DELAWARE

UNIFORM REAL PROPERTY ELECTRONIC

RECORDING ACT

REPORT FROM THE DELAWARE ELECTRONIC RECORDING COMMISSION

Pursuant to Title 25, Chapter 1 § 180§ 181 §182 §183 §184

TABLE OF CONTENTS

Delaware Electronic Recording Commission Members:

Honorable Michael E. Kozikowski, Sr.
New Castle County Recorder of Deeds
Business Phone: (302) 395-7749
Email: MKozikowski@nccde.org

Honorable Betty Lou McKenna
Kent County Recorder of Deeds
Business Phone: (302) 744-2314
Email: bettyatdeed@comcast.net

Honorable Scott M. Dailey
Sussex County Recorder of Deeds
Business Phone: (302) 855-7785
Email: sussexdeeds@ymail.com
scottdailey@sussexcountyde.gov

Richard J. Geisenberger
Chief Deputy Secretary of State
Business Phone: (302) 739-4111
Email: Rick.Geisenberger@state.de.us

Stephen Marz
Delaware State Archivist
Business Phone: (302) 744-5000
Email: Stephen.marz@state.de.us

The Delaware Electronic Recording Commission is responsible for the adoption of standards to implement the Delaware Uniform Real Property Electronic Recording Act (Delaware URPERA), Title 25, Chapter 1 § 180§ 181 §182 §183 §184.

Delaware Electronic Recording Commission
Delaware Uniform Real Property Electronic Recording Act

Section I: Introduction

The Delaware legislature established the Delaware Electronic Recording Commission (DERC) to adopt standards to implement the Uniform Real Property Electronic Recording Act (URPERA). Passed during the 2005 legislative session, the Delaware URPERA authorizes county Recorders to accept electronic documents for recording, provided that they do so in compliance with standards established by the DERC. The DERC is composed of five members representing a range of stakeholders in the real property recording process:

1. A recorder for each county in the State.
2. Two members at large appointed by the Secretary of State

The DERC, in accordance with the provisions of its authorizing legislation, used the electronic recording standards issued by the Property Records Industry Association (PRIA) as the foundation for Delaware standards, expanding upon or clarifying the PRIA standards when necessary. DERC standards address the following issues: Data standards Security (transactional and organizational) Electronic signatures Notary acknowledgment File formats for electronic recording Records retention and preservation Payment of fees The Delaware Uniform Real Property Electronic Recording Act will be updated periodically in response to changes in the technological environment. For a glossary of terms referenced in this document, see Appendix A. For acronyms referenced in this document, see Appendix B. For an explanation of electronic recording models, see Appendix C. For applicable Delaware statutes pertaining to electronic recording, see Appendix D.

Section II: Delaware Uniform Real Property Electronic Recording Act

1) Data Standards.

The DERC adopts the PRIA standards on electronic document formatting and document data fields.

Comments

PRIA data and document standards are the preferred standard for use by industry participants of electronic document recording. See Appendix E for a list of the PRIA standards and supporting documents.

It is further recommended that eRecording be offered and conducted at all three models of submission. See Appendix C for an explanation of e-recording models from the PRIA Implementation Guide.

2) Security.

Participants of electronic recording shall develop security standards and policies based on industry accepted security practices and protocols.

Comments

Transactional Security: All electronic documents must be secured in such a way that both the transmitting and receiving parties are assured of each other's identity, and that no unauthorized party can view or alter the electronic document during transmission, processing, and delivery. If the electronic document has been subject to those security measures identified in Chapter 6 of the *PRIA eRecording XML Implementation Guide For Version 2.4.1, Revision 2, Updated 03/05/2007* throughout the entire electronic document process of execution through recording, then the security obligations under these standards have been satisfied.

Organizational Security: Each Recorder' s office, which elects to accept electronic documents for recordation pursuant to Title 25, Chapter 1 § 180§ 181 §182 §183 §184., shall implement reasonable measures such that each electronic document accepted for recordation is protected from alteration and unauthorized access.

3) Electronic Signatures.

While Uniform Electronic Transactions Act (UETA), 15 U.S.C.A. §§ 7001 to 7031 (Information can be found at: http://delcode.delaware.gov/title6/c012a/index.shtml) and URPERA allow many types of electronic signatures, Recorders are only required to accept electronic signatures that they have the technology to support.

4) Notary Acknowledgement.

Transactions filed pursuant to Title 25, Chapter 1 § 180§ 181 §182 §183 §184 must comply with Title 29, Chapter 43 Notaries § 4321 to 4329 as amended from time to time.

5) Document Formats for Electronic Recording.

The DERC recommends that electronic recordings be converted to (if necessary) and preserved as TIFF or PDF files along with their associated metadata. Model 3 submissions should be converted to TIFF or PDF until the viability of preserving these eRecordings in their native format (i.e. XML, XHTML) has been demonstrated.

Comments

Recommended Preservation File Formats (See Appendix F):

TIFF: The Tagged Image File Format (TIFF) is widely adopted within the property recording industry and by recorders who have imaging systems. TIFF is a non-proprietary format that is recommended for storing scanned images.

PDF: Portable Document Format (PDF) is another commonly used file format in the property recording industry. PDF files capture the appearance of the original document, can store both text and images, are difficult to modify, and can be rendered with free, cross-platform viewer software. PDF is based on publicly available specifications, and as of January 2007 Adobe, the creator of the format, is releasing the 1.7 version of the format to become an international standard through the International Standards Organization (ISO).

XML: Extensible Markup Language (XML) is the recommended file format for long-term preservation of any metadata.

Metadata: Metadata is commonly described as "data about data." Metadata is used to locate and manage information resources by classifying those resources and by capturing information not inherent in the resource. In the eRecording context, metadata may be generated automatically or created manually and it may be internal or external to the digital object itself. Regardless of how it is created or stored, maintaining accurate and reliable metadata is essential to the long-term preservation of eRecordings.

Microfilm: The archival process for electronic records will require consistent and complex management in order to maintain authenticity and integrity. Digital preservation requires a well-developed plan and implementation with specific policies and procedures. Electronic records are subject to the same threats of destruction as other mediums such as natural or human-made disasters. There are the added challenges of hardware and software obsolescence, media longevity and migration, infrastructure failures and accidental damage from improper handling.

The majority of records in the custody of the Recorders must be preserved permanently. The durability of electronic records has not been proven to be as enduring as microfilm. In order to secure and preserve information created and stored electronically, security microfilm is recommended. Microfilm is an analog technology that allows documents to be read with magnification and a light source. If necessary, microfilm can be converted into a digital format. Producing microfilm that is created within the guidelines of the American National Standards Institute (ANSI) and properly stored and handled should provide secure records for hundreds of years.

6) Records Retention and Preservation.

Recorders must retain all records in their custody in accordance with requirements detailed in each County Recorder's record retention schedule, approved by the Delaware State Library, Archives and Public Records.

Comments

See Appendix F for guidance on the long-term preservation of electronic recordings.

7) Payment of Recording Fees.

Electronic payment of recording fees shall be collected by public agencies as prescribed by state and local statutes and in accordance with accepted industry standards without incurring unreasonable electronic processing fees.

Comments

Payments are a prerequisite to all methods of recording. Whether or not a payment is attached or an authorization of payment is included in a recording submission, the submission must incorporate some methodology for payment of fees associated with a particular document or set of documents.

Typical payment options include: ACH (Automated Clearing House), internal escrow accounts, credit and debit cards, and journal vouchers. The majority of jurisdictions interviewed currently engaged in electronic recording collect payment through ACH or by internal escrow accounts.

Fees are to be collected according to statute and in a manner consistent with the promotion of electronic recording, and in accordance with accepted industry standards. Each county recorder may collect electronic recording fees in a manner compatible with its internal software and county financial practices.

Section III: Appendices

APPENDICES

A) Glossary of Terms

B) Acronyms Used In This Document

C) Electronic Recording Models Explained

D) Related Statutes and Regulations

E) PRIA Standards and Guidelines

F) Records Retention and Preservation Statutes

G) Model Memorandum of Understanding

H) Frequently Asked Questions

Appendix A
Glossary of Terms

Asymmetric encryption: A method that uses two keys – a public key and a private key. Together, the keys constitute a key pair. Though the keys are mathematically related, it is not possible to deduce one from the other. The public key is published in a public repository and can be freely distributed. The private key remains secret, known only to the key holder.

Authentication: The act of tying an action or result to the person claiming to have performed the action. Authentication generally requires a password or encryption key to perform, and the process will fail if the password or key is incorrect.

Digital signature: A type of electronic signature consisting of a transformation of an electronic message using an asymmetric crypto system 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 private key that corresponds to the signer's public key; and

(2) the initial message has not been altered since the transformation was made.

Digitized signature: A representation of a person"s handwritten signature, existing as a computerized image file. Digitized signatures are just one of several types of electronic signatures, and have no relation to digital signatures.

Document type definition (DTD): A document created using the Standard Generalized Markup Language (SGML) that defines a unique markup language (such as XHTML or XML). A DTD includes a list of tags, attributes, and rules of usage.

Electronic commerce: Also known as e-commerce, it refers to trade that occurs electronically, usually over the Internet. Electronic commerce often involves buying, selling, and sharing information, extending both new and traditional services to customers via electronic means. E-commerce allows business to take advantage of email, the Web, and other online innovations to improve the business process and offer consumers more ways to access products, faster information transfer and ultimately decreasing costs.

Electronic document: A document that is received by the Recorders in an electronic form.

Electronic record: A record created, generated, sent, communicated, received or stored by electronic means.

Electronic notary: A notary public who has registered with the Secretary of State and who provides electronic notarial acts using a digital certificate authorized by the Secretary of State. (Title 29, Chapter 43 Notaries § 4321 to 4329)

Electronic signature: An electronic sound, symbol or process attached to or logically associated with a document and executed or adopted by a person with the intent to sign the document. (See also Title 25, Chapter 1 § 180§ 181 §182 §183 §184 and Title 29, Chapter 43 Notaries § 4321 to 4329)

Encrypt: To apply an encryption key to a message in order to make it unreadable in an effort to prevent unintended use of the information.

Extensible Markup Language (XML): A computer language used to create markup languages. XML allows developers to specify a document type definition (DTD) or schema in order to devise new markup languages for general or specific uses.

Hash function: A mathematical algorithm that takes an electronic document and creates a document fingerprint. The document fingerprint is much smaller than the original document, and does not allow the reconstitution of the original document from the fingerprint. A slightly different document, processed through the same hash function, would produce very different document fingerprint. A hash function helps to secure data by providing a way to ensure that data is not tampered with.

Key pair: A set of keys, including a private key and a public key, used in asymmetric cryptography. Sometimes a key pair will be reserved for specific uses, such as creating digital signatures (signing pair) or encrypting secret information (encryption pair).

Metadata: Commonly described as "data about data." Metadata is used to locate and manage information resources by classifying those resources and by capturing information not inherent in the resource.

Nonrepudiation: Effectively implementing a process in such a way that the creator of a digital signature cannot deny having created it. Nonrepudiation involves supplying enough evidence about the identity of the signer and the integrity of a message so that the origin, submission, delivery, and integrity of the message cannot be denied. Protection of a user"s private key is also a critical factor in ensuring nonrepudiation. The entire Public Key Infrastructure (PKI) industry exists to create and ensure the trust necessary for nonrepudiation.

Notary public: “Notary public” and “notary” mean any person appointed by the Secretary of State to perform notarial acts.

Portable Document Format (PDF): A file format created by Adobe Systems, Inc. that uses the PostScript printer description language to create documents. PDF files capture the appearance of the original document, can store both text and images, are difficult to modify, and can be rendered with free, cross-platform viewer software.

Portal: In eRecording terms, an electronic location where submitters can send their documents for further processing and delivery. A fully featured portal will incorporate specific index rules and information from other tables that assure conformity with the receiving County"s backend recording system. A portal should be capable of receiving various document types from various submitting parties and be able to deliver them to virtually any county regardless of their back end recording system or physical location.

Private Key: A large, randomly generated prime number used in asymmetric encryption. The private key is used to encrypt a document fingerprint (the result of processing an electronic document through a hash function) to create a digital signature. A private key is generated by its holder at the same time a related public key is created. While the public half of a key pair is made available to anyone who wants it, the private key is only known by its owner, who must keep it absolutely secret to maintain its integrity.

Proprietary: Indicates that software or other employed technology is owned or controlled exclusively by the vendor. These solutions are not transferable to other systems and must be used only on the vendor's systems.

Public Key: A large, randomly generated prime number that is used to decrypt an electronic document that has been encrypted with a private key. A public key is generated by its holder at the same time a related private key is created. Within the Public Key Infrastructure (PKI), public keys are used to verify digital signatures. Public keys are contained in digital certificates, published and otherwise distributed by the issuing certificate authority (CA).

Public Key Infrastructure (PKI): The framework of different entities working together to create trust in electronic transactions. The PKI industry facilitates signed transactions by using asymmetric cryptography to ensure security and verifiable authenticity. The PKI includes all parties, policies, agreements and technologies to a transaction. This sophisticated infrastructure allows all concerned parties to trust electronic transactions created within the standards set by the PKI industry.

Schema: A method for specifying the structure and content of specific types of electronic documents which use XML.

Secure Socket Layer (SSL): A security technology that uses both asymmetric and symmetric cryptography to protect data transmitted over the Internet.

Signature Authentication: The process by which a digital signature is used to confirm a signer's identity and a document's validity.

Signed Digital Document: An electronic document that includes an embedded digital signature. The digital signature contains an encrypted document fingerprint, which allows anyone receiving the document to verify its validity using the process of signature authentication.

SMART Doc™: A SMART Doc™ is a technical framework for representing documents in an electronic format. This format links data, the visual representation of the form, and signature. The visual representation of the documents can utilize a variety of technologies such as XHTML, PDF, and TIFF. Previously SMART docs™ were called eMortgage documents. In order to better describe the actual capabilities of the technology, the word "eMortgage" was replaced by the acronym "SMART" which represents: Securable, Manageable, Archivable, Retrievable, and Transferable.

Submitting Party: The entity that originates an electronic document. This is usually a bank, title company, attorney or anyone that inputs data into a specific template and/or associates an image and wishes to send the documentation for electronic recordation at the County.

Tagged information file format (TIFF): An image file format commonly used for photos, scanned documents, or other graphics. TIFF images are graphics that are made up of individual dots or pixels. Files in the TIFF format are distinguished by a .tif filename extension.

Third party vendor: Entity that may act as a middle man or liaison to an electronic transaction. The vendor will usually have some added value to the transaction such as verifying accuracy and completeness of index entries, authentication of the submitting party, or any other County specific requirement.

Uniform Electronic Transactions Act (UETA): A body of recommended legislation drafted in 1999 by the National Conference of Commissioners on Uniform State Laws (NCCUSL) for adoption by state legislatures. UETA allows electronic documents and digital signatures to stand as equals with their paper counterparts. Delaware adopted a modified version of UETA (see Title 6, Chapter 12A UETA §12A-101 to §12A-117).

Uniform Real Property Electronic Recording Act (URPERA): A body of recommended legislation drafted in 2004 by the National Conference of Commissioners on Uniform State Laws (NCCUSL) for adoption by state legislatures. URPERA authorizes Recorders to accept electronic documents for recording in accordance with established standards. Delaware adopted a modified version of URPERA (Title 25, Chapter 1 § 180§ 181 §182 §183 §184).

Wet signature: An original representation of a person's name applied to a document. Wet signatures are often highly stylized, sometimes bearing little resemblance to the name they are supposed to represent.

XML: See Extensible Markup Language.

XML Schema: See Schema.

Appendix B
Acronyms Used In This Document

DERC	Delaware Electronic Recording Commission
DETA	Delaware Electronic Transactions Act
ACH	Automated Clearing House
ANSI	American National Standards Institute
DTD	Document Type Definition (see Glossary)
E-SIGN	Electronic Signatures in Global & National Commerce
FTP	File Transfer Protocol
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ISO	International Standards Organization
MISMO	Mortgage Industry Standards Maintenance Organization
MOU	Memorandum of Understanding
NCCUSL	National Conference of Commissioners on Uniform State Laws
OAIS	Open Archival Information Systems
PDF	Portable Document Format
PKI	Public Key Infrastructure (see Glossary)
PRIA	Property Records Industry Association

RESVQ SSL	Secure Socket Layer (see Glossary)
TIFF	Tagged Information File Format (see Glossary)
UETA	Uniform Electronic Transaction Act
URPERA	Uniform Real Property Electronic Recording Act
VPN	Virtual Private Network
XHTML	Extensible Hyper Text Markup Language
XML	Extensible Markup Language (see Glossary)

Appendix C
Electronic Recording Models Explained

From the PRIA I-Guide©

2.3 eRecording Models

Electronic recordings, whether as pilot projects or live production initiatives, have occurred in twenty states. From these efforts, three distinct models have emerged. The models are referred to as Models 1, 2 and 3. Each has distinctive characteristics. Each also brings certain benefits to the submitters.

Over time the improvements in delivery methods and document formats have improved the processes as well. From scanned paper documents, to electronically-signed images of the documents wrapped with XML data and securely signed, to completely electronic, XML-integrated documents using electronic and digital signatures, these models bring continuing benefits to participating recorders and document submitters. Ongoing progress with increasing value from added benefits are expected as mortgage, legal and recording industry standards are implemented.

2.3.1 Model 1

Description

This model is an extension of the paper-based closing or payoff processes. Documents are prepared and printed. The parties sign and notarize the paper documents with ink signatures. When complete, the signed and notarized paper documents are scanned and electronically sent to the recorder. Transmission is done by the submitting parties logging on to the recorder's computer system over a secure network after first identifying, or authenticating, themselves to the recorder's computer. The recorder makes the same determination of record-ability as with paper documents, visually inspecting them for such things as signatures and acknowledgments as well as determining the recording fees. Fees are usually paid from an escrow account the submitter maintains with the recorder.

Once the recorder accepts the documents for recording the scanned image is "burned" with the recording information, including recording date and time as well as the unique recording reference number, such as book and page number or instrument number. Indexing is performed by the indexing staff of the recorder's office, as are paper documents. A copy of the recorded images is returned to the submitter. Usually a recording receipt, together with the recording endorsement data, is returned to the submitter, who uses the data to create and print a label with the recording endorsement information. The label is affixed to the paper document, which is then processed as usual by the submitter. In other jurisdictions, the paper document is fed through a printer and the recording endorsement information is printed on document (usually on the upper, right-hand corner of the first page).

In jurisdictions that use Model 1, such as Orange County, California, and Maricopa County, Arizona, the average elapsed time for the process is usually under an hour from the time the recorder receives the image until the receipt and data are returned to the submitter.

2.3.2 Model 2

Description

Model 2 recordings may be paper or electronic based. A document image whether from a scanned paper document signed and notarized by „wet ink" signatures or from an electronic document electronically signed and notarized, is wrapped in an XML wrapper containing the data necessary for processing, indexing and returning the document. In the case of a scanned paper document, Model 2 further extends Model 1 by adding data that improves the process, specifically the indexing process in the recorder's office. In the case of an electronic document, it begins to improve the process for the settlement agent, lender or loan servicer submitting the document.

The model may support one or more of a number of graphics formats. Uncompressed TIFF (Tagged Image File Format) images are commonly used, because this format preserves the image in the most accurate and legible form. The recordable documents are generally delivered to the county recorder's site by whatever means the parties agree, including hypertext transport protocol secure (HTTPS), web services, file transport protocol (FTP) and even email. Most counties require some authentication of the submitter, typically based on an account and personal identification number (PIN), although some use digital signatures and certificates in lieu of, or in addition to, the former. The documents are stored in a secure area on the recorder's web site until the recorder's system retrieves them.

Once imported into the recorder's system, the recorder's legacy system handles the recording functions. In this case the system imports the data from an XML wrapper, including index data. The recording process is partially automated, but the image must be visually inspected to determine that it meets recording requirements as well as possibly to validate against the data in the XML wrapper. The indexing data in the embedded image is not linked to the index data in the XML, so the recorder has no automated means to verify that it is the same.

If a document meets the requirements, it is recorded. The recording information is "burned" onto the image and returned to the submitter by means agreed upon by the parties. In some jurisdictions that use Model 2, the electronic recorded document is embedded into an XML wrapper with the recording information added so that the submitter can use the data in its internal processes.

The average elapsed time from receipt to returning the recorded electronic documents is about five minutes for Broward County, Florida. That compares to about five days for similar closing documents delivered by settlement agents. Average turn around for mail-in documents is about seven days.

2.3.3 Model 3

Description

In a number of counties electronic reconveyances of deeds of trust and satisfactions of mortgages are prepared by loan servicers and electronically submitted. Under Model 3, these

real estate documents are generated on a vendor's document preparation system in XHTML (extensible hypertext mark-up language) format. The document preparation person logs on to the system and enters the information necessary to complete the generation of the document. Once the document has been generated, the person signs it if she has the authority, or notifies the person with signing authority to sign. Secure access is required for all parties that must sign the document because signing is done by digital signature.

Once the documents are electronically signed and notarized, they are released for recording. The document preparation system compares each document against recording rules to ensure its recordability, and then calculates recording fees. Documents may be submitted in batches. Submission is by secure hypertext transport protocol (HTTPS) through the vendor's recording server to the recorder's office.

Documents received at the recorder's system are re-checked against the rules to determine whether or not they may be recorded. If not, they are returned to the submitter. Otherwise they are accepted for recording and the data for recording is extracted from the documents and passed to the legacy recording system. The endorsement data is received from the legacy system and entered onto the respective documents in XML format. If required, the XHTML is transformed to TIFF images for the recorder's archives and the XHTML documents with the recording endorsements are returned to the submitter.

Fee payment information is passed to the legacy system after the rules determine that the recording fees are correct. The recorder collects the fees from escrow accounts maintained by the respective submitters, or by Automated Clearing House (ACH) payment processing.

The average turnaround time is approximately 30 seconds from the time the recorder receives the document until the recorded document is returned. This time includes the entire process, from quality control verification to indexing, when run in an "unattended" or "lightsout" mode.

Characteristics of different eRecording Models

	Model 1	Model 2	Model 3
Document Type	Paper closings are scanned as TIFF images; no data is associated with the TIFF image. The recorder views the TIFF images to process the submission.	Electronic or paper closings are supported. The electronic document, whether image or other format is embedded in theXML "wrapper." Of index data and other information. The recorder processes the submission primarily from the data "wrapper". The recorder also has the option to view the document to validate data or image quality, or review the document to meet other requirements.	A single electronic file with both the signed document and indexing data is submitted and able to be processed by the recorder. Currently the XHTML format (XML data - HTML formatting) is used or other similar formats, such as MISMO's SMART Doc format or PDF's Intelligent Document, that incorporate the XML data and link it to the content displayed.
Signature Type	Ink signatures for borrowers and notary, documents are then scanned.	Electronic signatures (holographic signing/stylus & signing pad.)	Current adopters are using digital signatures and certificates for signers, notary and recorder. This model supports other forms of electronic signatures.
Security	Virtual Private Network (VPN)	Digital Signatures and Certificate (Closing Agent and Recorder) / SSL (Transmission).	Digital signature and certificate used as a tamper-evident signature for the document and for access control identification for transactions / SSL (Transmission).
Preparer	Title companies, Closing Agents and Lenders scan paper & transmit images.	Title companies, Closing Agents, and Lenders transmit 2 files in one electronic record; document images and XML data.	Currently title companies and lenders adopters prepare electronic documents in XHTML format; it supports preparation in compatible formats that provide the functionality of this model.
Recorder	Traditional processing; but no paper. Recorder examines, records, indexes and archives TIFF images.	Recorder examines, records and archives images; automated indexing by extracting XML data (QO process only).	All processes can be automated, including examination and indexing; or, the recorder can choose manual processing.
Recorded Document	Recorder transmits recorded TIFF ("burned") copy; label data sent also for paper docs.	Recorder transmits recorded image ("burned") to preparer.	Recorder's system adds recording information to the electronic document as XML data for use by the preparer; converts the recorded electronic document to TIFF for archiving.
Payment	"Draw-down" or escrow account for payment.	"Draw-down" or escrow account for payment / ACH transaction.	"Draw-down" or escrow account; debit account' ACH transaction.

Benefits from different eRecording Models

Model 1	Model 2	Model 3
Reduces recording time / Improves the amount of documents processed.	Reduces recording time / Improves throughout	Reduces recording time / Improves throughout
Reduces costs to recorder only.	Reduces costs to the recorder and title company, closing agent, or lender.	Reduces costs to the recorder and title company.
Improves productivity to recording office only.	Improves productivity for both document submitter and recorder.	Improves productivity for both document submitter and recorder.
Improves customer service and satisfaction.	Reduces the probability of documents being altered after transaction is closed/Encrypted "wrapper".	Reduces the probability of documents being altered after transactions is closed/Secure signatures.
	Uses open and non-proprietary systems and formats.	Standardizes processes and formats.
	Improves customer service and satisfaction.	"SMART" documents automate processes and systems.
		Uses open and non-proprietary systems and formats.
		Improves customer service and satisfaction.

Issues concerning different eRecording Models

Model 1	Model 2	Model 3
Complexity of the process of scanning and labeling for submitters	Images are unintelligent	Payment and electronic transaction disconnected/ adds complexity to process.
TIFF image is unintelligent; data is not extractable	Electronic document and XML data are disconnected; possible need for reconciliation.	
Costs increase to submitters; may be greater than or equal to paper	Closed system architecture and proprietary software	
Closed system architecture (proprietary)	Payment and electronic transaction disconnected adds complexity to process	
Payment and electronic transaction disconnected; adds complexity to process	Lacks embedded business rules.	
Cost for proprietary software and data connection	Process and transport are cumbersome.	
Lacks embedded business rules		
Process and transport are cumbersome.		

Appendix D
Related Statutes and Regulations

TITLE 25, Property, General Provisions

CHAPTER 1. DEEDS

Subchapter V. Electronic Recording

§ 180 § 181 § 182 § 183 § 184

http://delcode.delaware.gov/title25/c001/sc05/index.shtml

TITLE 6, Commerce and Trade

SUBTITLE II

Other Laws Relating to Commerce and Trade

CHAPTER 12A. UNIFORM ELECTRONIC TRANSACTIONS ACT

DETA: Delaware Electronic Transactions Act

§ 12A-101 § 12A-102 § 12A-103 § 12A-104 § 12A-105 § 12A-106 § 12A-107 § 12A-108 § 12A-109 § 12A-110 § 12A-111 § 12A-112 § 12A-113 § 12A-114 § 12A-115 § 12A-116 § 12A-117

http://delcode.delaware.gov/title6/c012a/

TITLE 29

State Government

State Agencies and Offices Not Created by Constitution

CHAPTER 43. NOTARIES PUBLIC

Subchapter II. Notarial Acts

Electronic Notary Statutes and Administrative Regulations

§ 4321 § 4322 § 4323 § 4324 § 4325 § 4326 § 4327 § 4328 § 4329

http://delcode.delaware.gov/title29/c043/sc02/index.shtml

TITLE 29

State Government

State Agencies and Offices Not Created by Constitution

CHAPTER 43. NOTARIES PUBLIC

Subchapter I. Office and Duties

§ 4301 § 4302 § 4303 § 4304 § 4305 § 4306 § 4307 § 4308 § 4309 § 4310 § 4311 § 4312 § 4313 § 4314

http://delcode.delaware.gov/title29/c043/sc01/index.shtml

Appendix E
PRIA Standards and Guidelines

The most current version of the following PRIA standards and guidelines may be found at: http://www.pria.us . Prior to accessing the documents listed below, the user will be required to agree to the terms and conditions of the PRIA eRecording XML Standards License Agreement that may be found at: http://www.pria.us/i4a/pages/index.cfm?pageID=3581.

Technical Standards

- Document Version 2.4.1 September 2006
- Notary Version 2.4.1 September 2006
- PRIA Request Version 2.4.2 July 2007
- PRIA Response Version 2.4.2 July2007

Guidelines

- PRIA URPERA Enactment and eRecording Standards Implementation Guide
- PRIA eRecording XML Implementation Guide (Technical iGuide)

Appendix F
Records Retention and Preservation Statutes

Delaware State Archives and Public Records

TITLE 29

State Government

General Provisions

CHAPTER 5. STATE ARCHIVES AND HISTORICAL OBJECTS

Subchapter I. Public Records

§ 501 § 502 § 503 § 504 § 505 § 506 § 507 § 508 § 509 § 510 § 511 § 512 § 513 § 514 § 515 § 516 § 517 § 518 § 519 § 520 § 521 § 522 § 523 § 524 § 525 § 526

http://delcode.delaware.gov/title29/c005/sc01/index.shtml

DELAWARE PUBLIC ARCHIVES
POLICY STATEMENT AND GUIDELINES

MODEL GUIDELINES FOR ELECTRONIC RECORDS

STATEMENT OF PURPOSE

The Delaware Public Archives (DPA) has issued "Model Guidelines for Electronic Records" for use by all agencies in state and local government in Delaware. These guidelines are intended to guide agencies toward developing electronic records systems that create records to meet the accepted standards for a variety of criteria, including legally acceptable, auditable, and evidential. The purpose of these guidelines is to give agencies some guidance in the development of systems that create electronic records.

Many electronic information systems currently in place throughout government may not be creating legally acceptable records. This is due to the nature of information systems, which store information in discrete chunks that can be recombined and reused without reference to their documentary context. Records systems are slightly different in that they provide evidence of business transactions, and record and preserve the documentary context in which transactions take place. These guidelines are designed to ensure that electronic information systems also support the legal requirements for record keeping in Delaware.

STATEMENT OF AUTHORITY

The Delaware Public Archives has, as part of its mandate, the responsibility for establishing and administering "an archives and records management program for the application of efficient and economical methods to the creation, utilization, maintenance, retention, preservation, and disposal of public records." (29 Del. Code, Chapter 5, §503) Public records are defined by Delaware Code as "any document, book, photographic image, electronic data recording, paper, sound recording or other material regardless of physical form or characteristics." (29 Del. Code, Chapter 5, §502) Electronic record means "a public record that is stored, generated, received, or communicated by electronic means for use by, or storage in, an information system or for transmission from one information system to another." (29 Del. Code, Chapter 5, §502)

STATEMENT OF BENEFIT

The implementation of sound records management practices can result in a number of benefits for government: reduced costs for storage of obsolete records, reduced resources for the retrieval of records required for business activity, and greater accountability on the expenditure of government funds. With electronic records, the benefits can be more substantial. In implementing sound records management practices for electronic records, agencies can ensure the legal acceptability of their electronic records, reduce costs for the retrieval of records no longer needed to be maintained on the system, and identify economies for the migration of records to successive generations of technology and systems.

The most important benefit is to ensure the creation and management of accurate and reliable electronic records. This allows agencies to fulfill legal mandates about the protection of their records and the adequacy of documentation about their operations. In implementing electronic record keeping, agencies can also achieve the full utilization of information technology and reduce the burden of paper records keeping.

RETENTION OF ELECTRONIC RECORDS

The Delaware Public Archives works with agencies to determine the administrative, legal, fiscal, evidential, and historical value of records created during business operations. The length of retention of electronic records is based on these factors as well as other factors, such as costs for maintaining electronic records and potential costs for migrating records to new systems and platforms.

The Delaware Public Archives works with agencies to establish Retention Agreements for electronic records. These agreements are in the form of a renewable memorandum of understanding between the Delaware Public Archives and the agency and serve to ensure agency compliance with the Delaware laws concerning record keeping.

The Retention Agreement certifies that an electronic records system has met the criteria for electronic records in Delaware. The agreements are renewable at regular intervals, such as when a system undergoes a

major revision or update. A sample agreement form can be found later within these guidelines.

MODEL GUIDELINES

1. Electronic records systems must comply with the legal and administrative requirements for recordkeeping for Delaware government.

Summary: Agencies must comply with the legal and administrative requirements for recordkeeping within Delaware. The external recordkeeping requirements must be known and linked to internal retention rules.

Activities: Appoint a Records Officer (RO) annually and assign primary responsibility to the RO for maintaining agency compliance with all rules, laws, policies, and regulations concerning record keeping.

Maintain accurate records retention agreements for electronic record systems.

Renew records retention agreements governing electronic records at regular intervals (such as when the system undergoes a major revision or update) to ensure compliance.

2. Electronic records systems must have accurately documented policies, assigned responsibilities, and formal methodologies for their management.

Activities: In order to ensure documented responsibility for the management of electronic records, agencies must:

Maintain a register of all policies governing the electronic record keeping system. This register will be maintained at the agency and will include superseded policies as part of a history file.

Identify staff members assigned responsibilities for managing the electronic record keeping system and provide evidence of their assignments through position descriptions, administrative memoranda, or other transmitted means.

Maintain an operations manual for the electronic records system. This manual will be maintained at the agency and will include superseded policies as part of a history file.

3. The electronic records system must serve as the official record copy for business functions accomplished by the system.

Summary: The electronic records systems must be employed at all times, or documented exception procedures must be demonstrated to have been operating in their absence.

Activities: Implement the use of a statement of primary use to be consented to by all employees who will access the system. The consent will state that any records created outside of the system shall be deemed unofficial records, unless exception criteria have been met.

Define through the policy the exception criteria.

4. Electronic records systems must produce consistent results for the records they create. Electronic records systems must produce identical outcomes for all data processes and be subject to system logic testing.

Summary: In order to ensure that the electronic records system is the product of a consistent and credible set of processes, agencies must present evidence that the system is compliant with ANSI/AIIM Standard TR31-1994 "Performance Guidelines for the Legal

Acceptance of Records Produced by Information Technology Systems." Systems should also be tested periodically to ensure compliance.

Activities: Require vendor certification of compliance with ANSI/AIIM TR31-1994.
Provide certification that system is compliant with State Information Transport Network Acceptable Use Policy.

5. Records must be created for all business transactions identified in the agency's retention agreement.

Summary: conjunction with the Delaware Public Archives, the agency shall identify the vital records created by the electronic records system in a retention agreement. These records will provide evidence of the transactions which support the core mission of the agency.

Activities: Identify the transactions within the system which meet the criteria for producing vital and evidential records.

Capture these records through the use of metadata encapsulation and store in a softwareindependent format.

Use the model metadata profile to ensure compliance.

6. Electronic records systems must maintain accurate links to the transactions supporting the records created.

Summary: Records must be linked to the transaction with unique data. These links must be Maintained and accurate.

Activity: Use the model metadata profile to ensure compliance.

7. Records which are created by the electronic records system must meet accepted definitions of accurate, understandable, and meaningful records.

Summary: Electronic records must be:
1. accurate, in that there is a quality control check to ensure correct data;
2. understandable, in that the relationship between the information is represented in a way that supports their meaning; and
3. meaningful, in that the contextual linkages of records must carry information that supports a correct understanding of the transactions they support.

Activity: Develop quality control checks on the system to be performed annually.

8. All electronic records must be created by authorized users. Documentation for authorization must exist.

Summary: All electronic records systems must maintain reference tables containing the information and rules governing the identification of authorized users, as well as contextual information on the authorization and deauthorization of users.

Activity: Maintain all reference tables indicating authorized users and a history of these tables as a vital/evidential record.

9. Electronic records created must continue to reflect the content, structure, and context within the system over the entire length of the prescribed retention.

Summary: The electronic records created in the system must meet the accepted definitions of inviolate, coherent, and auditable records:

1. inviolate, in that they are not damaged, destroyed, or modified;
2. coherent, in that when reconstructed, they represent the logical relations established by the original software environment (and not any updated platform or environment); and
3. auditable, in that all actions taken to a record during the course of its life are documented with a proper audit trail.

Activity: Require vendor certification of compliance with ANSI/AIIM TR31-1994.

10. Records created by the system must be deletable.

Summary: In accordance with an approved retention agreement, electronic records eligible for destruction must be deletable according to accepted practices for the destruction of public records.

Activity: Destroy records according to Delaware Public Archives procedures.

11. It must be possible to export records to other systems without the loss of information.

Summary: In order to ensure the proper migration of records to other systems, as well as the transfer of electronic records to other systems, all electronic records systems must be compliant with ANSI/AIIM Standard TR31-1994 "Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Systems."

Activity: Require vendor certification of compliance with ANSI/AIIM TR31-1994.

12. It must be possible to output record content, structure, and context.

Summary: Systems must be capable of exporting the content, structure, and context of a record in an integrated presentation.

Activity: Require vendor certification of compliance with ANSI/AIIM TR31-1994.

13. Records must be masked when it is necessary to deliver censored copies to exclude confidential or exempt information.

Summary: As part of the electronic record system description, agencies must define and identify the existence of confidential and exempt records, the rules governing access to confidential and exempt records, and operational guidelines on the generation of output reports containing confidential and exempt records.

Activity: Define through policy the confidential records maintained in the system.

ESTABLISHING RETENTION AGREEMENTS FOR ELECTRONIC RECORDS

Retention agreements will be used to determine the length of retention for electronic records. While they may be similar to retention schedules, there are some differences:

- ► retention agreements will be negotiated with agencies
- ► retention agreements will cover only records meeting vital and evidential value criteria
- ► retention agreements will give agencies flexibility in determining how they wish to retain their electronic records
- ► retention agreements will be renewed on a periodic basis

Delaware Public Archives' Information Resources Specialists (IRS) will work with agency staff, including the agency Information Resource Manager (IRM), the network administrator, and the network operator(s) in drafting the retention agreements.

Identifying Electronic Records

The traditional records inventory (which identifies discrete records which have already been created) will

be replaced with an analysis of transactions which occur in a system (which identify events for which records should be created). In order to analyze these transactions, the IRSs will need to review available data models, data flow diagrams, and data dictionaries.
The review will identify transactions which meet certain values, such as administrative, fiscal, legal, vital and evidential, and produce two recommendations: which transactions should result in electronic records being created, and how long those electronic records should be retained. The recommendation will be presented to the agency and negotiated.

Identifying Electronic Records Systems

Unlike paper records, where the properties of record keeping systems were inherent and immediately understandable (e.g., filed alphabetically by year, by subject, suspense file, etc.), electronic records are often stored without these logical properties. IRSs will work with agencies to locate these properties and ensure that activities support a clear understanding of not only the creation of electronic records, but also the system which created them. The Model Guidelines for Electronic Records are designed to guide agencies toward practices which support proper electronic records activities.
IRSs will negotiate with agencies how they plan to implement the Model Guidelines, allowing agencies flexibility in developing answers to the problem of electronic records management.

Final Product: Memorandum of Understanding/Retention Agreement

Once the IRS and the agency have agreed on the two fundamental pieces of the retention agreement: the identification and suggested retention of electronic records, plus the identification and suggested activities of the electronic record system, a Memorandum of Understanding/Retention Agreement is drafted which details the agency's agreed upon management plan for the electronic records.
The Memorandum of Understanding is signed by an agency representative and a representative of DPA. The length of its term is negotiable.

SAMPLE

MEMORANDUM OF UNDERSTANDING (MOU)
State Personnel Office (SPO)
Department of Technology and Information (DTI)
Division of Accounting (DOA)
and
Delaware Public Archives (DPA)

The Payroll and Human Resources Statewide Technology system (hereafter referred to as “PHRST”) is an electronic information system owned by the State of Delaware. The system operates in a client-server environment, resides on servers within the Department of Technology and Information, and is administered by the State Personnel Office.

The PHRST system serves as the official information system for life-cycle tracking activities relating to management of Human Resources (HR), Benefits Administration (BA), and Payroll (PR) records. As such, the PHRST system is considered to contain the official record copy of HR, BA and PR transactions.
For the purpose of this MOU the following terms are defined:

- An **electronic record** refers to “a public record that is stored, generated, received, or communicated by electronic means for use by, or storage in, an information system or for transmission from one information system to another.” (29 Del. Code, Chapter 5, §502)
- A **record-keeping system** provides evidence of business transactions by recording and preserving the documentary context in which electronic transactions take place.
-

DPA hereby attests that the PHRST system is in compliance with its “Model Guidelines for Electronic Records” [http://www.state.de.us/sos/dpa/govserv/index.htm] as noted:

Guideline 1: The PHRST system complies with legal and administrative requirements for record keeping for Delaware government. External record keeping requirements have been reviewed and linked to internal

retention rules. Records Officers (RO) are appointed or reappointed on or before July 1 of each year.

Guideline 2: PHRST has accurately documented policies, assigned responsibilities, and formal methodologies for its management.

2.1 A register of policies and a history file of superseded policies are available at http://intranet/state.de.us/phrst and 655 South Bay Road, Blue Hen Corporate Center, Dover, DE 19901.

2.2 Staff members assigned responsibilities for managing PHRST are available at http://intranet/state.de.us/phrst and 655 South Bay Road, Blue Hen Corporate Center, Dover, DE 19901.

2.3 An Operations Manual for PHRST is available at http://intranet/state.de.us/phrst.

2.4 Data dictionary and data flow diagram(s) are available at 655 South Bay Road, Blue Hen Corporate Center, Dover, DE 19901.

2.5 A PHRST User Reference Library is available at http://intranet/state.de.us/phrst.

Guideline 3: PHRST serves as the official record copy for business functions accomplished by the system.

3.1 PHRST users have consented in writing as to the nature of PHRST records as official record copies. Records created outside of the system are non-record copies.

Guideline 4: PHRST produces consistent results for created records in that the system produces identical outcomes for all data processes and is subject to system logic testing. (ANSI/AIIM TR31-1994.)

Guideline 5: PHRST creates records for applicable business transactions (e.g. transactions which produce vital and evidential records) identified in the retention schedule. Records are captured and stored in a software independent format. Note: Those not contained in PHRST are maintained in traditional filing systems.

Guideline 6: PHRST maintains accurate links to transactions supporting created records.

Guideline 7: PHRST records meet accepted definitions of being accurate (there is a quality control check to ensure correct data); understandable (the relationship between the information is represented in a way that supports their meaning); and meaningful (contextual linkages of records carry information which support a correct understanding of supported transactions) records.

Guideline 8: PHRST records are created or accessed by authorized users. Reference tables containing information and rules governing the identification of authorized users, as well as contextual information on authorization and deactivation of unauthorized users is available. Authorized users are defined as those persons having access to the system such as identified agency representatives, identified central (SPO and Division of Accounting) personnel, and those DTI and vendor staff directly supporting the PHRST system. Users sign an “Acceptable Use Policy” and submit appropriate PHRST and Information Security Form (ISF) documentation through their respective agency Information Security Officer (ISO).

Guideline 9: PHRST records reflect content, structure, and context within the system over the length of the prescribed retention (60 years after employment termination per current General Records Retention Schedule requirements for personnel records) and meet the accepted definitions of inviolate (they are not damaged, destroyed, or modified); coherent (when reconstructed they represent the logical relations established by the original software environment); and auditable (actions taken to a record during the course of its life are documented with an audit trail).

Guideline 10: PHRST records can be deleted when eligible for destruction under accepted practices for the destruction of public records.

Guideline 11: PHRST records can be exported to other systems without loss of information.

Guideline 12: PHRST is capable of exporting content, structure, and context of a record in an integrated presentation.

Guideline 13: Confidential and exempt records are identified and rules governing access to confidential and exempt records, and operational guidelines on the generation of output reports containing confidential and exempt records are available.

To maintain effective operations and continue to retrieve data from PHRST as the operating system changes over time, there must be full documentation of:

- hardware and software, including brand names, version numbers, dates of installation, upgrades, replacements and conversions;
- data structures and content, including file layout and data dictionaries;
- enhancement algorithms;
- operating procedures, including methods for scanning and entering data; revising, updating or expunging records; backing up disks, tapes and files; applying safeguards to prevent tampering and unauthorized access to protected information; and carrying out the disposition of original documents;
- logging and tracking to provide a full, trustworthy audit trail;
- indexes;
- labeling of disks, tapes, and similar storage media;
- full, frequent, and regular backing up of records;
- refreshment, migration, and conversion plans; and
- risk management and disaster recovery plans.

The Delaware Public Archives hereby certifies that the PHRST System meets the legal and administrative requirements for record-keeping in Delaware government.
This certification and agreement is valid for the period January 1, 2004 to December 31, 2006.

RECOMMENDED PRACTICES FOR SELECTION
AND USE OF ELECTRONIC RECORDS SYSTEMS AND SOFTWARE

SELECTION AND USE OF ELECTRONIC RECORDS SYSTEMS:
Electronic records systems require hardware (equipment) and software (computer programs) to retrieve and translate information into a human readable format. Because the storage medium is not permanent, and because hardware and software evolve regularly, state and local government agencies must select an appropriate system based on specific information/operational needs and operate it in a manner that allows retention and retrieval of information from the system over time as hardware and software change, technology enhancements evolve, and storage media physically deteriorate.

DPA offers the following suggestions to aid state and local government agencies in using technology in ways that comply with the Delaware Public Records Law and the Freedom of Information Act. These recommendations represent generally accepted principles and practices, and address issues of particular concern to government archives and records administrators. In this rapidly changing information technology environment, adherence to the recommendations will help keep state and local government agencies in conformity with industry standards as they develop.

LEGAL CONSIDERATIONS:
The Delaware Freedom of Information Act (29 Delaware Code, §10001-10005) requires that data in electronic records systems be maintained so that it is available for public access, unless the information is specifically restricted. State and local government agencies should adopt procedures that protect restricted records from unauthorized access, ensure the integrity of all data that the system holds, and allow for access to records open for public inspection consistent with this mandate.
As with all records systems, and especially those using electronic formats, the key to admissibility as evidence is the "trustworthiness" of the information and the system and operating policies and procedures that produce it.

SYSTEMS DOCUMENTATION:
To maintain an effective operation and continue to retrieve data from the electronic records system as the operating environment changes over time, there must be full documentation of:

Hardware and software, including brand names, version numbers and dates of installation, upgrades, replacements and conversions.
Data structures and content, including the file layout and data dictionaries.
Enhancement algorithms
Operating procedures, including methods for scanning and entering data; revising, updating or expunging records; backing up disks, tapes and files; applying safeguards to prevent tampering and unauthorized access to protected information; and carrying out the disposition of original documents. In addition, there should be documented procedures for logging and tracking to provide a full, "trustworthy" audit trail. Full documentation of systems and operating procedures is essential and will contribute to the legal acceptability of the records management program and help ensure that data produced by the electronic records systems will be admissible as evidence in legal or administrative proceedings.

HARDWARE AND SOFTWARE CONSIDERATIONS:
When purchasing hardware and software for your agency:

Select programs that meet the Department of Defense criteria for record-keeping capabilities of software programs. The specifics of Department of Defense Standard 5015.2 for certification of software programs can be found at jitc.fhu.disa.mil/recmgt/#standard.

Strongly promote selection of systems with open rather than proprietary designs. Open systems provide the most flexibility when choosing equipment and will support interconnection, information systems integration, and information sharing.

Prepare specifications for hardware and software that will require vendors to continue to support and maintain their products.

Establish performance standards and incorporate them into specifications for hardware and software, requiring vendors to support them with a substantial performance bond.

Select systems that provide sufficient scanning resolution with enough density to produce a highquality
image.

Seek vendors which use standard rather than proprietary compression algorithms to make future migrations of data more certain and reliable.

Require vendors to supply programs or provide services to test the reliability of your systems periodically.

Consider systems that allow for indexing or incorporation of other retrieval information directly into the system.

INDEXING:
When information is stored on a medium that is not human-readable, complete and accurate indices are essential. The electronic records system design must include provisions for appropriate indexing. When information will be maintained and accessed over a number of years, the indices must be developed and documented with future users in mind who may need the information for purposes not required by the creating agency. Operating procedures should include an index check for accuracy at the time the index is created.

LABELING:
It is essential to label disks, tapes, and similar storage media with extreme care since it is impossible to determine content merely by visual inspection. Accurate labeling is even more critical when the information and its index are on different media.

BACKUP AND STORAGE:
Full, frequent, and regular backing up of electronic records and indices are a critical operating procedure to ensure data protection and information “trustworthiness”. Storage of these backups should be off-site in a secure, fire-safe facility. As the environmental tolerances for storage of electronic media vary greatly, the manufacturer's specifications should be followed.

REFRESHMENT, MIGRATION AND CONVERSION PLANS:
There should be an active procedure to refresh data and to migrate and convert images and correlating indices to new storage media as needed to preserve records in an accessible form.

RISK MANAGEMENT AND DISASTER RECOVERY:
Delaware Code requirements for vital records protection include all records formats. Vital records are defined by 29 Delaware Code, Section 502 as "those records which contain information required for government to continue functioning during a disaster, protect the rights of Delaware citizens, and document the obligations of Delaware government, and reestablish operations after a calamity has ended". Each state and local government agency should develop and implement a comprehensive risk or disaster prevention and recovery plan for all record formats.

IN SUMMARY,
(a) Public records not scheduled for transfer to DPA can be maintained on electronic records systems and the original documents, if any, can be destroyed after data verification. Incorporate consistent data backup procedures and refresh and/or migrate data as required.

(b) Public records scheduled for permanent transfer to DPA at some point in their life cycle will be accepted by DPA in the following formats ONLY:

(1) TIFF or PDF (for scanned documents), or
(2) Text or PDF (for documents born digitally), or
(3) Files created using Microsoft Office productivity software programs (e.g. Word, Excel, Access, PowerPoint) operating under Microsoft Windows operating systems [95, 98, 2000 or higher]

Files must be transferred on Compact Disc (CD-R; Read Only Memory, ANSI/NISO/ISO 9660-1990) with appropriate electronic indices.

NOTE: Microfilm and COM (Computer Output Microfilm) produced to archivally acceptable standards are also appropriate for transferring archival records to DPA. See “Guidelines for Utilizing Paper and Computer Output Image Conversion Services” on DPA’s website for further discussion of this option.

For further information and assistance, contact the DPA Government Services section at:
Delaware Public Archives
121 Duke of York Street
Dover, DE 19901
ATTN: James Frazier, Government Services Manager
Tel: 302-744-5039
Fax: 302-739-2578
www.state.de.us/sos/dpa

Effective May 1998
Revised October 1999
Revised December 1, 2003

Appendix G
Model Memorandum of Understanding

The following Memorandum of Understanding (MOU) is included as a model form, and is not intended to be a complete or final document. Each Delaware Recorder of Deeds that offers electronic recording of documents will need to revise and/or modify this model MOU to describe specific login parameters, transmission protocols, and other technical and legal requirements.

DELAWARE RECORDER OF DEEDS
ELECTRONIC/DIGITAL RECORDING
MEMORANDUM OF UNDERSTANDING

THIS MEMORANDUM OF UNDERSTANDING (MOU), dated _____ is between _____ County and _____ (Company). This MOU shall become effective on the date of execution by all parties, subject to any approvals provided for in this MOU and shall continue in force until modified, amended or terminated.

County desires to offer recording of real property documents by electronically receiving and transmitting documents electronically in substitution for conventional paper based documents and to assure that transactions are not legally invalid or unenforceable as a result of the use of available electronic technologies for the mutual benefit of the parties of the transactions.

County and Company acknowledge that this MOU is subject to the Delaware Electronic Recording Standards, as adopted by the Delaware Electronic Recording Commission, and as subsequently amended. This MOU shall be construed and interpreted to be consistent with and in conformance to those standards.

1. **Electronic Recording:** For purposes of this Memorandum of Understanding, Electronic Recording is defined based on the level of automation and structure of the transaction. (See Attachment A for Accepted Levels for Electronic Recording). The three levels of automation are as follows:

Level 1: Submitting organizations transmit scanned image original of ink signed documents to the county. The county completes the recording process in the same way as paper using the imaged copy as the source document. An electronic recording endorsement is returned to the organization in the form of a label or printing process in order for the submitting organization to append that information to the original paper document.

Level 2: Submitting organizations transmit scanned images of ink signed documents along with electronic indexing information to the county. The county performs an electronic examination of the imaged documents and indexing data, and then completes

the recording process using the imaged copy and electronic indexing information. The electronic version of the recorded document is made available to the submitting organization.

Level 3: Submitting organizations transmit documents which have been created, signed and notarized electronically along with the electronic indexing information or a Smart documents which are a single object containing the electronic version of the document in such a way that enables the electronic extraction of data from the object. Smart documents are required to be signed and notarized electronically. Electronic signatures must comply with the Uniform Electronic Transaction Act (UETA), K.S.A. 16-1601, et seq. The county performs an electronic examination of the electronic documents and indexing information then completes the recording process using the electronic documents. Electronic and Smart documents are made available to the submitting organization.

2. Program Eligibility: Electronic Recording mandates a close working relationship as well as mutual trust between the County and the submitting entity. All parties of the Electronic Recording transaction desire to operate and maintain a secure recording system that safeguards parties to recordation from deceit, fraud and forgery. This Memorandum of Understanding outlines the procedures and rules for the trusted relationship between the County and Company to facilitate a safe and secure Electronic Recording relationship. Participation in the Electronic Recording program is voluntary and the decision to do so is a business judgment. There will be no added fees or costs of any kind charged by the County for Electronic Recording.

3. County Requirements: The Electronic Recording Program of _____County is defined by the requirements attached to this Memorandum of Understanding.

Attachment A defines the technical specifications including format, levels of recording supported, transmission protocols, and security requirements of the electronic records required by County. Company agrees to provide the transmission to the County following the specifications outlined. Company understands that the specifications may change from time to time. In the event changes to the specification are required, the County will provide a written notice to the Company within a reasonable timeframe.

Attachment B contains the document and indexing specifications for the Electronic Recording program. For each document, the County specific document code is provided along with the required indexing information. Any County specific editing rules will also be described in this attachment. All indexing specifications must follow the Property Records Industry Association (PRIA) standards as set out on their website. www.pria.us.

Attachment C contains the processing schedules and hours of operation for the Electronic Recording Program.

Attachment D provides the payment options supported for the Electronic Recording program.

4. Company Responsibilities: Company acknowledges that Electronic Recording permits them to prepare, sign and/or transmit in electronic formats documents and business records and the documents or records shall be considered as the "original" record of the transaction in substitution for, and with the same intended effect as, paper documents and, in the case that such documents bear a digital or electronic signature, paper documents bearing handwritten signatures.

Company shall ensure that only original documents are used to create the electronic documents. Company shall be diligent in ensuring that documents submitted for Electronic Recording have been checked before submission for errors, omissions, scanning defects, illegible areas, and other deficiencies that would affect the Recorder's ability record the document and the public notice to be created thereby.
By use of electronic or digital certificates to sign documents Company intends to be bound to those documents for all purposes as fully as if paper versions of the documents had been manually signed.

By use of electronic or digital certificates to sign documents, Company intends to be bound by those electronic signatures affixed to any documents and such electronic signature shall have the same legal effect as if that signature was manually affixed to a paper version of the document.

By use of digital certificates to seal electronic files containing images of original paper documents or documents bearing manual signatures, Company shall recognize such sealed images for all purposes as fully as the original paper documents and shall be responsible for any failure by Company to comply with quality control procedures for assuring the accuracy and completeness of the electronic files.

The Company and/or its employees attest to the accuracy and completeness of the electronic records and acknowledge responsibility for the content of the documents submitted through the Electronic Recording Program. Should a dispute or legal action arise concerning an electronic transaction, the County will be held harmless and not liable for any damages.

Company is responsible for the costs of the system or services provided by a third party that enables Company to meet the Electronic Recording Program requirements.

Company will immediately notify County of any security incident, including but not limited to attempts to or actual unauthorized access to Company's pathway, which could compromise or otherwise adversely affect the County's data systems.

Company shall work to insure that all security measures and credentials implemented are protected. Company assumes all responsibility for documents submitted through unique credentials provided to Company for the purposes of engaging in Electronic Recording.

Company is responsible for receiving receipt of documents recorded by County insuring that the source of the receipt is known to be the County. Company is responsible for

forwarding these documents to County insuring that the source of the documents is known to be the Company who has been authenticated and that the documents to be recorded pass from Company to County without modification. Company must maintain an audit trail of all activity, available to County, at its request, to resolve issues or investigate potential fraudulent activity. The audit trail must contain, at a minimum, submitter ID, submitted content at point of receipt from Company, submitted content as at point of delivery to County, dates and times submitted, size, and checksum.

Company is responsible for supporting any technical issues associated with Electronic Recording. Company shall work, in good faith, with County to resolve issues with the Electronic Recording process.

Company shall provide end user support to County through which problems or issues can be reported and addressed. In the event that problem is determined to be with the Electronic Recording software and not the infrastructure provided the Company shall work to resolve issues with County.

Company is responsible for coordinating all technical problems and issues through County.

5. County Responsibilities: County shall attempt to protect the integrity of the Recordation process through ongoing monitoring of documents received and recorded through Electronic Recording means.

County shall test and maintain Electronic Recording software and hardware required to operate the Electronic Recording capability. County, however, shall be held harmless and not liable for any damages resulting from software or equipment failure and assumes no contractual liability for any damages whatsoever via any part of this document. County shall apply the same level of diligence in handling documents submitted electronically as those submitted through the normal manual process.

6. General Understandings: The County will not incur any liability for the information electronically transmitted by the Company, included but not limited to any breach of security, fraud or deceit.

The County and Company will attempt in good faith to resolve any controversy or claim arising out of or relating to Electronic Recording through negotiation prior to initiating litigation.

Either party may terminate this Memorandum of Understanding for any reason by providing thirty (30) days written notice of termination.

The County and Company acknowledge that the electronic recording process is an emerging technology and that State and National standards will continue to evolve. To further the technology and the electronic recording process, the County and Company

will meet as needed to discuss changes and additions to this Memorandum of Understanding.

The County and Company understand that submission, acceptance and recording of any document must comply with all other applicable federal, state and local laws.

Documents may be rejected in accordance with Delaware law, including, but not limited to the following reasons: document errors, failure to pay the filing or other fees due, the document is not a type the Recorder of Deeds is authorized to accept for recording, or the document fails to meet any other applicable legal requirement.

Company's right to submit documents under this MOU is subject to County's review and acceptance of Company's pathway standards and procedures. Such approval will not be unreasonably withheld by County. This review will be directed to confirming that Company's pathway is secure and meets all requirements imposed by Delaware law or this MOU. Company agrees that following initial approval by County of Company's pathway, if Company materially modifies its pathway standards and procedures, County will be notified within a reasonable time, and County will be able to review and approve said material modifications.

County may suspend Company's right to electronically submit documents for recording for good cause, including, but not limited to failure to comply with any obligations imposed by Delaware law or this MOU. Notice of suspension will be immediately provided to Company by County. Company may be reinstated upon satisfactory resolution of the County's concern.

Any amendments or modifications to this MOU shall be in writing duly executed by each party's authorized official, which shall become effective at a time mutually agreed upon by the parties.

No alteration or variation of the terms of this MOU shall be valid unless made in writing and signed by the parties hereto, and no oral understanding or MOU not incorporated herein shall be binding on either party.

This MOU is not assignable by the Company either in whole or part, without the written consent of the County.

The Company agrees that all personal information which is considered privileged and confidential under Delaware law contained within the documents will not be released by the Company to any individual or other legal entity who would not otherwise have access to such information. Any release of information by the Company to any unauthorized individual or other legal entity may result in the County terminating this MOU. Notwithstanding any other time limits herein, County may terminate this MOU for unauthorized use or disclosure by written notice to the Company. Written notice to be effective upon facsimile (FAX) transmission to Company or five (5) days from the date of mailing of such notice.

Except for payment and indemnity obligations hereunder, neither party shall be deemed in default, nor shall it hold the other party responsible for, any cessation, interruption or delay in the performance of its obligation hereunder due to earthquake, flood, fire, storm, natural disaster, act of God, war, armed conflict, terrorist action, labor strike, lockout, boycott, provided that the party relying upon this paragraph: (a) shall have given the other party written notice thereof promptly and, in any event, within five (5) days of discovery thereof and, (b) shall take all reasonable steps reasonably necessary under the circumstances to mitigate the effects of the force majeure event upon which such notice is based; provided further, that in the event the force majeure event described in this paragraph extends for a period in excess of thirty (30) days in aggregate, the other party immediately may terminate this agreement.

This MOU is entered into in the State of Delaware and is governed by the provisions of the statutes of the State of Delaware.

If any provision of this MOU, or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, provision to other persons or circumstances shall not be affected by such finding of invalidity or unenforceability, and shall be interpreted in a manner that shall reasonably carry out the intent of the MOU.

Any party wishing to challenge any or all conditions of this MOU must do so in a court located within the County of _____, State of Delaware.

Agreed and Accepted:
By_____ (Company)
Name_____
Date_____
By_____ (County)
Name_____
Date_____

Attachment A
Technical Specifications

Format of the transmitted File

Property Records Industry Association (PRIA)/Mortgage Industry Standards Maintenance Organization (MISMO) file format standard will be used. Any multipage storage format as specified by the County.

Communications Protocol and Options

Transmission Control Protocol/Internet Protocol (TCP/IP), HTTP and HTTPS

Security Framework

Encryption will be a minimum 128 bit file and image encryption. Secure Socket Layer (SSL) and user login/password will be employed. User passwords are controlled by the Company and should be monitored/or changed periodically to ensure security. Computers on which documents originate must have all critical operating system patches applied , must have a firewall (hardware or software) installed, and must have up to date virus scan software.

Returned File Format

Property Records Industry Association (PRIA)/Mortgage Industry Standards Maintenance Organization (MISMO) file format standard will be used. Any multi-page storage format as specified by the County.

Levels of Electronic Recording Supported

Levels 2 and 3 or as specified by the County.

Electronic Signatures and Use of Digital Certificates

The use of Electronic Signatures and Digital Certificates will need to adhere to the guidelines set out in any applicable Delaware Secretary of State administrative rules.

Imaging Standards

Documents will be scanned at a minimum of 300 dpi.

Documents will be scanned in portrait mode.

Document images will be captured in any multi page storage format as specified by the County.

Scanned documents will be legible and reproducible – including signatures and notary seals.

Document details, such as margins, font size, and other similar requirements, must meet all applicable state or local standards.

Documents must be scanned to original size.

Attachment B
Documents and Indexing Specifications

Eligible Document Types

Mortgage releases

Assignments of Mortgages

County Specific Document Type Coding

Please refer to PRIA website for the Logical Data Dictionary, which lists all the acceptable "Document Types". www.pria.us It is the County's intention to not reject documents based on "incorrect or non-County specific document types. The County will correct the document type as part of the acceptance process.

Indexing Fields for each Document Code

All documents submitted will require the minimum index fields:
Grantor(s) or equivalent
Grantee(s) or equivalent
Document Type
Recording Fee
Related (original document number, in the case of releases, assignment, amendments, etc.).
Legal Description Fields as specified by County
Standard PRIA tags defined for these fields must be used. www.pria.us

Document Imaging Quality Control Standards

The xhtml document must display in W3C (World Wide Web Consortium) Standards.

Notary Requirements per Document

It is the responsibility of the Company to confirm that notary signatures and seals are present on all documents that require them.

Inked notary seals are strongly recommended, in place of embossed notary seals, which require "darkening" by the Company prior to submittal.

All electronic notaries must adhere to the Delaware Secretary of State Standards for electronic notaries.

Eligible Document Batches

Document batches will be submitted by a standard naming convention as specified by the County.

The maximum size of electronic document batches will be determined by the County.

Cover Sheet

Each document submitted shall be accompanied by a cover sheet in the form as follows:

Name of company submitting document: SOVEREIGN BANK

When recorded mail to: SOVEREIGN BANK

1130 BERKSHIRE BOULEVARD

WYOMISSING, PA 19610

Title of Document: REAL ESTATE MORTGAGE

Mortgage Amount: $10,000

Previously Paid Mortgage Amount: $50,000 See Affidavit on Page: 13

Original Document Date: 5/18/2003

Grantor(s): JOHN DOE

Grantee(s): JANE SMITH

Full Legal Description: LOT 1 BLOCK 1 WESTLINK 3rd ADDITION, BUCKS COUNTY, PENNSYLVANIA

**Please note that if you do not have room to enter the complete legal description, list the page number that the legal description is printed on.

Book(s): 0953 and Page(s): 2577 Document Number: 28814355

Attachment C
Service Offering

Hours of Operation

Documents may be submitted at any time during the week. Documents will only be processed between 8:30 a.m. and 4:15 p.m. on those days that the County Recording Office is open to the public for business.

Documents will not be processed on county holidays, weekends, snow days, declared emergencies, etc. or in the event of network or equipment failure. County will attempt to notify Company of any disruption in service.

Processing Schedules

Document batches must be received by 5:00 p.m. local standard or daylight savings time to be recorded or rejected on the date received.

Alternative Delivery Options

There are no other electronic delivery options at this time.

Return Options

Submitted documents that are accepted for recording will be made available to the Company in electronic format after recording.
Submitted documents that are rejected will be made available to the Company in electronic format after rejection, along with a description of the reason(s) for rejection.

Service Help Contact Information

County: County eRecording Vendor: Company:

Attachment D
Payment Options

Payment Options

The Company must sign authorization form, allowing an Automated Clearing House (ACH) transaction against the account being used to process fees for documents submitted by Company.

It will be the Company's responsibility to inform County of any changes that may effect an ACH transaction at least 10 days before the change.

Notwithstanding any other time limits set forth herein, County may terminate this MOU by written notice to the Company for failure to report changes in ACH as required in this MOU. Written notice to be effective upon facsimile (FAX) transmission to Company or five (5) days from the date of mailing of such notice.

The Company will not be able to access the E-Record system if applications have been accepted and the fees have not been collected.

Appendix H
Frequently Asked Questions

1. What are the minimum hardware requirements to implement eRecording?
2. What other requirements would there be?
3. What document types can be electronically recorded?
4. At which models may documents be received?
5. What is a SMART Doc™?
6. Why are standards important?
7. What are the three proven methods of delivery in eRecording?
8. How does the size of a county affect its ability to participate in eRecording?
9. What is the relationship between URPERA, UETA and E-SIGN?
10. What are the implications if Electronic Recording Commissions or state agencies overseeing the commission or committee adopt standards that are not aligned with the standards adopted by other states?
11. What types of output are generated by an Electronic Recording Commission?
12. Will the private industry solely drive the standards based on early adopters and the information they have already accumulated or will it be a collaborative effort by the early adopters from across the nation or state in both the private and public sectors?
13. What are significant national standards that guide eRecording today?
14. What is MISMO's relevance in eRecording?
15. What is PRIA's relevance in eRecording?
16. How much security is needed in eRecording?
17. What are the differences and benefits of digital signatures and digital certificates in eRecording?
18. Are digital signatures and electronic signatures the same?
19. What is the difference between a digital signature and a digitized signature?
20. What kinds of electronic signatures should be used? For which signatures?
21. How are electronic and paper documents meshed together?
22. Do current indexing standards also apply to electronic documents?
23. How can costs be reduced and controlled?
24. Are there more fraud concerns with electronic recording?
25. Can I use a sound as my signature?
26. How are recording fees paid?
27. Can a Recorder accept a document transmitted by facsimile for recording?
28. Will all Delaware counties accept electronic recording?

1. What are the minimum hardware requirements to implement eRecording? At a minimum, a county would need to have a server with enough disk space to enable a web services program. This program would typically be developed and provided by a vendor or portal solution at little or no cost to the county.

2. What other requirements would there be? The county would also need to have access to the Internet and have a web browser such as Internet Explorer, which is usually already included in the computer's packaged software when the unit was purchased.

3. What document types may be electronically recorded? All document types lend themselves to electronic recording. Plats or maps filed electronically may require special handling.

4. At which models can documents be received? Documents that can automatically be created by a template and have embedded index data submitted with the recording payload, and can be electronically signed and/or notarized, can be received by a Recorders if the Recorders system is capable of accepting model 3. Examples of these "Smart Docs" would be Satisfactions and possibly Assignments. Documents that require the original executed instrument to be recorded lend themselves to model 2 recording since an actual copy of the document with wet signatures must accompany the index data. Examples of this would be Deeds and Mortgages.

5. What is a SMART Doc™? A SMART Doc™ is found only on model 3 transactions. It gets its name from the fact that a human does not need to view or handle it for it to be recorded. SMART Docs™ contain all of the necessary information to create index entries and to electronically create a document that can be recorded. This indexing is accomplished by virtue of the submitter organizing and labeling the data payload in a standard format to which the recorder also subscribes.

6. Why are standards important? Standards are important because they allow various parties to communicate and understand each other in a predefined manner. Without standards there would be constant interpreting and deciphering of information. In the eRecording world standards allow each party to organize and submit data to the other in a universal manner, without having to employ the use of custom integration points, and in order to facilitate interstate communication.

7. What are the three proven methods of delivery in eRecording?

> The three methods are point-to point-integration, third party vendor, and a portal. In the beginning when eRecording was a new concept, the third party vendor method was popular due to the lack of document preparation software available at the submitter's site.
>
> As eRecording"s popularity caught on submitters sometimes found it beneficial to eliminate the costs of a third party vendor and develop a point-to-point integration directly

with the county. This was typically true with larger counties where greater recording volumes are common.

Inherent with many submitters trying to send to many counties and not wanting to develop unique integration and data schemes for each, the concept of a portal was born. The portal was designed to be a central clearinghouse for submitters and counties. As proven, a submitter can deliver various documents intended for several different counties nationwide to the portal. The portal has the ability to verify that specific county index standards have been met and then deliver each document to the specific county for which it is intended.

8. How does the size of a county affect its ability to participate in eRecording? Because there are many methods in which to participate, a county's size has little bearing on its ability to implement eRecording. A small county that has Internet access could use a web services program to receive and return documents. A medium or large county that has more volume could use a vendor solution or agree to a point-to-point integration directly with the submitter. A portal could be used with any size county since the portal doesn't care or factor in the size of a county to perform its functionality, or to deliver and return recorded documents from that county.

9. What is the relationship between URPERA, UETA and E-SIGN? E-SIGN and UETA are federal and uniform state laws, respectively, enacted to enable electronic commerce. While E-SIGN covers some additional issues, they are complementary acts. They are similar in their application to electronic documents and electronic signatures based on voluntary agreement between parties. Both are self-implementing. Between them they remove barriers on both interstate and intrastate levels. E-SIGN explicitly preempts certain state laws that do not conform to E-SIGN even where a state enacts UETA. URPERA is a follow up act to UETA with the purpose of clarifying ancillary recording issues. It also establishes a method for adopting standards on a statewide basis that has the potential for implementing uniform standards nationally.

10. What are the implications if Electronic Recording Commissions or state agencies overseeing the commission or committee adopt standards that are not aligned with the standards adopted by other states?

> Since mortgage lending and title insurance have become national businesses that are utilized by citizens, this is a significant question. Adopting multiple standards that are not aligned will result in higher costs for both document submitters and county recorders. Computer systems for mortgage lenders, attorneys, settlement agents, title insurance companies and county recorders will have to be designed to accommodate multiple sets of standards. Each different set will need to be mapped to the MISMO standards used by the industry. Even then, with incompatible specifications mapping may be inadequate.
>
> Current national standards are driven by the private sector needs of interoperability among trading partners. Standards developed by PRIA reuse industry (MISMO) architecture, structure and data points. Likewise, MISMO reuses PRIA standards for those pieces unique to recording.

11. What types of output are generated by an Electronic Recording Commission?

Document deliverables can be in two forms. One is to generate the standards, even if adopting from sources such as PRIA, in the format of XML Document Type Definitions (DTDs) or schema, data dictionaries, implementation guides, etc. The other is to issue compiled references to adopted specifications, citing the source and location of the specifications adopted.

12. Will the private industry solely drive the standards based on early adopters and the information they have already accumulated or will it be a collaborative effort by the early adopters from across the nation or state in both the private and public sectors?

The latter. Standards development has already been a collaborative effort, both by trading partners in the private sector and county recorders. However, the collaboration includes more than early adopters. A number of large entities have participated in the standards process even though they have not yet implemented electronic transaction solutions.

13. What are significant national standards that guide eRecording today?

PRIA eRecording; PRIA Notary; MISMO Closing, Servicing, Origination, Request and Response envelopes, eMortgage SMART Doc™, eMortgage eRegistry, eMortgage ePackage; PDF, TIFF; XML.

14. What is MISMO"s relevance in eRecording?

MISMO is the primary standards setting body for the financial services organizations where the lending process begins and whose work efforts result in recordable documents. Their standards will be used by those organizations to create documents and share data. Since this group includes those who create the vast majority of documents to be recorded, their standards will be a major factor in documents processed by county recorders.

15. What is PRIA"s relevance in eRecording?

PRIA is a public/private cooperative entity with both recorders and submitters among its members. Its mission is to create and maintain standards. Four technical standards have been developed specific to electronic recording by PRIA. Two are envelopes for submitting and returning recordings. A third is the specification for the document information. The final specification is for notarial information included in notarial certificates and incorporates notary signatures and commission information.

The PRIA technical specifications were developed in close coordination with the private sector (MISMO) to ensure the interoperability of the technical standards. In fact, PRIA reuses a number of the data elements developed by MISMO and as well as the MISMO architecture. In turn, MISMO has adopted the PRIA data elements specific to recording for incorporation into its data dictionary and technical specifications.

Ultimately, widespread adoption of a standard will facilitate electronic commerce in the real estate finance industry. Neither the private nor the public sector can afford applications that accommodate different interfaces with each different trading partner or customer. PRIA offers a universal interface for recorders that submitters can rely on.

16. How much security is needed in eRecording?

Security is a matter of quality rather than quantity. The quality must be sufficient to protect the assets to the degree that it covers the risk inherent in the process. Once completed the documents will be public record, so protection against prying eyes is not a high priority. On the other hand, documents must be secure from interception that results in their being delayed or not delivered, from substitution by different documents, or from alteration. And because recordings include payment of fees and taxes, the payment system must be secured.

Recorders need to prevent viruses, worms, Trojan horses and other malicious software from infecting their networks and systems. They also need to ensure unauthorized parties do not gain access to the parts of their networks that are not authorized to be accessed by the public.

It is not the Recorders" responsibility to ensure the accuracy or legality of the documents themselves, except insofar as they qualify to be recorded. Security for that lies outside the scope of recording.

17. What are the differences and benefits of digital signatures and digital certificates in eRecording?

Digital signatures enable both the recorders and the submitters to determine whether a document or set of documents was altered so they can decide whether or not to continue the process or rely on the resulting recording. While digital signatures require signers to use a key they control to complete the signature, the resulting signatures do not identify the signers in the same manner that a signature on a paper document is identifiable.

Digital certificates can provide a model of certainty that the signers are who they claim to be, thus providing a degree of trust. From a security aspect this can be an important tool insofar as the recorders can use it to decide who to accept documents from. Conversely, submitters or other parties can determine that particular recordings are authentic when documents are returned from the recorder's office with endorsement of recording information.

18. Are digital signatures and electronic signatures the same?

Yes and no. A digital signature is a kind of electronic signature. Not all electronic signatures are digital signatures in the same way not all pens are fountain pens.

19. What is the difference between a digital signature and a digitized signature?

As described in the Glossary found in Appendix A:

Digital signature: A complex string of electronic data that contains encoded information about a document and the person who signed it. Because they use powerful asymmetric encryption technology, digital signatures are the most secure type of electronic signature.

Digitized signature: A scanned image of a person's handwritten signature, which is captured using special digitizing hardware and stored as a computer file.

20. What kinds of electronic signatures should be used? For which signatures?

This is a matter of agreement between parties, except as to government entities that may have the authority to establish performance standards for signatures under certain circumstances. Even so, government entities need to exercise caution that one technology is not given a higher legal standing than others. E-SIGN claims preemption in such cases.

21. How are electronic and paper documents meshed together?

The concept of "meshing" electronic and paper documents together does not really exist. Once the electronic document is received into the Recorder's system, the process of calculating fees, assigning time, book & page, instrument numbers is the same as for paper documents. Depending on the model of the electronic document, the image may be transported automatically into the Recorder's system for public retrieval alongside the paper document that was scanned by Recorder's staff.

22. Do current indexing standards also apply to electronic documents?

Recorders have the same responsibility for indexing documents received electronically as paper documents received in person, by U.S. mail, and by express methods.

23. How can costs be reduced and controlled?

One option being studied is the establishment of a "portal" that would accept documents submitted electronically from ANY system and transmit those documents to the appropriate recorder's office, no matter what vendor they use for their back end system. This concept would eliminate the need for specific software between a submitter and each recorder with whom they file. Different versions of the "portal" concept are being used in other states, some more successfully than others.

24. Are there more fraud concerns with electronic recording?

There is less chance of a document being altered at the recording counter or en route to Recorders offices than might exist during the prior activities which occurred in the

attorney"s or title offices. Moreover, intentional fraud is a moral issue and will not be controlled by recording statutes or methods.

25. Can I use a sound as my signature?

DURPERA authorizes the use of many types of electronic signatures. A county"s memorandum of understanding will detail what technology is supported by that county.

26. How are recording fees paid?

Fees are to be collected according to statute and in a manner consistent with the promotion of electronic recording, and in accordance with accepted industry standards. Each county recorder may collect electronic recording fees in a manner compatible with its internal software and county financial practices. (See Standard 7 for more information.)

27. Can a Recorder accept a document transmitted by facsimile for recording?

No, a facsimile is an electronic document without an electronic signature, and does not include the requisite transactional and organizational security standards to be accepted for recording.

28. Will all Delaware counties accept electronic recording?

Fees are to be collected according to statute and in a manner consistent with the promotion of electronic recording, and in accordance with accepted industry standards. Each county recorder may collect electronic recording fees in a manner compatible with its internal software and county financial practices.