compromised by being "loaned" or "lost." By contrast, if one person attempts to write the handwritten signature of another person, the falsification would be difficult to execute and a long-standing body of investigational techniques would be available to detect the falsification. On the other hand, many electronic signatures are relatively easy to falsify and methods of falsification almost impossible to detect.

Accordingly, although the agency has attempted to keep controls for electronic falsify electronic signatures. One

record and electronic signatures analogous to traditional paper systems, it finds it necessary to establish certain controls specifically for electronic systems.

E. FDA Certification of Electronic Signature Systems

5. One comment requested FDA certification of what it described as a low-cost, biometric-based electronic signature system, one which uses dynamic signature verification with a parameter code recorded on magnetic stripe cards.

The agency does not anticipate the need to certify individual electronic signature products. Use of any electronic signature system that complies with the provisions of part 11 would form the basis for agency acceptance of the system regardless of what particular technology or brand is used. This approach is consistent with FDA's policy in a variety of program areas. The agency, for example, does not certify manufacturing equipment used to make drugs, medical devices, or food.

F. Biometric Electronic Signatures

6. One comment addressed the agency's statement in the proposed rule (59 FR 45160 at 45168) that the owner of a biometric/behavioral link could not lose or give it away. The comment stated that it was possible for an owner to "lend" the link for a file to be opened, as a collaborative fraudulent gesture, or to unwittingly assist a fraudulent colleague in an "emergency, a situation, the comment said, that was not unknown in the computer industry.

The agency acknowledges that such fraudulent activity is possible and that people determined to falsify records may find a means to do so despite whatever technology or preventive measures are in place. The controls in part 11 are intended to deter such actions, make it difficult to execute falsification by mishap or casual misdeed, and to help detect such alterations when they occur (see § 11.10 (introductory paragraph and especially §§ 11.10(j) and 11.200(b)).

G. Personnel Integrity

7. A few comments addressed the role of individual honesty and trust in ensuring that electronic records are reliable, trustworthy, and authentic. One comment noted that firms must rely confidentiality are consistent with the in large measure upon the integrity of their employees. Another said that subpart C of part 11, Electronic Signatures, appears to have been written with the belief that pharmaceutical manufacturers have an incentive to

comment expressed concern about possible signature falsification when an employee leaves a company to work elsewhere and the employee uses the electronic signature illegally.

The agency agrees that the integrity of any electronic signature/electronic record system depends heavily upon the honesty of employees and that most persons are not motivated to falsify records. However, the agency's experience with various types of records and signature falsification demonstrates that some people do falsify information under certain circumstances. Among those circumstances are situations in which falsifications can be executed with ease and have little likelihood of detection. Part 11 is intended to minimize the opportunities for readily executing falsifications and to maximize the chances of detecting falsifications.

Concerning signature falsification by former employees, the agency would expect that upon the departure of an employee, the assigned electronic signature would be "retired" to prevent the former employee from falsely using the signature.

H. Security of Industry Electronic Records Submitted to FDA

8. Several comments expressed concern about the security and confidentiality of electronic records submitted to FDA. One suggested that submissions be limited to such readonly formats as CD-ROM with raw data for statistical manipulation provided separately on floppy diskette. One comment suggested that in light of the proposed rule, the agency should review its own internal security procedures. Another addressed electronic records that may be disclosed under the Freedom of Information Act and expressed concern regarding agency deletion of trade secrets. One comment anticipated FDA's use of open systems to access industry records (such as medical device production and control records) and suggested that such access should be restricted to closed systems.

The agency is well aware of its legal obligation to maintain the confidentiality of trade secret information in its possession, and is committed to meet that obligation regardless of the form (paper or electronic) a record takes. The procedures used to ensure provisions of part 11. FDA is also examining other controls, such as use of digital signatures, to ensure submission integrity. To permit legitimate changes to be made, the agency does not believe that it is necessary to restrict submissions to those maintained in

read-only formats in all cases; each agency receiving unit retains the flexibility to determine whatever format is most suitable. Those intending to submit material are expected to consult with the appropriate agency receiving unit to determine the acceptable formats.

Although FDA access to electronic records on open systems maintained by firms is not anticipated in the near future, the agency believes it would be inappropriate to rule out such a procedure. Such access can be a valuable inspection tool and can enhance efficiencies by reducing the time investigators may need to be on site. The agency believes it is important to develop appropriate procedures and security measures in cooperation with industry to ensure that such access does not jeopardize data confidentiality or integrity.

I. Effective Date/Grandfathering

9. Several comments addressed the proposed effective date of the final rule, 90 days after publication in the Federal Register, and suggested potential exemptions (grandfathering) for systems now in use. Two comments requested an expedited effective date for the final rule. One comment requested an effective date at least 18 months after publication of the final rule to permit firms to modify and validate their systems. One comment expressed concern about how the rule, in general, will affect current systems, and suggested that the agency permit firms to continue to use existing electronic record systems that otherwise conform to good manufacturing or laboratory practices until these firms make major modifications to those systems or until 5 years have elapsed, whichever comes first. Several other comments requested grandfathering for specific sections of the proposed rule.

The agency has carefully considered the comments and suggestions regarding the final rule's effective date and has concluded that the effective date should be 5 months after date of publication in the Federal Register. The agency wishes to accommodate firms that are prepared now to comply with part 11 or will be prepared soon, so as to encourage and foster new technologies in a manner that ensures that electronic record and electronic signature systems are reliable, trustworthy, and compatible with FDA's responsibility to promote and protect public health. The agency believes that firms that have consulted with FDA before adopting new electronic record and electronic signature technologies (especially technologies that may impact on the ability of the agency to

conduct its work effectively) will need to make few, if any, changes to systems used to maintain records required by FDA.

The agency believes that the provisions of part 11 represent minimal standards and that a general exemption for existing systems that do not meet these provisions would be inappropriate and not in the public interest because such systems are likely to generate electronic records and electronic signatures that are unreliable, untrustworthy, and not compatible with FDA's responsibility to promote and protect public health. Such an exemption might, for example, mean that a firm could: (1) Deny FDA inspectional access to electronic record systems, (2) permit unauthorized access to those systems, (3) permit individuals to share identification codes and passwords, (4) permit systems to go unvalidated, and (5) permit records to be falsified in many ways and in a manner that goes undetected.

The agency emphasizes that these regulations do not require, but rather permit, the use of electronic records and signatures. Firms not confident that their electronic systems meet the minimal requirements of these regulations are free to continue to use traditional signatures and paper documents to meet recordkeeping requirements.

J. Comments by Electronic Mail (e-mail) and Electronic Distribution of FDA Documents

10. One comment specifically noted that the agency has accepted comments by e-mail and that this provides an additional avenue for public participation in the rulemaking process. Another comment encouraged FDA to expand the use of electronic media to provide information by such open systems as bulletin boards.

The agency intends to explore further the possibility of continuing to accept public comments by e-mail and other electronic means. For this current experiment, the agency received only one comment by e-mail. The comment that addressed this issue was, itself, transmitted in a letter. The agency recognizes the benefits of distributing information electronically, has expanded that activity, and intends to continue that expansion. Although only one e-mail comment was received, the agency does not attribute that low number to a lack of ability to send email because the agency received e-mail from 198 persons who requested the text of the proposed rule, including requests from people outside the United States.

K. Submissions by Facsimile (Fax)

11. One comment said that part 11 should include a provision for FDA acceptance of submissions by fax, such as import form FDA 2877. The comment noted that the U.S. Customs Service accepts fax signatures on its documents, and claimed that FDA's insistence on hard copies of form FDA 2877 is an impediment to imports.

The agency advises that part 11 permits the unit that handles import form FDA 2877 to accept that record in electronic form when it is prepared logistically to do so. As noted in the discussion on § 11.1(b) in comment 21 of this document, the agency recognizes that faxes can be in paper or electronic form, based on the capabilities of the sender and recipient.

L. Blood Bank Issues

12. Two comments addressed blood bank issues in the context of electronic records and electronic signatures and said the agency should clarify that part 11 would permit electronic crossmatching by a central blood center for individual hospitals. One comment stated that remote blood center and transfusion facilities should be permitted to rely on electronically communicated information, such as authorization for labeling/issuing units of blood, and that the electronic signature of the supervisor in the central testing facility releasing the product for labeling and issuance should be sufficient because the proposed rule guards against security and integrity problems.

One comment questioned whether, under part 11, electronic signatures would meet the signature requirements for the release of units of blood, and if there would be instances where a full signature would be required instead of a technician's identification. Another comment asserted that it is important to clarify how the term "batch" will be interpreted under part 11, and suggested that the term used in relation to blood products refers to a series of units of blood having undergone common manufacturing processes and recorded on the same computerized document. The comment contrasted this to FDA's current view that each unit of blood be considered a batch.

The agency advises that part 11 permits release records now in paper form to be in electronic form and traditional handwritten signatures to be electronic signatures. Under part 11, the name of the technician must appear in the record display or printout to clearly identify the technician. The appearance of the technician's identification code

alone would not be sufficient. The agency also advises that the definition of a "batch" for blood or other products is not affected by part 11, which addresses the trustworthiness and reliability of electronic records and electronic signatures, regardless of how a batch, which is the subject of those records and signatures, is defined.

M. Regulatory Flexibility Analysis

13. One comment said that, because part 11 will significantly impact a substantial number of small businesses. even though the impact would be beneficial, FDA is required to perform a regulatory flexibility analysis and should publish such an analysis in the Federal Register before a final rule is issued.

The comment states that the legislative history of the Regulatory Flexibility Act is clear that, "significant economic impact," as it appears at 5 U.S.C. 605(b) is neutral with respect to whether such impact is beneficial or adverse.

Contrary to the comment's assertion, the legislative history is not dispositive of this matter. It is well established that the task of statutory construction must begin with the actual language of the statute. (See Bailey v. United States, 116 S. Ct. 595, 597 (1996).) A statutory term must not be construed in isolation; a provision that may seem ambiguous in isolation is often clarified by the remainder of the statute. (See Dept. Of Revenue of Oregon v. ACF Industries, 114 S. Ct. 843, 850 (1994).) Moreover, it is a fundamental canon of statutory construction that identical terms within the same statute must bear the same meaning. (See Reno v. Koray, 115 S. Ct. 2021, 2026 (1995).)

In addition to appearing in 5 U.S.C. 605(b), the term "significant economic impact" appears elsewhere in the statute. The legislation is premised upon the congressional finding that alternative regulatory approaches may be available which "minimize the significant economic impact" of rules (5 U.S.C. 601 note). In addition, an initial regulatory flexibility analysis must describe significant regulatory alternatives that "minimize any significant economic impact" (5 U.S.C. 603(c)). Similarly, a final regulatory flexibility analysis must include a description of the steps the agency has taken to "minimize any significant economic impact" (5 U.S.C. 604(a)(5)). The term appeared as one of the elements of a final regulatory flexibility analysis, as originally enacted in 1980. (See Pub. L. No. 96-354, 3(a), 94 Stat. 1164, 1167 (1980) (formerly codified at 5 U.S.C. 604(a)(3)).) In addition, when

Congress amended the elements of a final regulatory flexibility analysis in 1996, it re-enacted the term, as set forth above. (See Pub. L. 104-121, 241(b), 110 Stat. 857, 865 (1996) (codified at 5 U.S.C.604(a)(5)).)

Unless the purpose of the statute was intended to increase the economic burden of regulations by minimizing positive or beneficial effects, 'significant economic impact'' cannot include such effects. Because it is beyond dispute that the purpose of the statute is not increasing economic burdens, the plain meaning of "significant economic impact" is clear and necessarily excludes beneficial or positive effects of regulations. Even where there are some limited contrary indications in the statute's legislative history, it is inappropriate to resort to legislative history to cloud a statutory text that is clear on its face. (See Ratzlaff v. United States, 114 S. Ct. 655, 662 (1994).) Therefore, the agency concludes that a final regulatory flexibility analysis is not required for this regulation or any regulation for which there is no significant adverse economic impact on small entities. Notwithstanding these conclusions, FDA has nonetheless considered the impact of the rule on small entities. (See section XVI. of this document.)

N. Terminology

14. One comment addressed the agency's use of the word "ensure" throughout the rule and argued that the agency should use the word "assure" rather than "ensure" because "ensure" means "to guarantee or make certain" whereas "assure" means "to make confident." The comment added that "assure" is also more consistent with terminology in other regulations.

The agency wishes to emphasize that it does not intend the word "ensure" to represent a guarantee. The agency prefers to use the word "ensure" because it means to make certain.

O. General Comments Regarding the Prescription Drug Marketing Act of 1987

15. Three comments addressed the use of handwritten signatures that are recorded electronically (SRE's) under part 11 and PDMA. One firm described its delivery information acquisition device and noted its use of time stamps to record when signatures are executed. The comments requested clarification that SRE's would be acceptable under the PDMA regulations. One comment assumed that subpart C of part 11 (Electronic Signatures) would not apply to SRE's, noting that it was not practical under PDMA (given the large number of by chance, a person's electronic

physicians who may be eligible to receive drug product samples) to use such alternatives as identification codes combined with passwords.

The agency advises that part 11 applies to handwritten signatures recorded electronically and that such signatures and their corresponding electronic records will be acceptable for purposes of meeting PDMA's requirements when the provisions of part 11 are met. Although subpart C of part 11 does not apply to handwritten signatures recorded electronically, the agency advises that controls related to electronic records (subpart B), and the general provisions of subpart A, do apply to electronic records in the context of PDMA. The agency emphasizes, however, that part 11 does not restrict PDMA signings to SRE's, and that organizations retain the option of using electronic signatures in conformance with part 11. Furthermore, the agency believes that the number of people in a given population or organization should not be viewed as an insurmountable obstacle to use of electronic signatures. The agency is aware, for example, of efforts by the American Society of Testing and Materials to develop standards for electronic medical records in which digital signatures could theoretically be used on a large scale.

P. Comments on the Unique Nature of Passwords

16. Several comments noted, both generally and with regard to §§ 11.100(a), 11.200(a), and 11.300, that the password in an electronic signature that is composed of a combination of password and identification code is not. and need not be, unique. Two comments added that passwords may be known to system security administrators who assist people who forget passwords and requested that the rule acknowledge that passwords need not be unique. One comment said that the rule should describe how uniqueness is to be determined.

The agency acknowledges that when an electronic signature consists of a combined identification code and password, the password need not be unique. It is possible that two persons in the same organization may have the same password. However, the agency believes that where good password practices are implemented, such coincidence would be highly unlikely. As discussed in section XIII. of this document in the context of comments on proposed § 11.300, records are less trustworthy and reliable if it is relatively easy for someone to deduce or execute,

signature where the identification code of the signature is not confidential and the password is easily guessed.

The agency does not believe that revising proposed §11.100(a) is necessary because what must remain unique is the electronic signature, which, in the case addressed by the comments, consists not of the password alone, but rather the password in combination with an identification code. If the combination is unique, then the electronic signature is unique.

The agency does not believe that it is necessary to describe in the regulations the various ways of determining uniqueness or achieving compliance with the requirement. Organizations thereby maintain implementation flexibility.

The agency believes that most system administrators or security managers would not need to know passwords to help people who have forgotten their own. This is because most administrators or managers have global computer account privileges to resolve such problems.

IV. Scope (§ 11.1)

17. One comment suggested adding a new paragraph to proposed § 11.1 that would exempt computer record maintenance software installed before the effective date of the final rule, and that would exempt electronic records maintained before that date. The comment argued that such exemptions were needed for economic and constitutional reasons because making changes to existing systems would be costly and because the imposition of additional requirements after the fact could be regarded as an ex post facto rule. The comment said firms have been using electronic systems that have demonstrated reliability and security for many years before the agency's publication of the ANPRM, and that the absence of FDA's objections in inspectional form FDA 483 was evidence of the agency's acceptance of the system.

As discussed in section III.I. of this document, the agency is opposed to "grandfathering" existing systems because such exemptions may perpetuate environments that provide opportunities for record falsification and impair FDA's ability to protect and promote public health. However, the agency wishes to avoid any confusion regarding the application of the provisions of part 11 to systems and electronic records in place before the rule's effective date. İmportant distinctions need to be made relative to an electronic record's creation, modification, and maintenance because various portions of part 11 address matters relating to these actions. Those provisions apply depending upon when a given electronic record is created, modified, or maintained.

Electronic records created before the effective date of this rule are not covered by part 11 provisions that relate to aspects of the record's creation, such as the signing of the electronic record. Those records would not, therefore, need to be altered retroactively. Regarding records that were first created before the effective date, part 11 provisions relating to modification of records, such as audit trails for record changes and the requirement that original entries not be obscured, would apply only to those modifications made on or after the rule's effective date, not to modifications made earlier. Likewise, maintenance provisions of part 11, such as measures to ensure that electronic records can be retrieved throughout their retention periods, apply to electronic records that are being maintained on or after the rule's effective date. The hardware and software, as well as operational procedures used on or after the rule's effective date, to create, modify, or maintain electronic records must comply with the provisions of part 11.

The agency does not agree with any suggestion that FDA endorsement or acceptance of an electronic record system can be inferred from the absence of objections in an inspection report. Before this rulemaking, FDA did not have established criteria by which it could determine the reliability and trustworthiness of electronic records and electronic signatures and could not sanction electronic alternatives when regulations called for signatures. A primary reason for issuing part 11 is to develop and codify such criteria. FDA will assess the acceptability of electronic records and electronic signatures created prior to the effective date of part 11 on a case-by-case basis.

18. One comment suggested that proposed § 11.1 exempt production of medical devices and in vitro diagnostic products on the grounds that the subject was already adequately addressed in the medical device CGMP regulations currently in effect in § 820.195 (21 CFR 820.195), and that additional regulations would be confusing and would limit compliance. the implication that all PDMA electronic records are, in fact, handled within closed systems. The classification of a system as open or closed in a particular situation. For example, the agency agrees that a close system exists where a drug producer's representative (the person responsible for the content of the electronic records are, in fact, handled within closed systems. The classification of a system as open or closed in a particular situation. For example, the agency agrees that a close system exists where a drug producer's representative (the person responsible content of the electronic records are, in fact, handled within closed systems. The classification of a system as open or closed in a particular situation. For example, the agency agrees that a close system exists where a drug producer's representative (the person responsible content of the closed system as open or closed in a particular situation. For example, the agency agrees that a close system exists where a drug producer's representative (the person responsible content of the closed system as open or closed in a particular situation. For example, the agency agrees that a close system exists where a drug producer's representative (the person responsible content of the closed system as open or closed in a particular situation depends on what is done in that situation.

The agency believes that part 11 complements, and is supportive of, the medical device CGMP regulations and the new medical device quality system regulation, as well as other regulations, and that compliance with one does not confound compliance with others. Before publication of the ANPRM, the

agency determined that existing regulations, including the medical device CGMP regulations, did not adequately address electronic records and electronic signatures. That determination was reinforced in the comments to the ANPRM, which focused on the need to identify what makes electronic records reliable. trustworthy, and compatible with FDA's responsibility to promote and protect public health. For example, the provision cited by the comment, § 820.195, states "When automated data processing is used for manufacturing or quality assurance purposes, adequate checks shall be designed and implemented to prevent inaccurate data output, input, and programming errors." This section does not address the many issues addressed by part 11, such as electronic signatures, record falsification, or FDA access to electronic records. The relationship between the quality system regulation and part 11 is discussed at various points in the preamble to the quality system regulation.

19. One comment asserted that for purposes of PDMA, the scope of proposed part 11 should be limited to require only those controls for assessing signatures in paper-based systems because physicians' handwritten signatures are executed to electronic records. The comment further asserted that, because drug manufacturers' representatives carry computers into physicians' offices (where the physicians then sign sample requests and receipts), only closed system controls should be needed.

The agency believes that, for purposes of PDMA, controls needed for electronic records bearing handwritten signatures are no different from controls needed for the same kinds of records and signatures used elsewhere, and that proposed § 11.1 need not make any such distinction.

In addition, the agency disagrees with the implication that all PDMA electronic records are, in fact, handled within closed systems. The classification of a system as open or closed in a particular situation depends on what is done in that situation. For example, the agency agrees that a closed representative (the person responsible for the content of the electronic record) has control over access to the electronic record system by virtue of possessing the portable computer and controlling who may use the computer to sign electronic records. However, should the firm's representative transfer copies of those records to a public online service that stores them for the drug firm's

subsequent retrieval, the agency considers such transfer and storage to be stating that part 11 does not apply to within an open system because access to paper records that are, or have been, the system holding the records is controlled by the online service, which is not responsible for the record's content. Activities in the first example would be subject to closed system controls and activities in the second example would be subject to open system controls.

20. One comment urged that proposed §11.1 contain a clear statement of what precedence certain provisions of part 11 have over other regulations.

The agency believes that such statements are found in § 11.1(c):

Where electronic signatures and their associated records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required under agency regulations unless specifically excepted by regulations * * *

and § 11.1(d) ("Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required."). These provisions clearly address the precedence of part 11 and the equivalence of electronic records and electronic signatures.

To further clarify the scope of the rule, FDA has revised § 11.1 to apply to

electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act (the act) and the Public Health Service Act (the PHS Act). This clarifies the point that submissions required by these statutes, but not specifically mentioned

in the Code of Federal Regulations (CFR), are subject to part 11.

21. Proposed § 11.1(b) stated that the regulations would apply to records in electronic form that are created, modified, maintained, or transmitted, under any records requirements set forth in Chapter I of Title 21. One comment suggested that the word "transmitted" be deleted from proposed § 11.1(b) because the wording would inappropriately apply to paper documents that are transmitted by fax. The comment noted that if the records are in machine readable form before or after transmission, they would still be covered by the revised wording.

The agency does not intend part 11 to apply to paper records even if such records are transmitted or received by fax. The agency notes that the records transmitted by fax may be in electronic form at the sender, the recipient, or both. Part 11 would apply whenever the record is in electronic form. To remedy the problem noted by the comment, the

agency has added a sentence to § 11.1(b) transmitted by electronic means.

22. One comment asked whether paper records created by computer would be subject to proposed part 11. The comment cited, as an example, the situation in which a computer system collects toxicology data that are printed out and maintained as "raw data."

Part 11 is intended to apply to systems that create and maintain electronic records under FDA's requirements in Chapter I of Title 21. even though some of those electronic records may be printed on paper at certain times. The key to determining part 11 applicability, under § 11.1(b), is the nature of the system used to create. modify, and maintain records, as well as the nature of the records themselves.

Part 11 is not intended to apply to computer systems that are merely incidental to the creation of paper records that are subsequently maintained in traditional paper-based systems. In such cases, the computer systems would function essentially like manual typewriters or pens and any signatures would be traditional handwritten signatures. Record storage and retrieval would be of the traditional "file cabinet" variety. More importantly, overall reliability, trustworthiness, and FDA's ability to access the records would derive primarily from wellestablished and generally accepted procedures and controls for paper records. For example, if a person were to use word processing software to generate a paper submission to FDA, part 11 would not apply to the computer system used to generate the submission. even though, technically speaking, an electronic record was initially created and then printed on paper.

When records intended to meet regulatory requirements are in electronic form, part 11 would apply to all the relevant aspects of managing those records (including their creation. signing, modification, storage, access, and retrieval). Thus, the software and hardware used to create records that are retained in electronic form for purposes of meeting the regulations would be subject to part 11.

Regarding the comment about "raw data," the agency notes that specific requirements in existing regulations may affect the particular records at issue, regardless of the form such records take. For example, "raw data," in the context of the good laboratory practices regulations (21 CFR part 58), include computer printouts from automated instruments as well as the same data recorded on magnetic media. In addition, regulations that cover data acquisition systems generally include requirements intended to ensure the trustworthiness and reliability of the collected data.

23. Several comments on proposed §11.1(b) suggested that the phrase "or archived and retrieved" be added to paragraph (b) to reflect more accurately a record's lifecycle.

The agency intended that record archiving and retrieval would be part of record maintenance, and therefore already covered by § 11.1(b). However, for added clarity, the agency has revised § 11.1(b) to add "archived and retrieved."

24. One comment suggested that, in describing what electronic records are within the scope of part 11, proposed § 11.1(b) should be revised by substituting "processed" for "modified" and "communicated" for "transmitted" because "communicated" reflects the fact that the information was dispatched and also received. The comment also suggested substituting "retained" for 'maintained," or adding the word "retained," because "maintain" does not necessarily convey the retention requirement.

The agency disagrees. The word "modified" better describes the agency's intent regarding changes to a record; the word "processed" does not necessarily infer a change to a record. FDA believes "transmitted" is preferable to "communicated" because "communicated" might infer that controls to ensure integrity and authenticity hinge on whether the intended recipient actually received the record. Also, as discussed in comment 22 of this document, the agency intends for the term "maintain" to include records retention.

25. Two comments suggested that proposed § 11.1(b) explicitly state that part 11 supersedes all references to handwritten signatures in 21 CFR parts 211 through 226 that pertain to a drug, and in 21 CFR parts 600 through 680 that pertain to biological products for human use. The comments stated that the revision should clarify coverage and permit blood centers and transfusion services to take full advantage of electronic systems that provide process controls.

The agency does not agree that the revision is necessary because, under § 11.1(b) and (c), part 11 permits electronic records or submissions under all FDA regulations in Chapter I of Title 21 unless specifically excepted by future regulations.

26. Several comments expressed concern that the proposed rule had inappropriately been expanded in scope

from the ANPRM to address electronic records as well as electronic signatures. One comment argued that the scope of part 11 should be restricted only to to be signed, witnessed, or initialed, and that the agency should not require electronic records to contain electronic signatures where the corresponding paper records are not required to be signed.

The agency disagrees with the assertion that part 11 should address only electronic signatures and not electronic records for several reasons. First, based on comments on the ANPRM, the agency is convinced that the reliability and trustworthiness of electronic signatures depend in large measure on the reliability and trustworthiness of the underlying electronic records. Second, the agency has concluded that electronic records, like paper records, need to be trustworthy, reliable, and compatible with FDA's responsibility to promote and protect public health regardless of whether they are signed. In addition, records falsification is an issue with respect to both signed and unsigned records. Therefore, the agency concludes that although the ANPRM focused primarily on electronic signatures, expansion of the subject to electronic records in the proposed rule was fully justified.

The agency stresses that part 11 does not require that any given electronic record be signed at all. The requirement that any record bear a signature is contained in the regulation that mandates the basic record itself. Where records are signed, however, by virtue of meeting a signature requirement or otherwise, part 11 addresses controls and procedures intended to help ensure the reliability and trustworthiness of those signatures.

27. Three comments asked if there were any regulations, including CGMP regulations, that might be excepted from part 11 and requested that the agency identify such regulations.

FDA, at this time, has not identified any current regulations that are specifically excepted from part 11. However, the agency believes it is prudent to provide for such exceptions should they become necessary in the future. It is possible that, as the agency's experience with part 11 increases. certain records may need to be limited to paper if there are problems with the electronic versions of such records.

28. One comment requested clarification of the meaning of the term "general signings" in proposed § 11.1(c), and said that the distinction between "full handwritten" signatures and

"initials" is unnecessary because handwritten includes initials in all common definitions of handwritten signature. The comment also suggested those records that are currently required changing the term "equivalent" to "at least equivalent" because electronic signatures are not precise equivalents of handwritten signatures and computerbased signatures have the potential of being more secure.

The agency advises that current regulations that require records to be signed express those requirements in different ways depending upon the agency's intent and expectations. Some regulations expressly state that records must be signed using "full handwritten" signatures, whereas other regulations state that records must be "signed or initialed;" still other regulations implicitly call for some kind of signing by virtue of requiring record approvals or endorsements. This last broad category is addressed by the term "general signings" in § 11.1(c).

Where the language is explicit in the regulations, the means of meeting the requirement are correspondingly precise. Therefore, where a regulation states that a signature must be recorded as "full handwritten," the use of initials is not an acceptable substitute. Furthermore, under part 11, for an electronic signature to be acceptable in place of any of these signings, the agency only needs to consider them as equivalent; electronic signatures need not be superior to those other signings to be acceptable.

29. Several comments requested clarification of which FDA records are required to be in paper form, and urged the agency to allow and promote the use of electronic records in all cases. One comment suggested that proposed § 11.1(d) be revised to read, in part, * * * unless the use of electronic records is specifically prohibited."

The agency intends to permit the use of electronic records required to be maintained but not submitted to the agency (as noted in § 11.2(a)) provided that the requirements of part 11 are met and paper records are not specifically required. The agency also wishes to encourage electronic submissions, but is limited by logistic and resource constraints. The agency is unaware of "maintenance records" that are currently explicitly required to be in paper form (explicit mention of paper is generally unnecessary because, at the time most regulations were prepared, only paper-based technologies were in use) but is providing for that possibility in the future. For purposes of part 11, the agency will not consider that a regulation requires "maintenance" records to be in paper form where the

regulation is silent on the form the record must take. FDA believes that the comments' suggested wording does not offer sufficient advantages to adopt the change.

However, to enable FDA to accept as many electronic submissions as possible, the agency is amending § 11.1(b) to include those submissions that the act and the PHS Act specifically require, even though such submissions may not be identified in agency regulations. An example of such records is premarket submissions for Class I and Class II medical devices, required by section 510(k) of the act (21 U.S.C.

360(k)). 30. Several comments addressed various aspects of the proposed requirement under § 11.1(e) regarding FDA inspection of electronic record systems. Several comments objected to the proposal as being too broad and going beyond the agency's legal inspectional authority. One comment stated that access inferred by such inspection may include proprietary financial and sales data to which FDA is not entitled. Another comment suggested adding the word "authorized" before "inspection." Some comments suggested revising proposed § 11.1(e) to limit FDA inspection only to the electronic records and electronic signatures themselves, thus excluding inspection of hardware and software used to manage those records and signatures. Other comments interpreted proposed § 11.1(e) as requiring them to keep supplanted or retired hardware and software to enable FDA inspection of those outdated systems.

The agency advises that FDA inspections under part 11 are subject to the same legal limitations as FDA inspections under other regulations. The agency does not believe it is necessary to restate that limitation by use of the suggested wording. However, within those limitations, it may be necessary to inspect hardware and software used to generate and maintain electronic records to determine if the provisions of part 11 are being met. Inspection of resulting records alone would be insufficient. For example, the agency may need to observe the use and maintenance of tokens or devices that contain or generate identification information. Likewise, to assess the adequacy of systems validation, it is generally necessary to inspect hardware that is being used to determine, among other things, if it matches the system documentation description of such hardware. The agency has concluded that hardware and software used to generate and maintain electronic records and signatures are "pertinent

equipment" within the meaning of section 704 of the act (21 U.S.C. 374).

The agency does not expect persons to maintain obsolete and supplanted computer systems for the sole purpose of enabling FDA inspection. However, the agency does expect firms to maintain and have available for inspection documentation relevant to those systems, in terms of compliance with part 11, for as long as the electronic records are required by other relevant regulations. Persons should also be mindful of the need to keep appropriate computer systems that are capable of reading electronic records for as long as those records must be retained. In some instances, this may mean retention of otherwise outdated and supplanted systems, especially where the old records cannot be converted to a form readable by the newer systems. In most cases, however, FDA believes that where electronic records are accurately and completely transcribed from one system to another, it would not be necessary to maintain older systems.

31. One comment requested that proposed part 11 be revised to give examples of electronic records subject to FDA inspection, including pharmaceutical and medical device production records, in order to reduce the need for questions.

The agency does not believe that it is necessary to include examples of records it might inspect because the addition of such examples might raise questions about the agency's intent to inspect other records that were not identified.

32. One comment said that the regulation should state that certain security related information, such as private keys attendant to cryptographic implementation, is not intended to be subject to inspection, although procedures related to keeping such keys confidential can be subject to inspection.

The agency would not routinely seek to inspect especially sensitive information, such as passwords or private keys, attendant to security systems. However, the agency reserves the right to conduct such inspections. consistent with statutory limitations, to enforce the provisions of the act and related statutes. It may be necessary, for example, in investigating cases of suspected fraud, to access and determine passwords and private keys. in the same manner as the agency may obtain specimens of handwritten signatures ("exemplars"). Should there be any reservations about such inspections, persons may, of course,

change their passwords and private keys clarify the slash in the phrase "records/ after FDA inspection.

33. One comment asked how persons were expected to meet the proposed requirement, under § 11.1(e), that computer systems be readily available for inspection when such systems include geographically dispersed networks. Another comment said FDA investigators should not be permitted to access industry computer systems as part of inspections because investigators would be untrained users.

The agency intends to inspect those parts of electronic record or signature systems that have a bearing on the trustworthiness and reliability of electronic records and electronic signatures under part 11. For geographically dispersed systems, inspection at a given location would extend to operations, procedures, and controls at that location, along with interaction of that local system with the wider network. The agency would inspect other locations of the network in a separate but coordinated manner. much the same way the agency currently conducts inspections of firms that have multiple facilities in different parts of the country and outside of the United States.

FDA does not believe it is reasonable to rule out computer system access as part of an inspection of electronic record or signature systems. Historically, FDA investigators observe the actions of establishment employees, and (with the cooperation of establishment management) sometimes request that those employees perform some of their assigned tasks to determine the degree of compliance with established requirements. However, there may be times when FDA investigators need to access a system directly. The agency is aware that such access will generally require the cooperation of and, to some degree, instruction by the firms being inspected. As new, complex technologies emerge, FDA will need to develop and implement new inspectional methods in the context of those technologies.

V. Implementation (§ 11.2)

34. Proposed § 11.2(a) stated that for "records required by chapter I of this title to be maintained, but not submitted to the agency, persons may use electronic records/signatures in lieu of paper records/conventional signatures, in whole or in part, * * *."

of the term "conventional signatures." One comment suggested that the term "traditional signatures" be used instead. undue burdens. However, the agency Another suggested rewording in order to expects persons to consult with the

signatures.'

The agency advises that the term "conventional signature" means handwritten signature. The agency agrees that the term "traditional signature" is preferable, and has revised § 11.2(a) and (b) accordingly. The agency has also clarified proposed §11.2(a) by replacing the slash with the word "or."

35. One comment asked if the term 'persons' in proposed § 11.2(b) would include devices because computer systems frequently apply digital time stamps on records automatically. without direct human intervention.

The agency advises that the term "persons" excludes devices. The agency does not consider the application of a time stamp to be the application of a signature.

36. Proposed § 11.2(b)(2) provides conditions under which electronic records or signatures could be submitted to the agency in lieu of paper. One condition is that a document, or part of a document, must be identified in a public docket as being the type of submission the agency will accept in electronic form. Two comments addressed the nature of the submissions to the public docket. One comment asked that the agency provide specifics. such as the mechanism for updating the docket and the frequency of such updates. One comment suggested making the docket available to the public by electronic means. Another comment suggested that acceptance procedures be uniform among agency units and that electronic mail be used to hold consultations with the agency. One comment encouraged the agency units receiving the submissions to work closely with regulated industry to ensure that no segment of industry is unduly burdened and that agency guidance is widely accepted.

The agency intends to develop efficient electronic records acceptance procedures that afford receiving units sufficient flexibility to deal with submissions according to their capabilities. Although agencywide uniformity is a laudable objective, to attain such flexibility it may be necessary to accommodate some differences among receiving units. The agency considers of primary importance, however, that all part 11 submissions be trustworthy, reliable, and in keeping with FDA regulatory activity. The agency expects to work Two comments requested clarification closely with industry to help ensure that the mechanics and logistics of accepting electronic submissions do not pose any

intended receiving units on the technical aspects of the submission, such as media, method of transmission. file format, archiving needs, and technical protocols. Such consultations will ensure that submissions are compatible with the receiving units' capabilities. The agency has revised proposed § 11.2(b)(2) to clarify this expectation.

Regarding the public docket, the agency is not at this time establishing a fixed schedule for updating what types of documents are acceptable for submission because the agency expects the docket to change and grow at a rate that cannot be predicted. The agency may, however, establish a schedule for updating the docket in the future. The agency agrees that making the docket available electronically is advisable and will explore this option. Elsewhere in this issue of the Federal Register, FDA is providing further information on this docket.

VI. Definitions (§ 11.3)

37. One comment questioned the incorporation in proposed § 11.3(a) of definitions under section 201 of the act (21 U.S.C. 321), noting that other FDA regulations (such as 21 CFR parts 807 and 820) lack such incorporation, and suggested that it be deleted.

The agency has retained the incorporation by reference to definitions under section 201 of the act because those definitions are applicable to part

38. One comment suggested adding the following definition for the term "digital signature:" "data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g., by the recipient."

The agency agrees that the term digital signature should be defined and has added new § 11.3(b)(5) to provide a definition for digital signature that is consistent with the Federal Information Processing Standard 186, issued May 19, 1995, and effective December 1, 1995, by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST). Generally, a digital signature is "an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.' FDA advises that the set of rules and parameters is established in each digital signature standard.

39. Several comments suggested various modifications of the proposed and suggested revisions that would exclude typing a password or identification code which, the comments noted, is a repeatable action. The comments suggested that actions be unique and measurable to meet the intent of a biometric method.

The agency agrees that the proposed definition of biometric/behavioral links should be revised to clarify the agency's intent that repetitive actions alone, such as typing an identification code and password, are not considered to be biometric in nature. Because comments also indicated that it would be preferable to simplify the term, the agency is changing the term "biometric/ behavioral link" to "biometrics." Accordingly, § 11.3(b)(3) defines the term "biometrics" to mean "a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.'

40. One comment said that the agency should identify what biometric methods are acceptable to verify a person's identity and what validation acceptance criteria the agency has used to determine that biometric technologies are superior to other methods, such as use of identification codes and passwords.

The agency believes that there is a wide variety of acceptable technologies, regardless of whether they are based on biometrics, and regardless of the particular type of biometric mechanism that may be used. Under part 11, electronic signatures that employ at least two distinct identification components such as identification codes and passwords, and electronic signatures based on biometrics are equally acceptable substitutes for traditional handwritten signatures. Furthermore, all electronic record systems are subject to the same requirements of subpart B of part 11 regardless of the electronic signature technology being used. These provisions include requirements for validation.

Regarding the comment's suggestion that FDA apply quantitative acceptance criteria, the agency is not seeking to set specific numerical standards or statistical performance criteria in determining the threshold of acceptability for any type of technology. If such standards were to be set for biometrics-based electronic signatures, similar numerical performance and reliability requirements would have to be applied to other technologies as well. The agency advises, however, that the differences between system controls for

definition of biometric/behavioral links, biometrics-based electronic signatures and other electronic signatures are a result of the premise that biometricsbased electronic signatures, by their nature, are less prone to be compromised than other methods such as identification codes and passwords. Should it become evident that additional controls are warranted for biometrics-based electronic signatures, the agency will propose to revise part 11 accordingly.

41. Proposed § 11.3(b)(4) defined a closed system as an environment in which there is communication among multiple persons, and where system access is restricted to people who are part of the organization that operates the system

Many comments requested clarification of the term "organization" and stated that the rule should account for persons who, though not strictly employees of the operating organization, are nonetheless obligated to it in some manner, or who would otherwise be granted system access by the operating organization. As examples of such persons, the comments cited outside contractors, suppliers, temporary employees, and consultants. The comments suggested a variety of alternative wording, including a change of emphasis from organizational membership to organizational control over system access. One comment requested clarification of whether the rule intends to address specific disciplines within a company.

Based on the comments, the agency has revised the proposed definition of closed system to state "an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system." The agency agrees that the most important factor in classifying a system as closed or open is whether the persons responsible for the content of the electronic records control access to the system containing those records. A system is closed if access is controlled by persons responsible for the content of the records. If those persons do not control such access, then the system is open because the records may be read. modified, or compromised by others to the possible detriment of the persons responsible for record content. Hence, those responsible for the records would need to take appropriate additional measures in an open system to protect those records from being read, modified, destroyed, or otherwise compromised by unauthorized and potentially unknown parties. The agency does not believe it is necessary to codify the basis or criteria for authorizing system access, such as existence of a fiduciary

responsibility or contractual relationship. By being silent on such criteria, the rule affords maximum flexibility to organizations by permitting them to determine those criteria for themselves.

42. Concerning the proposed definition of closed system, one comment suggested adding the words "or devices" after "persons" because communications may involve nonhuman entities.

The agency does not believe it is necessary to adopt the suggested revision because the primary intent of the regulation is to address communication among humans, not devices

43. One comment suggested defining a closed system in terms of functional characteristics that include physical access control, having professionally written and approved procedures with employees and supervisors trained to follow them, conducting investigations when abnormalities may have occurred, and being under legal obligation to the organization responsible for operating the system.

The agency agrees that the functional characteristics cited by the comment are appropriate for a closed system, but has decided that it is unnecessary to include them in the definition. The functional characteristics themselves, however, such as physical access controls, are expressed as requirements elsewhere in part 11.

44. Two comments said that the agency should regard as closed a system in which dial-in access via public phone lines is permitted, but where access is authorized by, and under the control of, the organization that operates the system.

The agency advises that dial-in access over public phone lines could be considered part of a closed system where access to the system that holds the electronic records is under the control of the persons responsible for the content of those records. The agency cautions, however, that, where an organization's electronic records are stored on systems operated by third parties, such as commercial online services, access would be under control of the third parties and the agency would regard such a system as being open. The agency also cautions that, by permitting access to its systems by public phone lines, organizations lose the added security that results from restricting physical access to computer terminal and other input devices. In such cases, the agency believes firms would be prudent to implement additional security measures above and beyond those controls that the

organization would use if the access device was within its facility and commensurate with the potential consequences of such unauthorized access. Such additional controls might include, for example, use of input device checks, caller identification checks (phone caller identification), call backs, and security cards.

45. Proposed § 11.3(b)(5) defined electronic record as a document or writing comprised of any combination of text, graphic representation, data. audio information, or video information, expressed as "foot candles," and (more that is created, modified, maintained, or transmitted in digital form by a computer or related system. Many comments suggested revising the proposed definition to reflect more accurately the nature of electronic records and how they differ from paper records. Some comments suggested distinguishing between machine readable records and paper records created by machine. Some comments noted that the term "document or writing" is inappropriate for electronic records because electronic records could form of computer data compilation of be any combination of pieces of information assembled (sometimes on a transient basis) from many noncontiguous places, and because the term does not accurately describe such electronic information as raw data or voice mail. Two comments suggested that the agency adopt definitions of electronic record that were established. respectively, by the United Nations Commission on International Trade Law (UNCITRAL) Working Group on Electronic Data Interchange, and the American National Standards Institute/ Institute of Electrical and Electronic Engineers Software Engineering (ANSI/ IEEE) Standard (729-1983).

The agency agrees with the suggested revisions and has revised the definition of "electronic record" to emphasize this unique nature and to clarify that the agency does not regard a paper record to be an electronic record simply because it was created by a computer system. The agency has removed "document or writing" from this definition and elsewhere in part 11 for the sake of clarity, simplicity, and consistency.

However, the agency believes it is preferable to adapt or modify the words "document" and "writing" to electronic technologies rather than discard them entirely from the lexicon of computer technology. The agency is aware that the terms "document" and "electronic document" are used in contexts that clearly do not intend to describe paper. Therefore, the agency considers the terms "electronic record" and "electronic document" to be generally

synonymous and may use the terms "writing," "electronic document." or "document" in other publications to describe records in electronic form. The agency believes that such usage is a prudent conservation of language and is consistent with the use of other terms and expressions that have roots in older technologies, but have nonetheless been adapted to newer technologies. Such terms include telephone "dialing," internal combustion engine "horse power," electric light luminance relevant to computer technology) execution of a "carriage return."

Accordingly, the agency has revised the definition of electronic record to mean "any combination of text. graphics, data, audio, pictorial, or other information representation in digital form that is created, modified. maintained, archived, retrieved, or distributed by a computer system."

46. Proposed § 11.3(b)(6) defined an electronic signature as the entry in the form of a magnetic impulse or other any symbol or series of symbols, executed, adopted or authorized by a person to be the legally binding equivalent of the person's handwritten signature. One comment supported the definition as proposed, noting its consistency with dictionary definitions (Random House Dictionary of the English Language, Unabridged Ed. 1983, and American Heritage Dictionary, 1982). Several other comments. however, suggested revisions. One comment suggested replacing "electronic signature" with "computer based signature," "authentication," or "computer based authentication" because "electronic signature" is imprecise and lacks clear and recognized meaning in the information security and legal professions. The comment suggested a definition closer to the UNCITRAL draft definition:

(1) [a] method used to identify the originator of the data message and to indicate the originator's approval of the information contained therein; and (2) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all circumstances, including any agreement between the originator and the addressee of the data message.

One comment suggested replacing "electronic signature" with "electronic identification" or "electronic authorization" because the terms include many types of technologies that are not easily distinguishable and because the preamble to the proposed rule gave a rationale for using "electronic signature" that was too "esoteric for practical consideration."

The agency disagrees that "electronic signature" as proposed should be replaced with other terms and definitions. As noted in the preamble to the proposed rule, the agency believes that it is vital to retain the word "signature" to maintain the equivalence and significance of various electronic technologies with the traditional handwritten signature. By not using the word "signature," people may treat the electronic alternatives as less important, less binding, and less in need of controls to prevent falsification. The agency also believes that use of the word signature provides a logical bridge between paper and electronic technologies that facilitates the general transition from paper to electronic environments. The term helps people comply with current FDA regulations that specifically call for signatures. Nor does the agency agree that this reasoning is beyond the reach of practical consideration.

The agency declines to accept the suggested UNCITRAL definition because it is too narrow in context in that there is not always a specified message addressee for electronic records required by FDA regulations (e.g., a batch production record does not have a specific "addressee").

47. Concerning the proposed definition of "electronic signature," other comments suggested deletion of the term "magnetic impulse" to render the term media neutral and thus allow for such alternatives as an optical disk. Comments also suggested that the term "entry" was unclear and recommended its deletion. Two comments suggested revisions that would classify symbols as an electronic signature only when they are committed to permanent storage because not every computer entry is a signature and processing to permanent storage must occur to indicate

completion of processing. The agency advises that the proposal did not limit electronic signature recordings to "magnetic impulse" because the proposed definition added, "or other form of computer data * * *. However, in keeping with the agency's intent to accept a broad range of technologies, the terms "magnetic impulse" and "entry" have been removed from the proposed definition. The agency believes that recording of computer data to "permanent" storage is not a necessary or warranted qualifier because it is not relevant to the concept of equivalence to a handwritten signature. In addition, use of the qualifier regarding permanent storage could impede detection of falsified records if, for example, the signed falsified record was deleted after a

predetermined period (thus, technically not recorded to "permanent" storage). An individual could disavow a signature because the record had ceased to exist.

For consistency with the proposed definition of handwritten signature, and to clarify that electronic signatures are those of individual human beings, and not those of organizations (as included in the act's definition of "person"), FDA is changing "person" to "individual" in the final rule.

Accordingly, § 11.3(b)(7) defines electronic signature as a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

48. Proposed § 11.3(b)(7) (redesignated § 11.3(b)(8) in the final rule) defined "handwritten signature" as the name of an individual, handwritten in script by that individual, executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The proposed definition also stated that the scripted name, while conventionally applied to paper, may also be applied to other devices which capture the written name.

Many comments addressed this proposed definition. Two comments suggested that it be deleted on the grounds it is redundant and that, when handwritten signatures are recorded electronically, the result fits the definition of electronic signature.

The agency disagrees that the definition of handwritten signature should be deleted. In stating the criteria under which electronic signatures may be used in place of traditional handwritten signatures, the agency believes it is necessary to define handwritten signature. In addition, the agency believes that it is necessary to distinguish handwritten signatures from electronic signatures because, with handwritten signatures, the traditional act of signing one's name is preserved. Although the handwritten signature recorded electronically and electronic signatures, as defined in part 11, may both ultimately result in magnetic impulses or other forms of computerized symbol representations, the means of achieving those recordings and, more importantly, the controls needed to ensure their reliability and trustworthiness are quite different. In addition, the agency believes that a definition for handwritten signature is warranted to accommodate persons who wish to implement record systems that

are combinations of paper and electronic technologies.

49. Several comments suggested replacing the reference to "scripted name" in the proposed definition of handwritten signature with "legal mark" so as to accommodate individuals who are physically unable to write their names in script. The comments asserted that the term "legal mark" would bring the definition to closer agreement with generally recognized legal interpretations of signature.

The agency agrees and has added the term "legal mark" to the definition of handwritten signature.

50. One comment recommended that the regulation state that, when the handwritten signature is not the result of the act of signing with a writing or marking instrument, but is applied to another device that captures the written name, a system should verify that the owner of the signature has authorized the use of the handwritten signature.

The agency declines to accept this comment because, if the act of signing or marking is not preserved, the type of signature would not be considered a handwritten signature. The comment appears to be referring to instances in which one person authorizes someone else to use his or her stamp or device. The agency views this as inappropriate when the signed record does not clearly show that the stamp owner did not actually execute the signature. As discussed elsewhere in this preamble, the agency believes that where one person authorizes another to sign a document on his or her behalf, the second person must sign his or her own name (not the name of the first person) along with some notation that, in doing so, he or she is acting in the capacity, or on behalf, of the first person.

51. One comment suggested that where handwritten signatures are captured by devices, there should be a register of manually written signatures to enable comparison for authenticity and the register also include the typed names of individuals.

The agency agrees that the practice of establishing a signature register has merit, but does not believe that it is necessary, in light of other part 11 controls. As noted elsewhere in this preamble (in the discussion of proposed § 11.50), the agency agrees that human readable displays of electronic records must display the name of the signer.

52. Several comments suggested various editorial changes to the proposed definition of handwritten signature including: (1) Changing the word "also" in the last sentence to "alternatively," (2) clarifying the

difference between the words "individual" and "person," (3) deleting the words "in a permanent form," and (4) changing "preserved" to "permitted." One comment asserted that the last sentence of the proposed definition was unnecessary.

The agency has revised the definition of handwritten signature to clarify its intent and to keep the regulation as flexible as possible. The agency believes that the last sentence of the proposed definition is needed to address devices that capture handwritten signatures. The agency is not adopting the suggestion that the word "preserved" be changed to "permitted" because "preserved" more accurately states the agency's intent and is a qualifier to help distinguish handwritten signatures from others. The agency advises that the word "individual" is used, rather than "person," because the act's definition of person extends beyond individual human beings to companies and partnerships. The agency has retained the term "permanent" to discourage the use of pencils, but recognizes that 'permanent'' does not mean eternal.

53. One comment asked whether a signature that is first handwritten and then captured electronically (e.g., by scanning) is an electronic signature or a handwritten signature, and asked how a handwritten signature captured electronically (e.g., by using a stylussensing pad device) that is affixed to a paper copy of an electronic record would be classified.

FDA advises that when the act of signing with a stylus, for example, is preserved, even when applied to an electronic device, the result is a handwritten signature. The subsequent printout of the signature on paper would not change the classification of the original method used to execute the signature.

54. One comment asserted that a handwritten signature recorded electronically should be considered to be an electronic signature, based on the medium used to capture the signature. The comment argued that the word signature should be limited to paper technology.

The agency disagrees and believes it is important to classify a signature as handwritten based upon the preserved action of signing with a stylus or other writing instrument.

55. One comment asked if the definition of handwritten signature encompasses handwritten initials.

The agency advises that, as revised, the definition of handwritten signature includes handwritten initials if the initials constitute the legal mark executed or adopted with the present

intention to authenticate a writing in a permanent form, and where the method of recording such initials involves the act of writing with a pen or stylus.

56. Proposed § 11.3(b) (8) (redesignated as § 11.3(b) (9) in the final rule) defined an open system as an environment in which there is electronic communication among multiple persons, where system access extends to people who are not part of the organization that operates the system.

Several comments suggested that, for simplicity, the agency define "open system" as any system that does not meet the definition of a closed system. One comment suggested that the definition be deleted on the grounds it is redundant, and that it is the responsibility of individual firms to take appropriate steps to ensure the validity and security of applications and information, regardless of whether systems are open or closed. Other comments suggested definitions of "open system" that were opposite to what they suggested for a closed system.

The agency has revised the definition of open system to mean "an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system." The agency believes that, for clarity, the definition should stand on its own rather than as any system that is not closed. The agency rejects the suggestion that the term need not be defined at all because FDA believes that controls for open systems merit distinct provisions in part 11 and defining the term is basic to understanding which requirements apply to a given system. The agency agrees that companies have the responsibility to take steps to ensure the validity and security of their applications and information. However, FDA finds it necessary to establish part 11 as minimal requirements to help ensure that those steps are, in fact, acceptable.

VII. Electronic Records—Controls for Closed Systems (§ 11.10)

The introductory paragraph of proposed § 11.10 states that:

Closed systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. * * *

The rest of the section lists specific

procedures and controls.
57. One comment expressed full support for the list of proposed controls, calling them generally appropriate and

stated that the agency is correctly accommodating the fluid nature of various electronic record and electronic signature technologies. Another comment, however, suggested that controls should not be implemented at the time electronic records are first created, but rather only after a document is accepted by a company.

The agency disagrees with this suggestion. To ignore such controls at a stage before official acceptance risks compromising the record. For example, if "preacceptance" records are signed by technical personnel, it is vital to ensure the integrity of their electronic signatures to prevent record alteration. The need for such integrity is no less important at preacceptance stages than at later stages when managers officially accept the records. The possibility exists that some might seek to disavow, or avoid FDA examination of, pertinent records by declaring they had not been formally "accepted." In addition, FDA routinely can and does inspect evolving paper documents (e.g., standard operating procedures and validation protocols) even though they have yet to receive a firm's final acceptance.

58. One comment said proposed § 11.10 contained insufficient requirements for firms to conduct periodic inspection and monitoring of their own systems and procedures to ensure compliance with the regulations. The comment also called for a clear identification of the personnel in a firm who would be responsible for system implementation, operation, change control, and monitoring.

The agency does not believe it is necessary at this time to codify a selfauditing requirement, as suggested by the comment. Rather, the agency intends to afford organizations flexibility in establishing their own internal mechanisms to ensure compliance with part 11. Self-audits, however, may be considered as a general control, within the context of the introductory paragraph of § 11.10. The agency encourages firms to conduct such audits periodically as part of an overall approach to ensure compliance with FDA regulations generally. Likewise, the agency does not believe it is necessary or practical to codify which individuals in an organization should be responsible for compliance with various provisions of part 11. However, ultimate responsibility for part 11 will generally rest with persons responsible for electronic record content, just as responsibility for compliance with paper record requirements generally lies with those responsible for the record's

59. Several comments interpreted proposed § 11.10 as applying all procedures and controls to closed systems and suggested revising it to permit firms to apply only those procedures and controls they deem necessary for their own operations. because some requirements are excessive in some cases.

The agency advises that, where a given procedure or control is not intended to apply in all cases, the language of the rule so indicates. Specifically, use of operational checks (§ 11.10(f)) and device checks (§ 11.10(h)) is not required in all cases. The remaining requirements do apply in all cases and are, in the agency's opinion, the minimum needed to ensure the trustworthiness and reliability of electronic record systems. In addition, certain controls that firms deem adequate for their routine internal operations might nonetheless leave records vulnerable to manipulation and, thus, may be incompatible with FDA's responsibility to protect public health. The suggested revision would effectively permit firms to implement various controls selectively and possibly shield records from FDA, employ unqualified personnel, or permit employees to evade responsibility for fraudulent use of their electronic signatures.

The agency believes that the controls in § 11.10 are vital, and notes that almost all of them were suggested by comments on the ANPRM. The agency believes the wording of the regulation nonetheless permits firms maximum flexibility in how to meet those

requirements.

60. Two comments suggested that the word "confidentiality" in the introductory paragraph of proposed § 11.10 be deleted because it is unnecessary and inappropriate. The comments stated that firms should determine if certain records need to be confidential, and that as long as records could not be altered or deleted without appropriate authority, it would not matter whether they could read the records.

The agency agrees that not all records required by FDA need to be kept confidential within a closed system and has revised the reference in the introductory paragraph of § 11.10 to state "* * * and, when appropriate, the confidentiality of electronic records." The agency believes, however that the need for retaining the confidentiality of certain records is not diminished because viewers cannot change them. It may be prudent for persons to carefully assess the need for record confidentiality. (See, e.g., 21 CFR

1002.42, Confidentiality of records furnished by dealers and distributors. with respect to certain radiological health products.) In addition, FDA's obligation to retain the confidentiality of information it receives in some submissions hinges on the degree to which the submitter maintains confidentiality, even within its own organization. (See, e.g., 21 CFR 720.8(b) with respect to cosmetic ingredient information in voluntary filings of cosmetic product ingredient and cosmetic raw material composition statements.)

61. One comment asked if the procedures and controls required by proposed § 11.10 were to be built into software or if they could exist in written

The agency expects that, by their nature, some procedures and controls. such as use of time-stamped audit trails and operational checks, will be built into hardware and software. Others. such as validation and determination of personnel qualifications, may be implemented in any appropriate manner regardless of whether the mechanisms are driven by, or are external to. software or hardware. To clarify this intent, the agency has revised the introductory paragraph of proposed §11.10 to read, in part, "Persons who use closed systems to create, modify * * *." Likewise, for clarity and consistency, the agency is introducing the same phrase, "persons who use * * *" in §§ 11.30 and 11.300.

62. One comment contended that the distinction between open and closed systems should not be predominant because a \$100,000 transaction in a closed system should not have fewer controls than a \$1 transaction in an

open system.

The agency believes that, within part 11, firms have the flexibility they need to adjust the extent and stringency of controls based on any factors they choose, including the economic value of the transaction. The agency does not believe it is necessary to modify part 11 at this time so as to add economic criteria.

63. One comment suggested that the reference to repudiation in the introductory paragraph of § 11.10 should be deleted because repudiation can occur at any time in legal proceedings. Another comment, noting that the proposed rule appeared to address only nonrepudiation of a signer, said the rule should address nonrepudiation of record "genuineness" or extend to nonrepudiation of submission, delivery, and receipt. The comment stated that some firms provide nonrepudiation services that can

prevent someone from successfully claiming that a record has been altered.

In response to the first comment, the agency does not agree that the reference to repudiation should be deleted because reducing the likelihood that someone can readily repudiate an electronic signature as not his or her own, or that the signed record had been altered, is vital to the agency's basic acceptance of electronic signatures. The agency is aware that the need to deter such repudiation has been addressed in many forums and publications that discuss electronic signatures. Absent adequate controls, FDA believes some people would be more likely to repudiate an electronically-signed record because of the relative ease with which electronic records may be altered and the ease with which one individual could impersonate another. The agency notes, however, that the rule does not call for nonrepudiation as an absolute guarantee, but requires that the signer cannot "readily" repudiate the signature.

In response to the second comment, the agency agrees that it is also important to establish nonrepudiation of submission, delivery, and receipt of electronic records, but advises that, for purposes of § 11.10, the agency's intent is to limit nonrepudiation to the genuineness of the signer's record. In other words, an individual should not be able to readily say that: (1) He or she did not, in fact, sign the record; (2) a given electronic record containing the individual's signature was not, in fact, the record that the person signed; or (3) the originally signed electronic record had been altered after having been

signed. 64. Proposed § 11.10(a) states that controls for closed systems are to include the validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to conclusively discern invalid or altered

records.

Many comments objected to this proposed requirement because the word 'conclusively' inferred an unreasonably high and unattainable standard, one which is not applied to

paper records.

The agency intends to apply the same validation concepts and standards to electronic record and electronic signature systems as it does to paper systems. As such, FDA does not intend the word "conclusively" to suggest an unattainable absolute and has, therefore, deleted the word from the final rule.

65. One comment suggested qualifying the proposed validation requirement in § 11.10(a) to state that validation be performed "where

commercially available software is not necessary because such software has already been thoroughly validated. The comment acknowledged that validation may be required for application programs written by manufacturers and others for special needs.

The agency disagrees with the comment's claim that all commercial software has been validated. The agency believes that commercial availability is no guarantee that software has undergone "thorough validation" and is unaware of any regulatory entity that has jurisdiction over general purpose software producers. The agency notes that, in general, commercial software packages are accompanied not by statements of suitability or compliance with established standards, but rather by disclaimers as to their fitness for use. The agency is aware of the complex and sometimes controversial issues in validating commercial software. However, the need to validate such software is not diminished by the fact that it was not written by those who will use the software.

In the future, the agency may provide guidance on validation of commercial software used in electronic record systems. FDA has addressed the matter of software validation in general in such documents as the "Draft Ğuideline for the Validation of Blood Establishment Computer Systems," which is available from the Manufacturers Assistance and Communications Staff, Center for Biologics Evaluation and Research (HFM-42), Food and Drug Administration, 1401 Rockville Pike, Rockville, MD 20852-1448, 301-594-2000. This guideline is also available by sending e-mail to the following Internet address:

CBER_INFO@A1.CBER.FDA.GOV). For the purposes of part 11, however, the agency believes it is vital to retain the validation requirement.

66. One comment requested an explanation of what was meant by the phrase "consistent intended" in proposed § 11.10(a) and why "consistent performance" was not used instead. The comment suggested that the rule should distinguish consistent intended performance from wellrecognized service "availability."

The agency advises that the phrase "consistent intended performance" relates to the general principle of validation that planned and expected performance is based upon predetermined design specifications (hence, "intended"). This concept is in accord with the agency's 1987 "Guideline on General Principles of Process Validation," which is available

necessary" and argued that validation of from the Division of Manufacturing and Product Quality, Center for Drug Evaluation and Research (HFD-320). Food and Drug Administration, 7520 Standish Pl., Rockville, MD 20855, 301– 594–0093). This guideline defines validation as establishing documented evidence that provides a high degree of assurance that a specific process will consistently produce a product meeting its predetermined specifications and quality attributes. The agency believes that the comment's concepts are accommodated by this definition to the extent that system "availability" may be one of the predetermined specifications or quality attributes.

67. One comment said the rule should indicate whether validation of systems does, or should, require any certification or accreditation.

The agency believes that although certification or accreditation may be a part of validation of some systems, such certification or accreditation is not necessary in all cases, outside of the context of any such approvals within an organization itself. Therefore, part 11 is silent on the matter.

68. One comment said the rule should clarify whether system validation should be capable of discerning the absence of electronic records, in light of agency concerns about falsification. The comment added that the agency's concerns regarding invalid or altered records can be mitigated by use of cryptographically enhanced methods, including secure time and date stamping.

The agency does not believe that it is necessary at this time to include an explicit requirement that systems be capable of detecting the absence of records. The agency advises that the requirement in § 11.10(e) for audit trails of operator actions would cover those actions intended to delete records. Thus, the agency would expect firms to document such deletions, and would expect the audit trail mechanisms to be included in the validation of the electronic records system.

69. Proposed § 11.10(b) states that controls for closed systems must include the ability to generate true copies of records in both human readable and electronic form suitable for argued that providing FDA with inspection, review, and copying by the agency, and that if there were any questions regarding the ability of the agency to perform such review and copying, persons should contact the agency.

Several comments objected to the requirement for "true" copies of electronic records. The comments asserted that information in an original record (as may be contained in a

database) may be presented in a copy in a different format that may be more usable. The comments concluded that, to generate precise "true" copies of electronic records, firms may have to retain the hardware and software that had been used to create those records in the first place (even when such hardware and software had been replaced by newer systems). The comments pointed out that firms may have to provide FDA with the application logic for "true" copies, and that this may violate copyright provisions. One comment illustrated the difference between "true" copies and other equally reliable, but not exact, copies of electronic records by noting that pages from FDA's paper publications (such as the CFR and the Compliance Policy Guidance Manual) look quite different from electronic copies posted to FDA's bulletin board. The comments suggested different wording that would effectively require accurate and complete copies, but not necessarily "true" copies.

The agency agrees that providing exact copies of electronic records in the strictest meaning of the word "true" may not always be feasible. The agency nonetheless believes it is vital that copies of electronic records provided to FDA be accurate and complete. Accordingly, in § 11.10(b), "true" has been replaced with "accurate and complete." The agency expects that this revision should obviate the potential problems noted in the comments. The revision should also reduce the costs of providing copies by making clear that firms need not maintain obsolete equipment in order to make copies that are "true" with respect to format and computer system.

70. Many comments objected to the proposed requirement that systems be capable of generating electronic copies of electronic records for FDA inspection and copying, although they generally agreed that it was appropriate to provide FDA with readable paper copies. Alternative wording was suggested that would make providing electronic copies optional, such that persons could provide FDA with nothing but paper copies if they so wished. The comments electronic copies was unnecessary, unjustified, not practical considering the different types of computer systems that may be in use, and would unfairly limit firms in their selection of hardware and software if they could only use systems that matched FDA's capabilities (capabilities which, it was argued, would not be uniform throughout the United States). One comment suggested that the rule specify

a particular format, such as ASCII, for electronic copies to FDA.

The agency disagrees with the assertion that FDA need only be provided with paper copies of electronic records. To operate effectively, the agency must function on the same technological plane as the industries it regulates. Just as firms realize efficiencies and benefits in the use of electronic records. FDA should be able to conduct audits efficiently and thoroughly using the same technology. For example, where firms perform computerized trend analyses of electronic records to improve their processes, FDA should be able to use computerized methods to audit electronic records (on site and off, as necessary) to detect trends. inconsistencies, and potential problem areas. If FDA is restricted to reviewing only paper copies of those records, the results would severely impede its operations. Inspections would take longer to complete, resulting in delays in approvals of new medical products, and expenditure of additional resources both by FDA (in performing the inspections and transcribing paper records to electronic format) and by the inspected firms, which would generate the paper copies and respond to questions during the resulting lengthened inspections.

The agency believes that it also may be necessary to require that persons furnish certain electronic copies of electronic records to FDA because paper copies may not be accurate and complete if they lack certain audit trail (metadata) information. Such information may have a direct bearing on record trustworthiness and reliability. These data could include information, for example, on when certain items of electronic mail were sent and received.

The agency notes that people who use different computer systems routinely provide each other with electronic copies of electronic records, and there are many current and developing tools to enable such sharing. For example, at a basic level, records may be created in, or transferred to, the ASCII format. Many different commercial programs have the capability to import from, and export to, electronic records having different formats. Firms use electronic data interchange (commonly known as EDI) and agreed upon transaction set formats to enable them to exchange copies of electronic records effectively. Third parties are also developing portable document formats to enable conversion among several diverse formats

Concerning the ability of FDA to handle different formats of electronic records, based upon the emergence of format conversion tools such as those mentioned above, the agency's experience with electronic submissions such as computer assisted new drug applications (commonly known as CANDA's), and the agency's planned Submissions Management and Review Tracking System (commonly known as SMART). FDA is confident that it can work with firms to minimize any formatting difficulties. In addition, substitution of the words "accurate and complete" for "true," as discussed in comment 69, should make it easier for firms to provide FDA with electronic copies of their electronic records. FDA does not believe it is necessary to specify any particular format in part 11 because it prefers, at this time, to afford industry and the agency more flexibility in deciding which formats meet the capabilities of all parties. Accordingly, the agency has revised proposed § 11.10(b) to read:

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

71. Proposed § 11.10(c) states that procedures and controls for closed systems must include the protection of records to enable their accurate and ready retrieval throughout the records retention period.

One firm commented that, because it replaces systems often (about every 3 years), it may have to retain supplanted systems to meet these requirements. Another comment suggested that the rule be modified to require records retention only for as long as "legally mandated."

The agency notes that, as discussed in comment 70 of this document, persons would not necessarily have to retain supplanted hardware and software systems provided they implemented conversion capabilities when switching to replacement technologies. The agency sequence or turning off an alarm to does not believe it is necessary to add the qualifier "legally mandated" because the retention period for a given record will generally be established by the regulation that requires the record. Where the regulations do not specify a given time, the agency would expect firms to establish their own retention periods. Regardless of the basis for the retention period, FDA believes that the requirement that a given electronic record be protected to permit it to be accurately and readily retrieved for as

long as it is kept is reasonable and necessary.

72. Proposed § 11.10(e) would require the use of time-stamped audit trails to document record changes, all write-tofile operations, and to independently record the date and time of operator entries and actions. Record changes must not obscure previously recorded information and such audit trail documentation must be retained for a period at least as long as required for the subject electronic documents and must be available for agency review and copying.

Many comments objected to the proposed requirement that all write-tofile operations be documented in the audit trail because it is unnecessary to document all such operations. The comments said that this would require audit trails for such automated recordings as those made to internal buffers, data swap files, or temporary files created by word processing programs. The comments suggested revising § 11.10(e) to require audit trails only for operator entries and actions.

Other comments suggested that audit trails should cover: (1) Operator data inputs but not actions, (2) only operator changes to records, (3) only critical write-to-file information, (4) operator changes as well as all actions, (5) only new entries, (6) only systems where data can be altered, (7) only information recorded by humans, (8) information recorded by both humans and devices, and (9) only entries made upon adoption of the records as official. One comment said audit trails should not be required for data acquisition systems, while another comment said audit trails are critical for data acquisition systems.

It is the agency's intent that the audit trail provide a record of essentially who did what, wrote what, and when. The write-to-file operations referenced in the proposed rule were not intended to cover the kind of "background" nonhuman recordings the comments identified.

The agency considers such operator actions as activating a manufacturing warrant the same audit trail coverage as operator data entries in order to document a thorough history of events and those responsible for such events. Although FDA acknowledges that not every operator "action," such as switching among screen displays, need be covered by audit trails, the agency is concerned that revising the rule to cover only "critical" operations would result in excluding much information and actions that are necessary to document events thoroughly.

The agency believes that, in general, the kinds of operator actions that need to be covered by an audit trail are those important enough to memorialize in the electronic record itself. These are actions which, for the most part, would be recorded in corresponding paper records according to existing recordkeeping requirements.

The agency intends that the audit trail capture operator actions (e.g., a command to open a valve) at the time they occur, and operator information (e.g., data entry) at the time the information is saved to the recording media (such as disk or tape), in much the same manner as such actions and information are memorialized on paper. The audit trail need not capture every keystroke and mistake that is held in a temporary buffer before those commitments. For example, where an operator records the lot number of an ingredient by typing the lot number, followed by the "return key" (where pressing the return key would cause the information to be saved to a disk file). the audit trail need not record every "backspace delete" key the operator may have previously pressed to correct a typing error. Subsequent "saved" corrections made after such a commitment, however, must be part of the audit trail.

At this time, the agency's primary concern relates to the integrity of human actions. Should the agency's experience with part 11 demonstrate a need to require audit trails of device operations and entries, the agency will propose appropriate revisions to these regulations. Accordingly, the agency has revised proposed § 11.10(e) by removing reference to all write-to-file operations and clarifying that the audit trail is to cover operator entries and actions that create, modify, or delete electronic records.

73. A number of comments questioned whether proposed § 11.10(e) mandated that the audit trail be part of the electronic record itself or be kept as a separate record. Some comments interpreted the word "independently" as requiring a separate record. Several comments focused on the question of whether audit trails should be generated manually under operator control or automatically without operator control. One comment suggested a revision that would require audit trails to be generated by computer, because the system, not the operator, should record the audit trail. Other comments said the rule should facilitate date and time recording by software, not operators, and that the qualifier "securely" be added to the language describing the audit trail. One comment, noting that

audit trails require validation and qualification to ensure that time stamps are accurate and independent, suggested that audit trails be required only when operator actions are witnessed.

The agency advises that audit trail information may be contained as part of the electronic record itself or as a separate record. FDA does not intend to require one method over the other. The word "independently" is intended to require that the audit trail not be under the control of the operator and, to prevent ready alteration, that it be created independently of the operator.

To maintain audit trail integrity, the agency believes it is vital that the audit trail be created by the computer system independently of operators. The agency believes it would defeat the purpose of audit trails to permit operators to write or change them. The agency believes that, at this time, the source of such independent audit trails may effectively be within the organization that creates the electronic record. However, the agency is aware of a situation under which time and date stamps are provided by trusted third parties outside of the creating organization. These third parties provide, in effect, a public electronic notary service. FDA will monitor development of such services in light of part 11 to determine if a requirement for such third party services should be included in these regulations. For now, the agency considers the advent of such services as recognition of the need for strict objectivity in recording time and date stamps.

The agency disagrees with the premise that only witnessed operator actions need be covered by audit trails because the opportunities for record falsification are not limited to cases where operator actions are witnessed. Also, the need for validating audit trails does not diminish the need for their implementation.

FDA agrees with the suggestion that the proposed rule be revised to require a secure audit trail—a concept inherent in having such a control at all. Accordingly, proposed § 11.10(e) has been revised to require use of "secure, computer-generated" audit trails.

74. A few comments objected to the requirement that time be recorded, in addition to dates, and suggested that time be recorded only when necessary and feasible. Other comments specifically supported the requirement for recording time, noting that time stamps make electronic signatures less vulnerable to fraud and abuse. The comments noted that, in any setting, and person responsible for adding to or

changing a value. One of the comments suggested that the rule require recording the reason for making changes to electronic records. Other comments implicitly supported recording time.

FDA believes that recording time is a critical element in documenting a sequence of events. Within a given day a number of events and operator actions may take place, and without recording time, documentation of those events would be incomplete. For example, without time stamps, it may be nearly impossible to determine such important sequencing as document approvals and revisions and the addition of ingredients in drug production. Thus, the element of time becomes vital to establishing an electronic record's trustworthiness and reliability.

The agency notes that comments on the ANPRM frequently identified use of date/time stamps as an important system control. Time recording, in the agency's view, can also be an effective deterrent to records falsification. For example, event sequence codes alone would not necessarily document true time in a series of events, making falsification of that sequence easier if time stamps are not used. The agency believes it should be very easy for firms to implement time stamps because there is a clock in every computer and document management software, electronic mail systems and other electronic record/electronic applications, such as digital signature programs, commonly apply date and time stamps. The agency does not intend that new technologies, such as cryptographic technologies, will be needed to comply with this requirement. The agency believes that implementation of time stamps should be feasible in virtually all computer systems because effective computer operations depend upon internal clock or timing mechanisms and, in the agency's experience, most computer systems are capable of precisely recording such time entries as when records are saved.

The agency is implementing the time stamp requirement based on the understanding that all current computers, electronic document software, electronic mail, and related electronic record systems include such technologies. The agency also understands that time stamps are applied automatically by these systems. meaning firms would not have to install additional hardware, software, or incur additional burden to implement this control. In recognition of this, the agency wishes to clarify that a primary there is a need to identify the date, time, intent of this provision is to ensure that people take reasonable measures to

ensure that those built in time stamps them casually so as to readily mask unauthorized record changes.

The agency advises that, although part 11 does not specify the time units (e.g., tenth of a second, or even the second) to be used, the agency expects the unit of time to be meaningful in terms of documenting human actions.

The agency does not believe part 11 needs to require recording the reason for record changes because such a requirement, when needed, is already in or system operational specification place in existing regulations that pertain to the records themselves.

75. One comment stated that proposed § 11.10(e) should not require an electronic signature for each write-tofile operation.

The agency advises that § 11.10(e) does not require an electronic signature

as the means of authenticating each write-to-file operation. The agency expects the audit trail to document who did what and when, documentation that can be recorded without electronic

signatures themselves.

76. Several comments, addressing the proposed requirement that record changes not obscure previously recorded information, suggested revising proposed § 11.10(e) to apply only to those entries intended to update previous information.

The agency disagrees with the suggested revision because the rewording is too narrow. The agency believes that some record changes may not be "updates" but significant modifications or falsifications disguised as updates. All changes to existing records need to be documented, regardless of the reason, to maintain a complete and accurate history, to document individual responsibility, and to enable detection of record falsifications.

77. Several comments suggested replacing the word "document" with "record" in the phrase "Such audit trails shall be retained for a period at least as long as required for the subject electronic documents * * *" because not all electronic documents are electronic records and because the word document connotes paper.

As discussed in section III.D. of this document, the agency equates electronic documents with electronic records, but for consistency, has changed the phrase to read "Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records * * *.

78. Proposed § 11.10(k) (ii) (§ 11.10(k)(2) in this regulation) addresses electronic audit trails as a systems documentation control. One

comment noted that this provision are accurate and that people do not alter appears to be the same as the audit trail provision of proposed § 11.10(e) and requested clarification.

> The agency wishes to clarify that the kinds of records subject to audit trails in the two provisions cited by the comment are different. Section 11.10(e) pertains to those records that are required by existing regulations whereas § 11.10(k)(2) covers the system documentation records regarding overall controls (such as access privilege logs, diagrams). Accordingly, the first sentence of § 11.10(e) has been revised to read "Use of secure, computergenerated, time-stamped audit trails to independently record and date the time of operator entries and actions that create, modify, or delete electronic records."

79. Proposed § 11.10(f) states that procedures and controls for closed systems must include the use of operational checks to enforce permitted sequencing of events, as appropriate.

Two comments requested clarification of the agency's intent regarding operational checks.

The agency advises that the purpose of performing operational checks is to ensure that operations (such as manufacturing production steps and signings to indicate initiation or completion of those steps) are not executed outside of the predefined order repudiate a signed record as not established by the operating organization.

80. Several comments suggested that. for clarity, the phrase "operational checks" be modified to "operational system checks."

The agency agrees that the added modifier "system" more accurately reflects the agency's intent that operational checks be performed by the computer systems and has revised proposed §11.10(f) accordingly.

81. Several comments suggested revising proposed § 11.10(f) to clarify what is to be checked. The comments suggested that "steps" in addition to "events" be checked, only critical steps be checked, and that "records" also be checked.

The agency intends the word "event" to include "steps" such as production steps. For clarity, however, the agency has revised proposed § 11.10(f) by adding the word "steps." The agency does not, however, agree that only critical steps need be subject to operational checks because a given specific step or event may not be critical, yet it may be very important that the step be executed at the proper time relative to other steps or events.

to add the modifier "records" to proposed § 11.10(f) because creation, deletion, or modification of a record is an event. Should it be necessary to create, delete, or modify records in a particular sequence, operational system checks would ensure that the proper sequence is followed.

82. Proposed § 11.10(g) states that procedures and controls for closed systems must include the use of authority checks to ensure that only authorized individuals use the system, electronically sign a record, access the operation or device, alter a record, or perform the operation at hand.

One comment suggested that the requirement for authority checks be qualified with the phrase "as appropriate," on the basis that it would not be necessary for certain parts of a system, such as those not affecting an electronic record. The comment cited pushing an emergency stop button as an example of an event that would not require an authority check. Another comment suggested deleting the requirement on the basis that some records can be read by all employees in an organization.

The agency advises that authority checks, and other controls under § 11.10, are intended to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure that signers cannot readily genuine. Functions outside of this context, such as pressing an emergency stop button, would not be covered. However, even in this example, the agency finds it doubtful that a firm would permit anyone, such as a stranger from outside the organization, to enter a facility and press the stop button at will regardless of the existence of an emergency. Thus, there would likely be some generalized authority checks built into the firm's operations.

The agency believes that few organizations freely permit anyone from within or without the operation to use their computer system, electronically sign a record, access workstations, alter records, or perform operations. It is likely that authority checks shape the activities of almost every organization. The nature, scope, and mechanism of performing such checks is up to the operating organization. FDA believes, however, that performing such checks is one of the most fundamental measures to ensure the integrity and trustworthiness of electronic records.

Proposed § 11.10(g) does not preclude all employees from being permitted to read certain electronic records. However, the fact that some records may The agency does not believe it necessary be read by all employees would not

justify deleting the requirement for authority checks entirely. The agency believes it is highly unlikely that all of a firm's employees would have authority to read, write, and sign all of its electronic records.

83. One comment said authority checks are appropriate for document access but not system access, and suggested that the phrase "access the operation or device" be deleted. The comment added, with respect to authority checks on signing records, that in many organizations, more than one individual has the authority to sign documents required under FDA regulations and that such authority should be vested with the individual as designated by the operating organization. Another comment said proposed § 11.10(g) should explicitly require access authority checks and suggested that the phrase "use the system" be changed to "access and use the system." The comment also asked for clarification of the term "device."

The agency disagrees that authority checks should not be required for system access because, as discussed in comment 82 of this document, it is unlikely that a firm would permit any unauthorized individuals to access its computer systems. System access control is a basic security function because system integrity may be impeached even if the electronic records themselves are not directly accessed. For example, someone could access a system and change password requirements or otherwise override important security measures, enabling individuals to alter electronic records or read information that they were not authorized to see. The agency does not believe it necessary to add the qualifier "access and" because § 11.10(d) already requires that system access be limited to authorized individuals. The agency intends the word "device" to mean a computer system input or output device and has revised proposed § 11.10(g) to clarify this point.

Concerning signature authority, FDA advises that the requirement for authority checks in no way limits organizations in authorizing individuals to sign multiple records. Firms may use any appropriate mechanism to implement such checks. Organizations do not have to embed a list of authorized signers in every record to perform authority checks. For example, a record may be linked to an authority code that identifies the title or organizational unit of people who may sign the record. Thus, employees who have that corresponding code, or belong to that unit, would be able to sign the record. Another way to implement

controls would be to link a list of authorized records to a given individual, so that the system would permit the individual to sign only records in that list.

84. Two comments addressed authority checks within the context of PDMA and suggested that such checks not be required for drug sample receipt records. The comments said that different individuals may be authorized to accept drug samples at a physician's office, and that the large number of physicians who would potentially qualify to receive samples would be too great to institute authority checks.

The agency advises that authority checks need not be automated and that in the context of PDMA such checks would be as valid for electronic records as they are for paper sample requests because only licensed practitioners or their designees may accept delivery of drug samples. The agency, therefore, acknowledges that many individuals may legally accept samples and, thus, have the authority to sign electronic receipts. However, authority checks for electronic receipts could nonetheless be performed by sample manufacturer representatives by using the same procedures as the representatives use for paper receipts. Accordingly, the agency disagrees with the comment that proposed § 11.10(g) should not apply to PDMA sample receipts.

The agency also advises that under PDMA, authority checks would be particularly important in the case of drug sample request records because only licensed practitioners may request drug samples.

Accordingly, proposed § 11.10(g) has been revised to read: "Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand."

85. Proposed § 11.10(h) states that procedures and controls for closed systems must include the use of device (e.g., terminal) location checks to determine, as appropriate, the validity of the source of data input or operational instruction. Several comments objected to this proposed requirement and suggested its deletion because it is: (1) Unnecessary (because the data source is always known by virtue of system design and validation); (2) problematic with respect to mobile devices, such as those connected by modem; (3) too much of a "how to;" (4) not explicit enough to tell firms what to do; (5) unnecessary in the case of PDMA; and (6) technically challenging. One comment stated that a device's

identification, in addition to location, may be important and suggested that the proposed rule be revised to require device identification as well.

FDA advises that, by use of the term "as appropriate," it does not intend to require device checks in all cases. The agency believes that these checks are warranted where only certain devices have been selected as legitimate sources of data input or commands. In such cases, the device checks would be used to determine if the data or command source was authorized. In a network, for example, it may be necessary for security reasons to limit issuance of critical commands to only one authorized workstation. The device check would typically interrogate the source of the command to ensure that only the authorized workstation, and not some other device, was, in fact. issuing the command.

The same approach applies for remote sources connected by modem, to the extent that device identity interrogations could be made automatically regardless of where the portable devices were located. To clarify this concept, the agency has removed the word "location" from proposed §11.10(h). Device checks would be necessary under PDMA when the source of commands or data is relevant to establishing authenticity, such as when licensed practitioners order drug samples directly from the manufacturer or authorized distributor without the intermediary of a sales representative. Device checks may also be useful to firms in documenting and identifying which sales representatives are transmitting drug sample requests from licensed practitioners.

FDA believes that, although validation may demonstrate that a given terminal or workstation is technically capable of sending information from one point to another, validation alone would not be expected to address whether or not such device is authorized to do so.

86. Proposed § 11.10(i) states that procedures and controls for closed systems must include confirmation that persons who develop, maintain, or use electronic record or signature systems have the education, training, and experience to perform their assigned tasks.

Several comments objected to the word "confirmation" because it is redundant with, or more restrictive than, existing regulations, and suggested alternate wording, such as "evidence." Two comments interpreted the proposed wording as requiring that checks of personnel qualifications be performed automatically by computer systems that perform database type

matches between functions and personnel training records.

The agency advises that, although there may be some overlap in proposed § 11.10(i) and other regulations regarding the need for personnel to be properly qualified for their duties, part 11 is specific to functions regarding electronic records, an issue that other regulations may or may not adequately address. Therefore, the agency is retaining the requirement.

The agency does not intend to require that the check of personnel qualifications be performed automatically by a computer system itself (although such automation is desirable). The agency has revised the introductory paragraph of § 11.10, as discussed in section VII. of this document, to clarify this point. The agency agrees that another word should be used in place of "confirmation," and for clarity has selected "determination."

87. One comment suggested that the word "training" be deleted because it has the same meaning as "education" and "experience," and objected to the implied requirement for records of employee training. Another comment argued that applying this provision to system developers was irrelevant so long as systems perform as required and have been appropriately validated. The comment suggested revising proposed § 11.10(i) to require employees to be trained only "as necessary." One comment, noting that training and experience are very important, suggested expanding proposed § 11.10(i) to require appropriate examination and certification of persons who perform certain high-risk, high-trust functions and tasks.

The agency regards this requirement as fundamental to the proper operation of a facility. Personnel entrusted with important functions must have sufficient training to do their jobs. In FDA's view, formal education (e.g., academic studies) and general industry experience would not necessarily prepare someone to begin specific, highly technical tasks at a given firm. Some degree of on-the-job training would be customary and expected. The agency believes that documentation of such training is also customary and not unreasonable.

The agency also disagrees with the assertion that personnel qualifications of system developers are irrelevant. The qualifications of personnel who develop systems are relevant to the expected performance of the systems they build and their ability to explain and support these systems. Validation does not lessen the need for personnel to have the education, training, and experience

to do their jobs properly. Indeed, it is highly unlikely that poorly qualified developers would be capable of producing a system that could be validated. The agency advises that, although the intent of proposed § 11.10(i) is to address qualifications of those personnel who develop systems within an organization, rather than external "vendors" per se, it is nonetheless vital that vendor personnel are likewise qualified to do their work. The agency agrees that periodic examination or certification of personnel who perform certain critical tasks is desirable. However, the agency does not believe that at this time a specific requirement for such examination and certification is necessary.

88. Proposed §11.10(j) states that procedures and controls for closed systems must include the establishment of, and adherence to, written policies that hold individuals accountable and liable for actions initiated under their electronic signatures, so as to deter record and signature falsification.

Several comments suggested changing the word "liable" to "responsible" because the word "responsible" is broader, more widely understood by employees, more positive and inclusive of elements of honesty and trust, and more supportive of a broad range of disciplinary measures. One comment argued that the requirement would not deter record or signature falsification because employee honesty and integrity cannot be regulated.

The agency agrees because, although

the words "responsible" and "liable" are generally synonymous. "responsible" is preferable because it is more positive and supportive of a broad range of disciplinary measures. There may be a general perception that electronic records and electronic signatures (particularly identification codes and passwords) are less significant and formal than traditional paper records and handwritten signatures. Individuals may therefore not fully equate the seriousness of electronic record falsification with paper record falsification. Employees need to understand the gravity and consequences of signature or record falsification. Although FDA agrees that employee honesty cannot be ensured by requiring it in a regulation, the presence of strong accountability and responsibility policies is necessary to ensure that employees understand the

of electronic records and signatures. 89. Several comments expressed concern regarding employee liability for actions taken under their electronic

importance of maintaining the integrity

signatures in the event that such signatures are compromised, and requested "reasonable exceptions." The comments suggested revising proposed § 11.10(j) to hold people accountable only where there has been intentional falsification or corruption of electronic data.

The agency considers the compromise of electronic signatures to be a very serious matter, one that should precipitate an appropriate investigation into any causative weaknesses in an organization's security controls. The agency nonetheless recognizes that where such compromises occur through no fault or knowledge of individual employees, there would be reasonable limits on the extent to which disciplinary action would be taken. However, to maintain emphasis on the seriousness of such security breeches and deter the deliberate fabrication of "mistakes," the agency believes § 11.10 should not provide for exceptions that may lessen the import of such a fabrication.

90. One comment said the agency should consider the need for criminal law reform because current computer crime laws do not address signatures when unauthorized access or computer use is not an issue. Another comment argued that proposed § 11.10(j) should be expanded beyond "individual" accountability to include business entities.

The agency will consider the need for recommending legislative initiatives to address electronic signature falsification in light of the experience it gains with this regulation. The agency does not believe it necessary to address business entity accountability specifically in § 11.10 because the emphasis is on actions and accountability of individuals, and because individuals, rather than business entities, apply signatures.

91. One comment suggested that proposed § 11.10(j) should be deleted because it is unnecessary because individuals are presumably held accountable for actions taken under their authority, and because, in some organizations, individuals frequently delegate authority to sign their names.

As discussed in comments 88 to 90 of this document, the agency has concluded that this section is necessary. Furthermore it does not limit delegation of authority as described in the comment. However, where one individual signs his or her name on behalf of someone else, the signature applied should be that of the delegatee, with some notation of that fact, and not the name of the delegator. This is the

same procedure commonly used on paper documents, noted as "X for Y.

paper documents, noted as "X for Y." 92. Proposed § 11.10(k) states that procedures and controls for closed systems must include the use of appropriate systems documentation controls, including: (1) Adequate controls over the distribution, access to, and use of documentation for system operation and maintenance; and (2) records revision and change control procedures to maintain an electronic audit trail that documents timesequenced development and modification of records. Several comments requested clarification of the type of documents covered by proposed § 11.10(k). One comment noted that this section failed to address controls for record retention. Some comments suggested limiting the scope of systems documentation to application and configurable software, or only to software that could compromise system security or integrity. Other comments suggested that this section should be deleted because some documentation needs wide distribution within an organization, and that it is an onerous burden to control user manuals.

The agency advises that § 11.10(k) is intended to apply to systems documentation, namely, records describing how a system operates and is maintained, including standard operating procedures. The agency believes that adequate controls over such documentation are necessary for various reasons. For example, it is important for employees to have correct and updated versions of standard operating and maintenance procedures. If this documentation is not current. errors in procedures and/or maintenance are more likely to occur. Part 11 does not limit an organization's discretion as to how widely or narrowly any document is to be distributed, and FDA expects that certain documents will, in fact, be widely disseminated. However, some highly sensitive documentation, such as instructions on how to modify system security features, would not routinely be widely distributed. Hence, it is important to control distribution of, access to, and use of such documentation.

Although the agency agrees that the most critical types of system documents would be those directly affecting system security and integrity, FDA does not agree that control over system documentation should only extend to security related software or to application or configurable software. Documentation that relates to operating systems, for example, may also have an impact on security and day-to-day operations. The agency does not agree

that it is an onerous burden to control documentation that relates to effective operation and security of electronic records systems. Failure to control such documentation, as discussed above, could permit and foster records falsification by making the enabling instructions for these acts readily available to any individual.

93. Concerning the proposed requirement for adequate controls over documentation for system operation and maintenance, one comment suggested that it be deleted because it is under the control of system vendors, rather than operating organizations. Several comments suggested that the proposed provision be deleted because it duplicates § 11.10(e) with respect to audit trails. Some comments also objected to maintaining the change control procedures in electronic form and suggested deleting the word "electronic" from "electronic audit trails."

The agency advises that this section is intended to apply to systems documentation that can be changed by individuals within an organization. If systems documentation can only be changed by a vendor, this provision does not apply to the vendor's customers. The agency acknowledges that systems documentation may be in paper or electronic form. Where the documentation is in paper form, an audit trail of revisions need not be in electronic form. Where systems documentation is in electronic form. however, the agency intends to require the audit trail also be in electronic form, in accordance with § 11.10(e). The agency acknowledges that, in light of the comments, the proposed rule may not have been clear enough regarding audit trails addressed in § 11.10(k) compared to audit trails addressed in §11.10(e) and has revised the final rule to clarify this matter.

The agency does not agree, however, that the audit trail provisions of § 11.10(e) and (k), as revised, are entirely duplicative. Section 11.10(e) applies to electronic records in general (including systems documentation); § 11.10(k) applies exclusively to systems documentation, regardless of whether such documentation is in paper or electronic form.

required. The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not expect to be performed by individual firms on an ad hoc basis, and one FDA does not now seek to perform.

The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not expect to be performed by individual firms on an ad hoc basis, and one FDA does not now seek to perform.

The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not now seek to perform.

As revised, § 11.10(k) now reads as follows:

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. VIII. Electronic Records—Controls for Open Systems (§ 11.30)

Proposed § 11.30 states that: "Open systems used to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and confidentiality of electronic records from the point of their creation to the point of their receipt." In addition, § 11.30 states:

* * Such procedures and controls shall include those identified in § 11.10, as appropriate, and such additional measures as document encryption and use of established digital signature standards acceptable to the agency, to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

94. One comment suggested that the reference to digital signature standards be deleted because the agency should not be setting standards and should not dictate how to ensure record authenticity, integrity, and confidentiality. Other comments requested clarification of the agency's expectations with regard to digital signatures: (1) The kinds that would be acceptable, (2) the mechanism for announcing which standards were acceptable (and whether that meant FDA would be certifying particular software), and (3) a definition of digital signature. One comment asserted that FDA should accept international standards for digital signatures. Some comments also requested a definition of encryption. One comment encouraged the agency to further define open systems.

The agency advises that § 11.30 requires additional controls, beyond those identified in § 11.10, as needed under the circumstances, to ensure record authenticity, integrity, and confidentiality for open systems. Use of digital signatures is one measure that may be used, but is not specifically required. The agency wants to ensure that the digital signature standard used is, in fact, appropriate. Development of digital signature standards is a complex undertaking, one FDA does not expect to be performed by individual firms on an ad hoc basis, and one FDA does not now seek to perform.

The agency is nonetheless concerned that such standards be robust and secure. Currently, the agency is aware of two such standards, the RSA (Rivest-Shamir-Adleman), and NIST's Digital Signature Standard (DSS). The DSS became Federal Information Processing Standard (FIPS) 186 on December 1, 1994. These standards are incorporated in different software programs. The agency does not seek to certify or otherwise approve of such programs,

but expects people who use such programs to ensure that they are suitable for their intended use. FDA is aware that NIST provides certifications regarding mathematical conformance to the DSS core algorithms, but does not formally evaluate the broader programs that contain those algorithms. The agency has revised the final rule to clarify its intent that firms retain the flexibility to use any appropriate digital signature as an additional system control for open systems. FDA is also including a definition of digital signature under § 11.3(b)(5).

The agency does not believe it necessary to codify the term "encryption" because, unlike the term digital signature, it has been in general use for many years and is generally understood to mean the transforming of a writing into a secret code or cipher. The agency is aware that there are several commercially available software programs that implement both digital signatures and encryption.

95. Two comments noted that use of digital signatures and encryption is not necessary in the context of PDMA, where access to an electronic record is limited once it is signed and stored. One of the comments suggested that proposed § 11.30 be revised to clarify this point.

As discussed in comment 94 of this document, use of digital signatures and encryption would be an option when extra measures are necessary under the circumstances. In the case of PDMA records, such measures may be warranted in certain circumstances, and unnecessary in others. For example, if electronic records were to be transmitted by a firm's representative by way of a public online service to a central location, additional measures would be necessary. On the other hand, where the representative's records are hand delivered to that location, or transferred by direct connection between the representative and the central location, such additional measures to ensure record authenticity, confidentiality, and integrity may not be necessary. The agency does not believe that it is practical to revise § 11.30 to elaborate on every possible situation in which additional measures would or would not be needed.

96. One comment addressed encryption of submissions to FDA and asked if people making those submissions would have to give the agency the appropriate "keys" and, if so, how the agency would protect the security of such information.

The agency intends to develop appropriate procedures regarding the exchange of "keys" attendant to use of

encryption and digital signatures, and will protect those keys that must remain confidential, in the same manner as the agency currently protects trade secrets. Where the agency and a submitter agree to use a system that calls for the exchange of secret keys, FDA will work with submitters to achieve mutually agreeable procedures. The agency notes. however, that not all encryption and digital signature systems require that enabling keys be secret.

97. One comment noted that proposed § 11.30 does not mention availability and nonrepudiation and requested clarification of the term "point of receipt." The comment noted that, where an electronic record is received at a person's electronic mailbox (which resides on an open system), additional measures may be needed when the record is transferred to the person's own local computer because such additional transfer entails additional security risks. The comment suggested wording that would extend open system controls to the point where records are ultimately retained.

The agency agrees that, in the situation described by the comment. movement of the electronic record from an electronic mailbox to a person's local computer may necessitate open system controls. However, situations may vary considerably as to the ultimate point of receipt, and FDA believes proposed § 11.30 offers greater flexibility in determining open system controls than revisions suggested by the comment. The agency advises that the concept of nonrepudiation is part of record authenticity and integrity, as already covered by § 11.10(c). Therefore, FDA is not revising § 11.30 as suggested.

IX. Electronic Records—Signature Manifestations (§ 11.50)

Proposed § 11.50 requires that electronic records that are electronically signed must display in clear text the printed name of the signer, and the date and time when the electronic signature was executed. This section also requires that electronic records clearly indicate the meaning (such as review, approval, responsibility, and authorship) associated with their attendant signatures.

98. Several comments suggested that the information required under proposed § 11.50 need not be contained in the electronic records themselves, but only in the human readable format (screen displays and printouts) of such records. The comments explained that the records themselves need only contain links, such as signature attribute require them to be signed. The agency codes, to such information to produce the displays of information required.

The comments noted, for example, that, where electronic signatures consist of an identification code in combination with a password, the combined code and password itself would not be part of the display. Some comments suggested that proposed § 11.50 be revised to clarify what items are to be displayed.

The agency agrees and has revised proposed § 11.50 accordingly. The intent of this section is to require that human readable forms of signed electronic records, such as computer screen displays and printouts bear: (1) The printed name of the signer (at the time the record is signed as well as whenever the record is read by humans); (2) the date and time of signing; and (3) the meaning of the signature. The agency believes that revised § 11.50 will afford persons the flexibility they need to implement the display of information appropriate for their own electronic records systems, consistent with other system controls in part 11, to ensure record integrity and prevent falsification.

99. One comment stated that the controls in proposed § 11.50 would not protect against inaccurate entries.

FDA advises that the purpose of this section is not to protect against inaccurate entries, but to provide unambiguous documentation of the signer, when the signature was executed, and the signature's meaning. The agency believes that such a record is necessary to document individual responsibility and actions.

In a paper environment, the printed name of the individual is generally present in the signed record, frequently part of a traditional "signature block." In an electronic environment, the person's name may not be apparent, especially where the signature is based on identification codes combined with passwords. In addition, the meaning of a signature is generally apparent in a paper record by virtue of the context of the record or, more often, explicit phrases such as "approved by," "reviewed by," and "performed by." Thus, the agency believes that for clear documentation purposes it is necessary to carry such meanings into the electronic record environment.

100. One comment suggested that proposed § 11.50 should apply only to those records that are required to be signed, and that the display of the date and time should be performed in a secure manner.

The agency intends that this section apply to all signed electronic records regardless of whether other regulations believes that if it is important enough that a record be signed, human readable

displays of such records must include the printed name of the signer, the date and time of signing, and the meaning of the signature. Such information is crucial to the agency's ability to protect public health. For example, a message from a firm's management to employees instructing them on a particular course of action may be critical in litigation. This requirement will help ensure clear documentation and deter falsification regardless of whether the signature is electronic or handwritten.

The agency agrees that the display of information should be carried out in a secure manner that preserves the integrity of that information. The agency, however, does not believe it is necessary at this time to revise § 11.50 to add specific security measures because other requirements of part 11 have the effect of ensuring appropriate security.

Because signing information is important regardless of the type of signature used, the agency has revised § 11.50 to cover all types of signings.

101. Several comments objected to the requirement in proposed § 11.50(a) that the time of signing be displayed in addition to the date on the grounds that such information is: (1) Unnecessary, (2) costly to implement, (3) needed in the electronic record for auditing purposes, but not needed in the display of the record, and (4) only needed in critical applications. Some comments asserted that recording time should be optional. One comment asked whether the time should be local to the signer or to a central network when electronic record systems cross different time zones.

The agency believes that it is vital to record the time when a signature is applied. Documenting the time when a signature was applied can be critical to demonstrating that a given record was, or was not, falsified. Regarding systems that may span different time zones, the agency advises that the signer's local time is the one to be recorded.

102. One comment assumed that a person's user identification code could be displayed instead of the user's printed name, along with the date and time of signing.

This assumption is incorrect. The agency intends that the printed name of the signer be displayed for purposes of unambiguous documentation and to emphasize the importance of the act of signing to the signer. The agency believes that because an identification code is not an actual name, it would not be a satisfactory substitute.

103. One comment suggested that the word "printed" in the phrase "printed name" be deleted because the word was superfluous. The comment also stated

that the rule should state when the clear text must be created or displayed because some computer systems, in the context of electronic data interchange transactions, append digital signatures to records before, or in connection with. communication of the record.

The agency disagrees that the word "printed" is superfluous because the intent of this section is to show the name of the person in an unambiguous manner that can be read by anyone. The agency believes that requiring the printed name of the signer instead of codes or other manifestations, more effectively provides clarity.

The agency has revised this section to clarify the point at which the signer's information must be displayed, namely, as part of any human readable form of the electronic record. The revision, in the agency's view, addresses the comment's concern regarding the application of digital signatures. The agency advises that under § 11.50, any time after an electronic record has been signed, individuals who see the human readable form of the record will be able to immediately tell who signed the record, when it was signed, and what the signature meant. This includes the signer who, as with a traditional signature to paper, will be able to review the signature instantly.

104. One comment asked if the operator would have to see the meaning of the signature, or if the information had to be stored on the physical

electronic record.

As discussed in comment 100 of this document, the information required by §11.50(b) must be displayed in the human readable format of the electronic record. Persons may elect to store that information directly within the electronic record itself, or in logically associated records, as long as such information is displayed any time a person reads the record.

105. One comment noted that proposed § 11.50(b) could be interpreted to require lengthy explanations of the signatures and the credentials of the signers. The comment also stated that this information would more naturally be contained in standard operating procedures, manuals, or accompanying literature than in the electronic records themselves.

The agency believes that the comment misinterprets the intent of this provision. Recording the meaning of the signature does not infer that the signer's credentials or other lengthy explanations be part of that meaning. The statement must merely show what is meant by the act of signing (e.g., review, approval, responsibility, authorship)

106. One comment noted that the meaning of a signature may be included in a (digital signature) public key certificate and asked if this would be acceptable. The comment also noted that the certificate might be easily accessible by a record recipient from either a recognized database or one that might be part of, or associated with, the electronic record itself. The comment further suggested that FDA would benefit from participating in developing rules of practice regarding certificatebased public key cryptography and infrastructure with the Information Security Committee, Section of Science and Technology, of the American Bar Association (ABA).

The intent of this provision is to clearly discern the meaning of the signature when the electronic record is displayed in human readable form. The agency does not expect such meaning to be contained in or displayed by a public key certificate because the public key is generally a fixed value associated with an individual. The certificate is used by the recipient to authenticate a digital signature that may have different meanings, depending upon the record being signed. FDA acknowledges that it is possible for someone to establish different public keys, each of which may indicate a different signature meaning. Part 11 would not prohibit multiple "meaning" keys provided the meaning of the signature itself was still clear in the display of the record, a feature that could conceivably be implemented by software.

Regarding work of the ABA and other standard-setting organizations, the agency welcomes an open dialog with such organizations, for the mutual benefit of all parties, to establish and facilitate the use of electronic record/ electronic signature technologies. FDA's participation in any such activities would be in accordance with the agency's policy on standards stated in the Federal Register of October 11, 1995 (60 FR 53078).

Revised § 11.50, signature manifestations, reads as follows:

- (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:
- (1) The printed name of the signer; (2) The date and time when the signature was executed; and
- (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature
- (b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

X. Electronic Records—Signature/ Record Linking (§ 11.70)

107. Proposed § 11.70 states that electronic signatures and handwritten signatures executed to electronic records must be verifiably bound to their respective records to ensure that signatures could not be excised, copied, or otherwise transferred to falsify another electronic record.

Many comments objected to this provision as too prescriptive, unnecessary, unattainable, and excessive in comparison to paper-based records. Some comments asserted that the objectives of the section could be attained through appropriate procedural and administrative controls. The comments also suggested that objectives of the provision could be met by appropriate software (i.e., logical) links between the electronic signatures and electronic records, and that such links are common in systems that use identification codes in combination with passwords. One firm expressed full support for the provision, and noted that its system implements such a feature and that signature-to-record binding is similar to the record-locking provision of the proposed PDMA regulations.

The agency did not intend to mandate use of any particular technology by use of the word "binding." FDA recognizes that, because it is relatively easy to copy an electronic signature to another electronic record and thus compromise or falsify that record, a technology based link is necessary. The agency does not believe that procedural or administrative controls alone are sufficient to ensure that objective because such controls could be more easily circumvented than a straightforward technology based approach. In addition, when electronic records are transferred from one party to another, the procedural controls used by the sender and recipient may be different. This could result in record falsification by signature transfer.

The agency agrees that the word "link" would offer persons greater flexibility in implementing the intent of this provision and in associating the names of individuals with their identification codes/passwords without actually recording the passwords themselves in electronic records. The agency has revised proposed § 11.70 to state that signatures shall be linked to their electronic records.

108. Several comments argued that proposed § 11.70 requires absolute protection of electronic records from falsification, an objective that is

unrealistic to the extent that determined individuals could falsify records.

The agency acknowledges that, despite elaborate system controls, certain determined individuals may find a way to defeat antifalsification measures. FDA will pursue such illegal activities as vigorously as it does falsification of paper records. For purposes of part 11, the agency's intent is to require measures that prevent electronic records falsification by ordinary means. Therefore, FDA has revised § 11.70 by adding the phrase "by ordinary means" at the end of this section.

109. Several comments suggested changing the phrase "another electronic record" to "an electronic record" to clarify that the antifalsification provision applies to the current record as well as any other record.

The agency agrees and has revised § 11.70 accordingly.

110. Two comments argued that signature-to-record binding is unnecessary, in the context of PDMA, beyond the point of record creation (i.e., when records are transmitted to a point of receipt). The comments asserted that persons who might be in a position to separate a signature from a record (for purposes of falsification) are individuals responsible for record integrity and thus unlikely to falsify records. The comments also stated that signature-torecord binding is produced by software coding at the time the record is signed, and suggested that proposed § 11.70 clarify that binding would be necessary only up to the point of actual transmission of the electronic record to a central point of receipt.

The agency disagrees with the comment's premise that the need for binding to prevent falsification depends on the disposition of people to falsify records. The agency believes that reliance on individual tendencies is insufficient insurance against falsification. The agency also notes that in the traditional paper record, the signature remains bound to its corresponding record regardless of where the record may go.

111. One comment suggested that proposed § 11.70 be deleted because it appears to require that all records be kept on inalterable media. The comment also suggested that the phrase "otherwise transferred" be deleted on the basis that it should be permissible for copies of handwritten signatures (recorded electronically) to be made when used, in addition to another unique individual identification mechanism

The agency advises that neither § 11.70, nor other sections in part 11,

requires that records be kept on inalterable media. What is required is that whenever revisions to a record are made, the original entries must not be obscured. In addition, this section does not prohibit copies of handwritten signatures recorded electronically from being made for legitimate reasons that do not relate to record falsification. Section 11.70 merely states that such copies must not be made that falsify electronic records.

112. One comment suggested that proposed § 11.70 be revised to require application of response cryptographic methods because only those methods could be used to comply with the regulation. The comment noted that, for certificate based public key cryptographic methods, the agency should address verifiable binding between the signer's name and public key as well as binding between digital signatures and electronic records. The comment also suggested that the regulation should reference electronic signatures in the context of secure time and date stamping.

The agency intends to permit maximum flexibility in how organizations achieve the linking called for in § 11.70, and, as discussed above, has revised the regulation accordingly. Therefore, FDA does not believe that cryptographic and digital signature methods would be the only ways of linking an electronic signature to an electronic document. In fact, one firm commented that its system binds a person's handwritten signature to an electronic record. The agency agrees that use of digital signatures accomplishes the same objective because, if a digital signature were to be copied from one record to another, the second record would fail the digital signature verification procedure. Furthermore, FDA notes that concerns regarding binding a person's name with the person's public key would be addressed in the context of § 11.100(b) because an organization must establish an individual's identity before assigning or certifying an electronic signature (or any of the electronic signature components).

113. Two comments requested clarification of the types of technologies that could be used to meet the requirements of proposed § 11.70.

As discussed in comment 107 of this document, the agency is affording persons maximum flexibility in using any appropriate method to link electronic signatures to their respective electronic records to prevent record falsification. Use of digital signatures is one such method, as is use of software locks to prevent sections of codes

representing signatures from being copied or removed. Because this is an area of developing technology, it is likely that other linking methods will emerge.

XI. Electronic Signatures—General Requirements (§ 11.100)

Proposed § 11.100(a) states that each electronic signature must be unique to one individual and not be reused or reassigned to anyone else.

114. One comment asserted that several people should be permitted to share a common identification code and password where access control is limited to inquiry only.

Part 11 does not prohibit the establishment of a common group identification code/password for read only access purposes. However, such commonly shared codes and passwords would not be regarded, and must not be used, as electronic signatures. Shared access to a common database may nonetheless be implemented by granting appropriate common record access privileges to groups of people, each of whom has a unique electronic signature.

115. Several comments said proposed § 11.100(a) should permit identification codes to be reused and reassigned from one employee to another, as long as an audit trail exists to associate an identification code with a given individual at any one time, and different passwords are used. Several comments said the section should indicate if the agency intends to restrict authority delegation by the nonreassignment or nonreuse provision, or by the provision in § 11.200(a)(2) requiring electronic signatures to be used only by their genuine owners. The comments questioned whether reuse means restricting one noncryptographic based signature to only one record and argued that passwords need not be unique if the combined identification code and password are unique to one individual. One comment recommended caution in using the term "ownership" because of possible confusion with intellectual property rights or ownership of the computer systems themselves.

The agency advises that, where an electronic signature consists of the combined identification code and password, § 11.100 would not prohibit the reassignment of the identification code provided the combined identification code and password remain unique to prevent record falsification. The agency believes that such reassignments are inadvisable, however, to the extent that they might be combined with an easily guessed password, thus increasing the chances that an individual might assume a

signature belonging to someone else. The agency also advises that where people can read identification codes (e.g., printed numbers and letters that are typed at a keyboard or read from a card), the risks of someone obtaining that information as part of a falsification effort would be greatly increased as compared to an identification code that is not in human readable form (one that is, for example, encoded on a "secure card" or other device).

Regarding the delegation of authority to use electronic signatures, FDA does not intend to restrict the ability of one individual to sign a record or otherwise act on behalf of another individual. However, the applied electronic signature must be the assignee's and the record should clearly indicate the capacity in which the person is acting (e.g., on behalf of, or under the authority of, someone else). This is analogous to traditional paper records and handwritten signatures when person "A" signs his or her own name under the signature block of person "B," with appropriate explanatory notations such as "for" or "as representative of" person B. In such cases, person A does not simply sign the name of person B. The

used for electronic records and electronic signatures.

The agency intends the term "reuse" to refer to an electronic signature used by a different person. The agency does not regard as "reuse" the replicate application of a noncryptographic based electronic signature (such as an identification code and password) to different electronic records. For clarity, FDA has revised the phrase "not be reused or reassigned to" to state "not be reused by, or reassigned to," in

§ 11.100(a).

The reference in § 11.200(a) to ownership is made in the context of an individual owning or being assigned a particular electronic signature that no other individual may use. FDA believes this is clear and that concerns regarding ownership in the context of intellectual property rights or hardware are misplaced.

116. One comment suggested that proposed § 11.100(a) should accommodate electronic signatures assigned to organizations rather than individuals.

The agency advises that, for purposes of part 11, electronic signatures are those of individual human beings and not organizations. For example, FDA does not regard a corporate seal as an individual's signature. Humans may represent and obligate organizations by signing records, however. For clarification, the agency is substituting

the word "individual" for "person" in the definition of electronic signature (§ 11.3(b)(7)) because the broader definition of person within the act includes organizations.

117. Proposed § 11.100(b) states that, before an electronic signature is assigned to a person, the identity of the individual must be verified by the assigning authority.

Two comments noted that where people use identification codes in combination with passwords only the identification code portion of the electronic signature is assigned, not the password. Another comment argued that the word "assigned" is inappropriate in the context of electronic signatures based upon public key cryptography because the appropriate authority certifies the bind between the individual's public key and identity, and not the electronic signature itself.

handwritten signatures when person "A" signs his or her own name under the signature block of person "B," with appropriate explanatory notations such as "for" or "as representative of" person B. In such cases, person A does not simply sign the name of person B. The agency expects the same procedure to be used for electronic records and electronic signatures.

The agency acknowledges that, for certain types of electronic signatures, the authorizing or certifying organization issues or approves only a portion of what eventually becomes an individual's electronic signature. FDA wishes to accommodate a broad variety of electronic signatures and is therefore revising § 11.100(b) to require that an organization verify the identity of an individual before it establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature or any element of such electronic signatures.

118. One comment suggested that the word "verified" in proposed § 11.100(b) be changed to "confirmed." Other comments addressed the method of verifying a person's identity and suggested that the section specify acceptable verification methods, including high level procedures regarding the relative strength of that verification, and the need for personal appearances or supporting documentation such as birth certificates. Two comments said the verification provision should be deleted because normal internal controls are adequate. and that it was impractical for multinational companies whose employees are globally dispersed.

The agency does not believe that there is a sufficient difference between "verified" and "confirmed" to warrant a change in this section. Both words indicate that organizations substantiate a person's identity to prevent impersonations when an electronic signature, or any of its elements, is being established or certified. The agency disagrees with the assertion that this requirement is unnecessary. Without verifying someone's identity at the outset of establishing or certifying

an individual's electronic signature, or a scope and burden of certification to a portion thereof, an imposter might easily access and compromise many records. Moreover, an imposter could continue this activity for a prolonged period of time despite other system controls, with potentially serious consequences.

The agency does not believe that the size of an organization, or global dispersion of its employees, is reason to abandon this vital control. Such dispersion may, in fact, make it easier for an impostor to pose as someone else in the absence of such verification. Further, the agency does not accept the implication that multinational firms would not verify the identity of their employees as part of other routine procedures, such as when individuals are first hired.

In addition, in cases where an organization is widely dispersed and electronic signatures are established or certified centrally, § 11.100(b) does not prohibit organizations from having their local units perform the verification and relaying this information to the central authority. Similarly, local units may conduct the electronic signature assignment or certification.

FDA does not believe it is necessary at this time to specify methods of identity verification and expects that organizations will consider risks attendant to sanctioning an erroneously assigned electronic signature.

119. Proposed § 11.100(c) states that persons using electronic signatures must certify to the agency that their electronic signature system guarantees the authenticity, validity, and binding nature of any electronic signature. Persons utilizing electronic signatures would, upon agency request, provide additional certification or testimony that a specific electronic signature is authentic, valid, and binding. Such certification would be submitted to the FDA district office in which territory the electronic signature system is in use.

Many comments objected to the proposed requirement that persons provide FDA with certification regarding their electronic signature systems. The comments asserted that the requirement was: (1) Unprecedented, (2) unrealistic, (3) unnecessary, (4) contradictory to the principles and intent of system validation, (5) too burdensome for FDA to manage logistically, (6) apparently intended only to simplify FDA litigation, (7) impossible to meet regarding "guarantees" of authenticity, and (8) an apparent substitute for FDA inspections.

FDA agrees in part with these comments. This final rule reduces the

statement of intent that electronic signatures are the legally binding equivalent of handwritten signatures.

As noted previously, the agency believes it is important, within the context of its health protection activities, to ensure that persons who implement electronic signatures fully equate the legally binding nature of electronic signatures with the traditional handwritten paper-based signatures. The agency is concerned that individuals might disavow an electronic signature as something completely different from a traditional handwritten signature. Such contention could result in confusion and possibly extensive litigation.

Moreover, a limited certification as provided in this final rule is consistent with other legal, regulatory, and commercial practices. For example, electronic data exchange trading partner agreements are often written on paper and signed with traditional handwritten signatures to establish that certain electronic identifiers are recognized as equivalent to traditional handwritten signatures.

FDA does not expect electronic signature systems to be guaranteed foolproof. The agency does not intend, under § 11.100(c), to establish a requirement that is unattainable. Certification of an electronic signature system as the legally binding equivalent of a traditional handwritten signature is separate and distinct from system validation. This provision is not intended as a substitute for FDA inspection and such inspection alone may not be able to determine in a conclusive manner an organization's intent regarding electronic signature

equivalency. The agency has revised proposed §11.100(c) to clarify its intent. The agency wishes to emphasize that the final rule dramatically curtails what FDA had proposed and is essential for the agency to be able to protect and promote the public health because FDA must be able to hold people to the commitments they make under their electronic signatures. The certification in the final rule is merely a statement of intent that electronic signatures are the legally binding equivalent of traditional handwritten signatures.

120. Several comments questioned the procedures necessary for submitting the certification to FDA, including: (1) The scheduling of the certification; (2) whether to submit certificates for each individual or for each electronic signature; (3) the meaning of "territory" in the context of wide area networks; (4) whether such certificates could be

submitted electronically; and (5) whether organizations, after submitting a certificate, had to wait for a response from FDA before implementing their electronic signature systems. Two comments suggested revising proposed § 11.100(c) to require that all certifications be submitted to FDA only upon agency request. One comment suggested changing "should" to "shall" in the last sentence of § 11.100(c) if the agency's intent is to require certificates to be submitted to the respective FDA district office.

The agency intends that certificates be submitted once, in the form of a paper letter, bearing a traditional handwritten signature, at the time an organization first establishes an electronic signature system after the effective date of part 11, or, where such systems have been used before the effective date, upon continued use of the electronic signature system.

A separate certification is not needed for each electronic signature, although certification of a particular electronic signature is to be submitted if the agency requests it. The agency does not intend to establish certification as a review and approval function. In addition, organizations need not await FDA's response before putting electronic signature systems into effect. or before continuing to use an existing system.

A single certification may be stated in broad terms that encompass electronic signatures of all current and future employees, thus obviating the need for subsequent certifications submitted on a preestablished schedule.

To further simplify the process and to minimize the number of certifications that persons would have to provide, the agency has revised § 11.100(c) to permit submission of a single certification that covers all electronic signatures used by an organization. The revised rule also simplifies the process by providing a single agency receiving unit. The final rule instructs persons to send certifications to FDA's Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. Persons outside the United States may send their certifications to the same office.

The agency offers, as guidance, an example of an acceptable § 11.100(c) certification:

Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that [name of organization] intends that all electronic signatures executed by our employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten

The agency has revised § 11.100 to clarify where and when certificates are to be submitted.

The agency does not agree that the initial certification be provided only upon agency request because FDA believes it is vital to have such certificates, as a matter of record, in advance of any possible litigation. This would clearly establish the intent of organizations to equate the legally binding nature of electronic signatures with traditional handwritten signatures. In addition, the agency believes that having the certification on file ahead of time will have the beneficial effect of reinforcing the gravity of electronic signatures by putting an organization's employees on notice that the organization has gone on record with FDA as equating electronic signatures with handwritten signatures.

121. One comment suggested that proposed §11.100(c) be revised to exclude from certification instances in which the purported signer claims that he or she did not create or authorize the signature.

The agency declines to make this revision because a provision for nonrepudiation is already contained in § 11.10.

As a result of the considerations discussed in comments 119 and 120 of this document, the agency has revised proposed § 11.100(c) to state that:

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

XII. Electronic Signature Components and Controls (§ 11.200)

122. Proposed § 11.200 sets forth requirements for electronic signature identification mechanisms and controls. Two comments suggested that the term "identification code" should be defined. Several comments suggested that the term "identification mechanisms" should be changed to "identification components" because each component of an electronic signature need not be executed by a different mechanism.

The agency believes that the term "identification code" is sufficiently broad and generally understood and

does not need to be defined in these regulations. FDA agrees that the word "component" more accurately reflects the agency's intent than the word "mechanism," and has substituted "component" for "mechanism" in revised § 11.200. The agency has also revised the section heading to read "Electronic signature components and controls" to be consistent with the wording of the section.

123. Proposed § 11.200(a) states that electronic signatures not based upon biometric/behavioral links must: (1) Employ at least two distinct identification mechanisms (such as an identification code and password), each of which is contemporaneously executed at each signing; (2) be used only by their genuine owners; and (3) be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Two comments said that proposed § 11.200(a) should acknowledge that passwords may be known not only to their genuine owners, but also to system administrators in case people forget their passwords.

The agency does not believe that system administrators would routinely need to know an individual's password because they would have sufficient privileges to assist those individuals who forget passwords.

124. Several comments argued that the agency should accept a single password alone as an electronic signature because: (1) Combining the password with an identification code adds little security, (2) administrative controls and passwords are sufficient, (3) authorized access is more difficult when two components are needed, (4) people would not want to gain unauthorized entry into a manufacturing environment, and (5) changing current systems that use only a password would be costly.

The comments generally addressed the need for two components in electronic signatures within the context of the requirement that all components be used each time an electronic signature is executed. Several comments suggested that, for purposes of system access, individuals should enter both a user identification code and password, but that, for subsequent signings during one period of access, a single element (such as a password) known only to, and usable by, the individual should be sufficient.

The agency believes that it is very important to distinguish between those (nonbiometric) electronic signatures that components of a nonbiometric

are executed repetitively during a single, continuous controlled period of time (access session or logged-on period) and those that are not. The agency is concerned, from statements made in comments, that people might use passwords that are not always unique and are frequently words that are easily associated with an individual. Accordingly, where nonbiometric electronic signatures are not executed repetitively during a single, continuous controlled period, it would be extremely bad practice to use a password alone as an electronic signature. The agency believes that using a password alone in such cases would clearly increase the likelihood that one individual, by chance or deduction, could enter a password that belonged to someone else and thereby easily and readily impersonate that individual. This action could falsify electronic records.

The agency acknowledges that there are some situations involving repetitive signings in which it may not be necessary for an individual to execute each component of a nonbiometric electronic signature for every signing. The agency is persuaded by the comments that such situations generally involve certain conditions. For example, an individual performs an initial system access or "log on," which is effectively the first signing, by executing all components of the electronic signature (typically both an identification code and a password). The individual then performs subsequent signings by executing at least one component of the electronic signature, under controlled conditions that prevent another person from impersonating the legitimate signer. The agency's concern here is the possibility that, if the person leaves the workstation, someone else could access the workstation (or other computer device used to execute the signing) and impersonate the legitimate signer by entering an identification code or password.

The agency believes that, in such situations, it is vital to have stringent controls in place to prevent the impersonation. Such controls include: (1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would "de-log" the first individual if no entries or actions were taken within a fixed short timeframe: and (3) requiring that the single component needed for subsequent signings be known to, and usable only by, the authorized individual.

The agency's objective in accepting the execution of fewer than all the

	l
	(
	l
	l
	l
	•

13458 Federal Register / Vol. 62, No. 54 / Thursday, March 20, 1997 / Rules and Regulations

electronic signature for repetitive signings is to make it impractical to falsify records. The agency believes that this would be attained by complying with all of the following procedures where nonbiometric electronic signatures are executed more than once during a single, continuous controlled session: (1) All electronic signature components are executed for the first signing; (2) at least one electronic signature component is executed at each subsequent signing; (3) the electronic signature component executed after the initial signing is only used by its genuine owner, and is designed to ensure it can only be used by its genuine owner; and (4) the electronic signatures are administered and executed to ensure that their attempted use by anyone other than their genuine owners requires collaboration of two or more individuals. Items 1 and 4 are already incorporated in proposed § 11.200(a). FDA has included items 2 and 3 in final § 11.200(a).

The agency cautions, however, that if its experience with enforcement of part 11 demonstrates that these controls are insufficient to deter falsifications, FDA may propose more stringent controls.

125. One comment asserted that, if the agency intends the term "identification code" to mean the typical user identification, it should not characterize the term as a distinct mechanism because such codes do not necessarily exhibit security attributes. The comment also suggested that proposed § 11.200(a) address the appropriate application of each possible combination of a twofactor authentication method.

The agency acknowledges that the identification code alone does not exhibit security attributes. Security derives from the totality of system controls used to prevent falsification. However, uniqueness of the identification code when combined with another electronic signature component, which may not be unique (such as a password), makes the combination unique and thereby enables a legitimate electronic signature. FDA does not now believe it necessary to address, in §11.200(a), the application of all possible combinations of multifactored authentication methods.

126. One comment requested clarification of "each signing," noting that a laboratory employee may enter a group of test results under one signing.

The agency advises that each signing means each time an individual executes a signature. Particular requirements regarding what records need to be signed derive from other regulations. not part 11. For example, in the case of

a laboratory employee who performs a number of analytical tests, within the context of drug CGMP regulations, it is permissible for one signature to indicate the performance of a group of tests (21 CFR 211.194(a) (7)). A separate signing is not required in this context for each separate test as long as the record clearly shows that the single signature means the signer performed all the tests.

127. One comment suggested that the proposed requirement, that collaboration of at least two individuals is needed to prevent attempts at electronic signature falsification, be deleted because a responsible person should be allowed to override the electronic signature of a subordinate. Several comments addressed the phrase "attempted use" and suggested that it be deleted or changed to "unauthorized use." The comments said that willful breaking or circumvention of any security measure does not require two or more people to execute, and that the central question is whether collaboration is required to use the electronic signature.

The agency advises that the intent of the collaboration provision is to require that the components of a nonbiometric electronic signature cannot be used by one individual without the prior knowledge of a second individual. One type of situation the agency seeks to prevent is the use of a component such as a card or token that a person may leave unattended. If an individual must collaborate with another individual by disclosing a password, the risks of betrayal and disclosure are greatly increased and this helps to deter such actions. Because the agency is not condoning such actions, § 11.200(a)(2) requires that electronic signatures be used only by the genuine owner. The agency disagrees with the comments that the term "attempted use" should be changed to "unauthorized uses," because "unauthorized uses" could infer that use of someone else's electronic signature is acceptable if it is authorized.

Regarding electronic signature "overrides," the agency would consider 92N-0251, and includes as falsification the act of substituting the recommendations from public signature of a supervisor for that of a subordinate. The electronic signature of the subordinate must remain inviolate for purposes of authentication and documentation. Although supervisors may overrule the actions of their staff. the electronic signatures of the subordinates must remain a permanent part of the record, and the supervisor's own electronic signature must appear separately. The agency believes that such an approach is fully consistent with procedures for paper records.

As a result of the revisions noted in comments 123 to 127 of this document, § 11.200(a) now reads as follows:

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single. continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners:

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

128. Proposed § 11.200(b) states that electronic signatures based upon biometric/behavioral links be designed to ensure that they could not be used by anyone other than their genuine owners.

One comment suggested that the agency make available, by public workshop or other means, any information it has regarding existing biometric systems so that industry can provide proper input. Another comment asserted that proposed § 11.200(b) placed too great an emphasis on biometrics, did not establish particular levels of assurance for biometrics, and did not provide for systems using mixtures of biometric and nonbiometric electronic signatures. The comment recommended revising the phrase "designed to ensure they cannot be used" to read "provide assurances that prevent their execution.'

The agency's experience with biometric electronic signatures is contained in the administrative record for this rulemaking, under docket no. comments to the ANPRM and the proposed rule. The agency has also gathered, and continues to gather, additional information from literature reviews, general press reports, meetings, and the agency's experience with this technology. Interested persons have had extensive opportunity for input and comment regarding biometrics in part 11. In addition, interested persons may continue to contact the agency at any time regarding biometrics or any other relevant technologies. The agency notes

that the rule does not require the use of biometric-based electronic signatures.

As the agency's experience with biometric electronic signatures increases, FDA will consider holding or participating in public workshops if that approach would be helpful to those wishing to adopt such technologies to comply with part 11.

The agency does not believe that proposed § 11.200(b) places too much emphasis on biometric electronic signatures. As discussed above, the regulation makes a clear distinction between electronic signatures that are and are not based on biometrics, but treats their acceptance equally.

The agency recognizes the inherent security advantages of biometrics, however, in that record falsification is more difficult to perform. System controls needed to make biometricbased electronic signatures reliable and trustworthy are thus different in certain respects from controls needed to make nonbiometric electronic signatures reliable and trustworthy. The requirements in part 11 reflect those differences.

The agency does not believe that it is necessary at this time to set numerical security assurance standards that any system would have to meet.

The regulation does not prohibit individuals from using combinations of biometric and nonbiometric-based electronic signatures. However, when combinations are used, FDA advises that requirements for each element in the combination would also apply. For example, if passwords are used in combination with biometrics, then the benefits of using passwords would only be realized, in the agency's view, by adhering to controls that ensure password integrity (see § 11.300).

In addition, the agency believes that the phrase "designed to ensure that they cannot be used" more accurately reflects the agency's intent than the suggested alternate wording, and is more consistent with the concept of systems validation. Under such validation, falsification preventive attributes would be designed into the biometric systems.

To be consistent with the revised definition of biometrics in § 11.3(b)(3), the agency has revised § 11.200(b) to read, "Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners."

XIII. Electronic Signatures—Controls for Identification Čodes/Passwords (§ 11.300)

The introductory paragraph of proposed § 11.300 states that electronic signatures based upon use of

identification codes in combination ensure their security and integrity.

To clarify the intent of this provision, the agency has added the words "[p]ersons who use" to the first sentence of § 11.300. This change is consistent with §§ 11.10 and 11.30. The introductory paragraph now reads, "Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: * * *."

129. One comment suggested deletion of the phrase "in combination with passwords" from the first sentence of this section.

The agency disagrees with the suggested revision because the change is inconsistent with FDA's intent to address controls for electronic signatures based on combinations of identification codes and passwords, and would, in effect, permit a single component nonbiometric-based electronic signature.

130. Proposed § 11.300(a) states that controls for identification codes/ passwords must include maintaining the uniqueness of each issuance of identification code and password.

One comment alleged that most passwords are commonly used words, such as a child's name, a State, city, street, month, holiday, or date, that are significant to the person who creates the password. Another stated that the rule should explain uniqueness and distinguish between issuance and use because identification code/password combinations generally do not change for each use.

FDA does not intend to require that individuals use a completely different identification code/password combination each time they execute an electronic signature. For reasons explained in the response to comment 16, what is required to be unique is each combined password and identification code and FDA has revised the wording of § 11.300(a) to clarify this provision. The agency is aware, however, of identification devices that generate new passwords on a continuous basis in synchronization with a "host' computer. This results in unique passwords for each system access. Thus, it is possible in theory to generate a unique nonbiometric electronic signature for each signing.

The agency cautions against using passwords that are common words easily associated with their originators because such a practice would make it relatively easy for someone to impersonate someone else by guessing

the password and combining it with an with passwords must employ controls to unsecured (or even commonly known) identification code.

131. Proposed § 11.300(b) states that controls for identification codes/ passwords must ensure that code/ password issuances are periodically checked, recalled, or revised.

Several comments objected to this proposed requirement because: (1) It is unnecessary, (2) it excessively prescribes "how to," (3) it duplicates the requirements in § 11.300(c), and (4) it is administratively impractical for larger organizations. However, the comments said individuals should be encouraged to change their passwords periodically. Several comments suggested that proposed § 11.300(b) include a clarifying example such as "to cover events such as password aging.' One comment said that the section should indicate who is to perform the periodic checking, recalling, or revising.

The agency disagrees with the objections to this provision. FDA does not view the provision as a "how to" because organizations have full flexibility in determining the frequency and methods of checking, recalling, or revising their code/password issuances. The agency does not believe that this paragraph duplicates the regulation in § 11.300(c) because paragraph (c) specifically addresses followup to losses of electronic signature issuances, whereas § 11.300(b) addresses periodic issuance changes to ensure against their having been unknowingly compromised. This provision would be met by ensuring that people change their passwords periodically.

FDA disagrees that this system control is unnecessary or impractical in large organizations because the presence of more people may increase the opportunities for compromising identification codes/passwords. The agency is confident that larger organizations will be fully capable of handling periodic issuance checks. revisions, or recalls.

FDA agrees with the comments that suggested a clarifying example and has revised § 11.300(b) to include password aging as such an example. The agency cautions, however, that the example should not be taken to mean that password expiration would be the only rationale for revising, recalling, and checking issuances. If, for example, identification codes and passwords have been copied or compromised, they should be changed.

FDA does not believe it necessary at this time to specify who in an organization is to carry out this system control, although the agency expects

that units that issue electronic

signatures would likely have this duty. 132. Proposed § 11.300(c) states that controls for identification codes/passwords must include the following of loss management procedures to electronically deauthorize lost tokens, cards, etc., and to issue temporary or permanent replacements using suitable, rigorous controls for substitutes.

One comment suggested that this section be deleted because it excessively prescribes "how to." Another comment argued that the proposal was not detailed enough and should distinguish among fundamental types of cards (e.g., magstripe, integrated circuit, and optical) and include separate sections that address their respective use. Two comments questioned why the proposal called for "rigorous controls" in this section as opposed to other sections. One of the comments recommended that this section should also apply to cards or devices that are stolen as well as lost.

The agency believes that the requirement that organizations institute loss management procedures is neither too detailed nor too general. Organizations retain full flexibility in establishing the details of such procedures. The agency does not believe it necessary at this time to offer specific provisions relating to different types of cards or tokens. Organizations that use such devices retain full flexibility to establish appropriate controls for their operations. To clarify the agency's broad intent to cover all types of devices that contain or generate identification code or password information. FDA has revised § 11.300(c) to replace "etc." with "and other devices that bear or generate identification code or password information.'

The agency agrees that § 11.300(c) should cover loss management procedures regardless of how devices become potentially compromised, and has revised this section by adding, after the word "lost," the phrase "stolen, missing, or otherwise potentially compromised." FDA uses the term "rigorous" because device disappearance may be the result of inadequate controls over the issuance and management of the original cards or devices, thus necessitating more stringent measures to prevent problem recurrence. For example, personnel training on device safekeeping may need to be strengthened.

133. Proposed § 11.300(d) states that controls for identification codes/passwords must include the use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and, detecting and reporting to the system security unit and

organizational management in an emergent manner any attempts at their unauthorized use.

Several comments suggested that the term "emergent" in proposed § 11.300(d) be replaced with "timely" to describe reports regarding attempted unauthorized use of identification codes/passwords because: (1) A timely report would be sufficient, (2) technology to report emergently is not available, and (3) timely is a more recognizable and common term.

FDA agrees in part. The agency considers attempts at unauthorized use of identification codes and passwords to be extremely serious because such attempts signal potential electronic signature and electronic record falsification, data corruption, or worse consequences that could also ultimately be very costly to organizations. In FDA's view, the significance of such attempts requires the immediate and urgent attention of appropriate security personnel in the same manner that individuals would respond to a fire alarm. To clarify its intent with a more widely recognized term, the agency is replacing "emergent" with "immediate and urgent" in the final rule. The agency believes that the same technology that accepts or rejects an identification code and password can be used to relay to security personnel an appropriate message regarding attempted misuse.

134. One comment suggested that the word "any" be deleted from the phrase "any attempts" in proposed § 11.300(d) because it is excessive. Another comment, noting that the question of attempts to enter a system or access a file by unauthorized personnel is very serious, urged the agency to substitute "all" for "any." This comment added that there are devices on the market that can be used by unauthorized individuals to locate personal identification codes and passwords.

The agency believes the word "any" is sufficiently broad to cover all attempts at misuse of identification codes and passwords, and rejects the suggestion to delete the word. If the word "any" were deleted, laxity could result from any inference that persons are less likely to be caught in an essentially permissive, nonvigilant system. FDA is aware of the "sniffing" devices referred to by one comment and cautions persons to establish suitable countermeasures against them.

135. One comment suggested that proposed § 11.300(d) be deleted because it is impractical, especially when simple typing errors are made. Another suggested that this section pertain to access to electronic records, not just the

system, on the basis that simple miskeys may be typed when accessing a system.

As discussed in comments 133 and 134 of this document, the agency believes this provision is necessary and reasonable. The agency's security concerns extend to system as well as record access. Once having gained unauthorized system access, an individual could conceivably alter passwords to mask further intrusion and misdeeds. If this section were removed, falsifications would be more probable to the extent that some establishments would not alert security personnel.

However, the agency advises that a simple typing error may not indicate an unauthorized use attempt, although a pattern of such errors, especially in short succession, or such an apparent error executed when the individual who "owns" that identification code or password is deceased, absent, or otherwise known to be unavailable, could signal a security problem that should not be ignored. FDA notes that this section offers organizations maximum latitude in deciding what they perceive to be attempts at unauthorized use.

136. One comment suggested substituting the phrase "electronic signature" for "passwords and/or identification codes."

The agency disagrees with this comment because the net effect of the revision might be to ignore attempted misuse of important elements of an electronic signature such as a "password" attack on a system.

137. Several comments argued that:
(1) It is not necessary to report misuse attempts simultaneously to management when reporting to the appropriate security unit, (2) security units would respond to management in accordance with their established procedures and lines of authority, and (3) management would not always be involved.

The agency agrees that not every misuse attempt would have to be reported simultaneously to an organization's management if the security unit that was alerted responded appropriately. FDA notes, however, that some apparent security breeches could be serious enough to warrant management's immediate and urgent attention. The agency has revised proposed § 11.300(d) to give organizations maximum flexibility in establishing criteria for management notification. Accordingly, § 11.300(d) now states that controls for identification codes/passwords must include:

Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report

Federal Register / Vol. 62, No. 54 / Thursday, March 20, 1997 / Rules and Regulations

in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

138. Proposed § 11.300(e) states that controls for identification codes/ passwords must include initial and periodic testing of devices, such as tokens or cards, bearing identifying information, for proper function.

Many comments objected to this proposed device testing requirement as unnecessary because it is part of system validation and because devices are access fail-safe in that nonworking devices would deny rather than permit system access. The comments suggested revising this section to require that failed devices deny user access. One comment stated that § 11.300(e) is unclear on the meaning of "identifying information" and that the phrase "tokens or cards" is redundant because cards are a form of tokens.

FDA wishes to clarify the reason for this proposed requirement, and to emphasize that proper device functioning includes, in addition to system access, the correctness of the identifying information and security performance attributes. Testing for system access alone could fail to discern significant unauthorized device alterations. If, for example, a device has been modified to change the identifying information, system access may still be allowed, which would enable someone to assume the identity of another person. In addition, devices may have been changed to grant individuals additional system privileges and action authorizations beyond those granted by the organization. Of lesser significance would be simple wear and tear on such devices, which result in reduced performance. For instance, a bar code may not be read with the same consistent accuracy as intended if the code becomes marred, stained, or otherwise disfigured. Access may be granted, but only after many more scannings than desired. The agency expects that device testing would detect

Because validation of electronic signature systems would not cover unauthorized device modifications, or subsequent wear and tear, validation would not obviate the need for periodic

The agency notes that § 11.300(e) does not limit the types of devices organizations may use. In addition, not all tokens may be cards, and identifying information is intended to include identification codes and passwords. Therefore, FDA has revised proposed § 11.300(e) to clarify the agency's intent and to be consistent with § 11.300(c). Revised § 11.300(e) requires initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

XIV. Paperwork Reduction Act of 1995

This final rule contains information collection provisions that are subject to review by the Office of Management and Budget (OMB) under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501-3520). Therefore, in accordance with 5 CFR 1320, the title, description, and description of respondents of the collection of information requirements are shown below with an estimate of the annual reporting and recordkeeping burdens. Included in the estimate is the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

Most of the burden created by the information collection provision of this final rule will be a one-time burden associated with the creation of standard operating procedures, validation, and certification. The agency anticipates the use of electronic media will substantially reduce the paperwork burden associated with maintaining FDA-required records.

Title: Electronic records; Electronic signatures.

Description: FDA is issuing regulations that provide criteria for acceptance of electronic records. electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records. Rules apply to any FDA records requirements unless specific restrictions are issued in the future. Records required to be submitted to FDA may be submitted electronically, provided the agency has stated its ability to accept the records electronically in an agency established public docket.

Description of Respondents: Businesses and other for-profit organizations, state or local governments, Federal agencies, and nonprofit institutions.

Although the August 31, 1994, proposed rule (59 FR 45160) provided a 90-day comment period under the Paperwork Reduction Act of 1980, FDA is providing an additional opportunity for public comment under the Paperwork Reduction Act of 1995. which was enacted after the expiration of the comment period and applies to this final rule. Therefore, FDA now invites comments on: (1) Whether the proposed collection of information is necessary for the proper performance of FDA's functions, including whether the information will have practical utility: (2) the accuracy of FDA's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used: (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques, when appropriate, and other forms of information technology. Individuals and organizations may submit comments on the information collection provisions of this final rule by May 19, 1997. Comments should be directed to the Dockets Management Branch (address

At the close of the 60-day comment period, FDA will review the comments received, revise the information collection provisions as necessary, and submit these provisions to OMB for review and approval. FDA will publish a notice in the Federal Register when the information collection provisions are submitted to OMB, and an opportunity for public comment to OMB will be provided at that time. Prior to the effective date of this final rule, FDA will publish a notice in the Federal Register of OMB's decision to approve, modify, or disapprove the information collection provisions. An agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

TABLE 1.—ESTIMATED ANNUAL RECORDKEEPING BURDEN

	21 CFR Section	Annual No. of Recordkeepers	Hours per Recordkeeper	Total Hours
11.10		50	40	2,000
11.30		50	40	2,000
11.50		50	40	2,000

Federal Register / Vol. 62, No. 54 / Thursday, March 20, 1997 / Rules and Regulations

TABLE 1.—ESTIMATED ANNUAL RECORDKEEPING BURDEN—Continued

21 CFR Section	Annual No. of Recordkeepers	Hours per Recordkeeper	Total Hours
11.300 Total annual burden hours	50	40	2,000 8,000

TABLE 2.—ESTIMATED ANNUAL REPORTING BURDEN

21 CFR Section	Annual No. of Respondents	Hours per Response	Total Burden Hours	
11.100 Total annual burden hours	1,000	1	1,000 1,000	

XV. Environmental Impact

The agency has determined under 21 CFR 25.24(a)(8) that this action is of a type that does not individually or cumulatively have a significant effect on the human environment. Therefore, neither an environmental assessment nor an environmental impact statement is required.

XVI. Analysis of Impacts

FDA has examined the impacts of the final rule under Executive Order 12866. under the Regulatory Flexibility Act (5 U.S.C. 601-612), and under the Unfunded Mandates Reform Act (Pub. L. 104-4). Executive Order 12866 directs agencies to assess all costs and benefits of available regulatory alternatives and, when regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety, and other advantages; and distributive impacts and equity). Unless an agency certifies that a rule will not have a significant economic impact on a substantial number of small entities, the Regulatory Flexibility Act requires an analysis of regulatory options that would minimize any significant impact of a rule on small entities. The Unfunded Mandates Reform Act requires that agencies prepare an assessment of anticipated costs and benefits before proposing any rule that may result in an annual expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of \$100 million (adjusted annually for inflation).

The agency believes that this final rule is consistent with the regulatory philosophy and principles identified in the Executive Order. This rule permits persons to maintain any FDA required record or report in electronic format. It also permits FDA to accept electronic records, electronic signatures, and handwritten signatures executed to

records and handwritten signatures executed on paper. The rule applies to any paper records required by statute or agency regulations. The rule was substantially influenced by comments to the ANPRM and the proposed rule. The provisions of this rule permit the use of electronic technology under conditions that the agency believes are necessary to ensure the integrity of electronic systems, records, and signatures, and the ability of the agency to protect and promote the public health.

This rule is a significant regulatory action as defined by the Executive Order and is subject to review under the Executive Order. This rule does not impose any mandates on State, local, or tribal governments, nor is it a significant regulatory action under the Unfunded Mandates Reform Act.

The activities regulated by this rule are voluntary; no entity is required by this rule to maintain or submit records electronically if it does not wish to do so. Presumably, no firm (or other regulated entity) will implement electronic recordkeeping unless the benefits to that firm are expected to exceed any costs (including capital and maintenance costs). Thus, the industry will incur no net costs as a result of this rule.

Based on the fact that the activities regulated by this rule are entirely voluntary and will not have any net adverse effects on small entities, the Commissioner of Food and Drugs certifies that this rule will not have a significant economic impact on a substantial number of small entities. Therefore, under the Regulatory Flexibility Act, no further regulatory flexibility analysis is required.

Although no further analysis is required, in developing this rule, FDA has considered the impact of the rule on small entities. The agency has also considered various regulatory options to number is substantial. For example, maximize the net benefits of the rule to within the medical devices industry small entities without compromising the alone, the Small Business

electronic records as equivalent to paper integrity of electronic systems, records, and signatures, or the agency's ability to protect and promote the public health. The following analysis briefly examines the potential impact of this rule on small businesses and other small entities, and describes the measures that FDA incorporated in this final rule to reduce the costs of applying electronic record/signature systems consistent with the objectives of the rule. This analysis includes each of the elements required for a final regulatory flexibility analysis under 5 U.S.C. 604(a).

A. Objectives

The purpose of this rule is to permit the use of a technology that was not contemplated when most existing FDA regulations were written, without undermining in any way the integrity of records and reports or the ability of FDA to carry out its statutory health protection mandate. The rule will permit regulated industry and FDA to operate with greater flexibility, in ways that will improve both the efficiency and the speed of industry's operations and the regulatory process. At the same time, it ensures that individuals will assign the same level of importance to affixing an electronic signature, and the records to which that signature attests, as they currently do to a handwritten signature.

B. Small Entities Affected

This rule potentially affects all large and small entities that are required by any statute administered by FDA, or any FDA regulation, to keep records or make reports or other submissions to FDA, including small businesses, nonprofit organizations, and small government entities. Because the rule affects such a broad range of industries, no data currently exist to estimate precisely the total number of small entities that will potentially benefit from the rule, but the

Administration (SBA) estimates that over 3,221 firms are small businesses (i.e., have fewer than 500 employees). SBA also estimates that 504 pharmaceutical firms are small businesses with fewer than 500 employees. Of the approximately 2,204 registered blood and plasma establishments that are neither government-owned nor part of the American Red Cross, most are nonprofit establishments that are not nationally dominant and thus may be small entities as defined by the Regulatory Flexibility Act.

Not all submissions will immediately be acceptable electronically, even if the submission and the electronic record conform to the criteria set forth in this rule. A particular required submission will be acceptable in electronic form only after it has been identified to this effect in public docket 92S-0251. (The agency unit that can receive that electronic submission will also be identified in the docket.) Thus, although all small entities subject to FDA regulations are potentially affected by this rule, the rule will actually only benefit those that: (1) Are required to submit records or other documents that have been identified in the public docket as acceptable if submitted electronically, and (2) choose this method of submission, instead of traditional paper record submissions. The potential range of submissions includes such records as new drug applications, medical device premarket notifications, food additive petitions, and medicated feed applications. These, and all other required submissions, will be considered by FDA as candidates for optional electronic format.

Although the benefits of making electronic submissions to FDA will be phased in over time, as the agency accepts more submissions in electronic date, immediately benefit from using electronic records/signatures for records they are required to keep, but not submit to FDA. Such records include, but are not limited to: Pharmaceutical and medical device batch production records, complaint records, and food

processing records.

Some small entities will be affected by this rule even if they are not among the industries regulated by FDA. Because it will increase the market demand for certain types of software (e.g., document management, signature. and encryption software) and services (e.g., digital notaries and digital signature certification authorities), this rule will benefit some small firms engaged in developing and providing those products and services.

C. Description of the Impact

For any paper record that an entity is required to keep under existing statutes or FDA regulations, FDA will now accept an electronic record instead of a paper one, as long as the electronic record conforms to the requirements of this rule. FDA will also consider an electronic signature to be equivalent to a handwritten signature if it meets the requirements of this rule. Thus, entities regulated by FDA may, if they choose, submit required records and authorizations to the agency electronically once those records have been listed in the docket as acceptable in electronic form. This action is voluntary; paper records and handwritten signatures are still fully acceptable. No entity will be required to change the way it is currently allowed to submit paper records to the agency.

1. Benefits and costs

For any firm choosing to convert to electronic recordkeeping, the direct benefits are expected to include:

- (1) Improved ability for the firm to analyze trends, problems, etc.. enhancing internal evaluation and quality control:
- (2) Reduced data entry errors, due to automated checks;
- (3) Reduced costs of storage space; (4) Reduced shipping costs for data transmission to FDA; and

(5) More efficient FDA reviews and approvals of FDA-regulated products.

No small entity will be required to convert to electronic submissions. Furthermore, it is expected that no individual firm, or other entity, will choose the electronic option unless that firm finds that the benefits to the firm from conversion will exceed any conversion costs.

There may be some small entities that form, firms can, upon the rule's effective currently submit records on paper, but archive records electronically. These entities will need to ensure that their existing electronic systems conform to the requirements for electronic recordkeeping described in this rule. Once they have done so, however, they may also take advantage of all the other benefits of electronic recordkeeping. Therefore, no individual small entity is expected to experience direct costs that exceed benefits as a result of this rule.

Furthermore, because almost all of the rule's provisions reflect contemporary security measures and controls that respondents to the ANPRM identified. most firms should have to make few, if any, modifications to their systems.

For entities that do choose electronic recordkeeping, the magnitude of the costs associated with doing so will

depend on several factors, such as the level of appropriate computer hardware and software already in place in a given firm, the types of conforming technologies selected, and the size and dispersion of the firm. For example, biometric signature technologies may be more expensive than nonbiometric technologies; firms that choose the former technology may encounter relatively higher costs. Large, geographically dispersed firms may need some institutional security procedures that smaller firms, with fewer persons in more geographically concentrated areas, may not need. Firms that require wholesale technology replacements in order to adopt electronic record/signature technology may face much higher costs than those that require only minor modifications (e.g., because they already have similar technology for internal security and quality control purposes). Among the firms that must undertake major changes to implement electronic recordkeeping, costs will be lower for those able to undertake these changes simultaneously with other planned computer and security upgrades. New firms entering the market may have a slight advantage in implementing technologies that conform with this rule, because the technologies and associated procedures can be put in place as part of the general startup.

2. Compliance requirements

If a small entity chooses to keep electronic records and/or make electronic submissions, it must do so in ways that conform to the requirements for electronic records and electronic signatures set forth in this rule. These requirements, described previously in section II. of this document, involve measures designed to ensure the integrity of system operations, of information stored in the system, and of the authorized signatures affixed to electronic records. The requirements apply to all small (and large) entities in all industry sectors regulated by FDA.

The agency believes that because the rule is flexible and reflects contemporary standards, firms should have no difficulty in putting in place the needed systems and controls. However, to assist firms in meeting the provisions of this rule, FDA may hold public meetings and publish more detailed guidance. Firms may contact FDA's Industry and Small Business Liaison Staff, HF-50, at 5600 Fishers Lane, Rockville, MD 20857 (301-827-3430) for more information.

3. Professional skills required

If a firm elects electronic recordkeeping and submissions, it must take steps to ensure that all persons involved in developing, maintaining, and using electronic records and electronic signature systems have the education, training, and experience to perform the tasks involved. The level of training and experience that will be required depends on the tasks that the person performs. For example, an individual whose sole involvement with electronic records is infrequent might only need sufficient training to understand and use the required procedures. On the other hand, an individual involved in developing an electronic record system for a firm wishing to convert from a paper recordkeeping system would probably need more education or training in computer systems and software design and implementation. In addition, FDA expects that such a person would also have specific on-the-job training and experience related to the particular type of records kept by that firm.

The relevant education, training, and experience of each individual involved in developing, maintaining, or using electronic records/submissions must be documented. However, no specific examinations or credentials for these individuals are required by the rule.

D. Minimizing the Burden on Small Entities

This rule includes several conditions that an electronic record or signature must meet in order to be acceptable as an alternative to a paper record or handwritten signature. These conditions are necessary to permit the agency to protect and promote the public health. For example, FDA must retain the ability to audit records to detect unauthorized modifications, simple errors, and to deter falsification. Whereas there are many scientific techniques to show changes in paper records (e.g., analysis of the paper, signs of erasures, and handwriting analysis), these methods do not apply to electronic records. For electronic records and submissions to have the same integrity as paper records, they must be developed, maintained, and used under circumstances that make it difficult for them to be inappropriately modified. Without these assurances, FDA's objective of enabling electronic records and signatures to have standing equal to paper records and handwritten signatures, and to satisfy the requirements of existing statutes and regulations, cannot be met.

Within these constraints, FDA has attempted to select alternatives that provide as much flexibility as practicable without endangering the integrity of the electronic records. The agency decided not to make the required extent and stringency of controls dependent on the type of record or transactions, so that firms can decide for themselves what level of controls are worthwhile in each case. For example, FDA chose to give firms maximum flexibility in determining: (1) The circumstances under which management would have to be notified of security problems, (2) the means by which firms achieve the required link between an electronic signature and an electronic record, (3) the circumstances under which extra security and authentication measures are warranted in open systems, (4) when to use operational system checks to ensure proper event sequencing, and (5) when to use terminal checks to ensure that data and instructions originate from a valid source.

Numerous other specific considerations were addressed in the public comments to the proposed rule. A summary of the issues raised by those comments, the agency's assessment of these issues, and any changes made in the proposed rule as a result of these comments is presented earlier in this preamble.

FDA rejected alternatives for limiting potentially acceptable electronic submissions to a particular category, and for issuing different electronic submissions standards for small and large entities. The former alternative would unnecessarily limit the potential benefits of this rule; whereas the latter alternative would threaten the integrity of electronic records and submissions from small entities.

As discussed previously in this preamble, FDA rejected comments that suggested a total of 17 additional more stringent controls that might be more expensive to implement. These include: (1) Examination and certification of individuals who perform certain important tasks, (2) exclusive use of cryptographic methods to link electronic signatures to electronic records, (3) controls for each possible combination of a two factored authentication method, (4) controls for each different type of identification card, and (5) recording in audit trails the reason why records were changed.

List of Subjects in 21 CFR Part 11

Administrative practice and procedure, Electronic records, Electronic signatures, Reporting and recordkeeping requirements.

Therefore, under the Federal Food, Drug, and Cosmetic Act, the Public Health Service Act, and under authority delegated to the Commissioner of Food and Drugs, Title 21, Chapter I of the Code of Federal Regulations is amended by adding part 11 to read as follows:

PART 11—ELECTRONIC RECORDS; ELECTRONIC SIGNATURES

Subpart A—General Provisions

Sec.

- 11.1 Scope.
- 11.2 Implementation.
- 11.3 Definitions.

Subpart B-Electronic Records

- 11.10 Controls for closed systems.
- 11.30 Controls for open systems.
- 11.50 Signature manifestations.11.70 Signature/record linking.

Subpart C-Electronic Signatures

- 11.100 General requirements.
- 11.200 Electronic signature components and controls.
- 11.300 Controls for identification codes/ passwords.

Authority: Secs. 201–903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321–393); sec. 351 of the Public Health Service Act (42 U.S.C. 262).

Subpart A—General Provisions

§11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after

August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

§11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§11.3 Definitions.

- (a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.
- (b) The following definitions of terms also apply to this part:(1) Act means the Federal Food, Drug,
- (1) Act means the Federal Food, Dru and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).
- (2) Agency means the Food and Drug Administration.
- (3) Biometrics means a method of verifying an individual's identity based

on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

- (8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.
- (9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B—Electronic Records

§11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

(b) The ability to generate accurate and complete copies of records in both

human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

(d) Limiting system access to authorized individuals.

- (e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.
- (f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.
- (g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.
- (h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.
- (i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
- (j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.
- (k) Use of appropriate controls over systems documentation including:
- (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.
- (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

§11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to

ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

§11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

§11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Subpart C—Electronic Signatures

§11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic

signature, the organization shall verify the identity of the individual.

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

§11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

§ 11.300 Controls for identification codes/ passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Dated: March 11, 1997.
William B. Schultz,
Deputy Commissioner for Policy.
[FR Doc. 97–6833 Filed 3–20–97; 8:45 am]
BILLING CODE 4160–01–F