

E-Signatures: A Compliance Overview

White Paper

Updated: Spring 2011

<http://www.orisys.com/>



United States Patent 6,745,936, 7,246,097



CONTENTS

COMPLIANCE OVERVIEW	1
CONTENTS	2
INTRODUCTION	3
Knowing what laws apply to your business	3
COMPLIANCE REQUIREMENTS	4
Electronic Signature Compliance: General Requirements.	4
COMMERCIAL COMPLIANCE IN THE US	6
Commercial transactions: governing laws, regulations	6
COMPLIANCE IN GOVERNMENT TRANSACTIONS	8
Government Applications: State and Federal regulations	8
INDUSTRY SPECIFIC COMPLIANCES	10
Industry-Specific Laws and Guidelines on the use of electronic....	10
"INDIRECT IMPACT" COMPLIANCES	12
Laws that may indirectly impact your paperless initiative.	12
CONCLUSION	14

INTRODUCTION

Knowing what laws apply to your business

With the signing of the Electronic Signatures in Global and National Commerce Act (ESIGN) in 2000, a movement toward paperless transactions (electronic documents and signatures) that had begun years before was formally recognized by the US government. While the ESIGN Act provides clear endorsement for electronic records and signatures in most industries, it does not govern all industries, nor does it address newer privacy laws, identity theft guidelines as well as other industry specific regulations that exist and continue to evolve. As a leading provider of electronic signature and other biometric software solutions, Orion Systems has developed a deep understanding of the requirements for legal enforceability of electronic signatures and contracts, as well as a thorough knowledge of the transaction, business and other processes that direct it. Through ongoing research and development, Orion has become an expert authority on using and securing electronic records of all types - legally binding contracts, leases, loans, HIPAA forms, and personal information documents among them.

In this paper, we attempt to address some of the key laws and regulations that govern customer compliance as they begin their electronic signature project. (Please note: This paper is not intended to substitute for competent legal advice, nor is it intended to be all encompassing. For further information on electronic records and/or signatures, please contact your corporate attorney. In addition to these laws, customers must maintain compliance with existing laws that impact the industries and states in which they do business.

For more information on Orion's Solutions, please visit our website at <http://www.orisys.com/>

Electronic Signature Compliance: General Requirements.

There are a variety of existing laws and requirements, as well as industry-specific regulations that govern the implementation and use of electronic documents and signatures today. While differences may exist in terms of industry-specific requirements, there are some basic criteria that must be met in every industry under every law, for electronic documents and signatures to be considered legally compliant.

For Electronic Signatures (defined here as ANY unique human identifier that may be used to “sign” a document or transaction, including handwritten signature, fingerprint etc.) to be considered minimally compliant, some fundamental criteria must be met:

- the signer must intend for the electronic signature to have the same legal effect (and enforceability) as a handwritten, “wet” (live ink) signature.
- the signature must both be unique to the person using it and be verifiable as such.
- the signature must be, at all times during the signing process, under the control of its “owner” or the person to whom it belongs.
- the signature must be attached to the document in such a way that the integrity of the document and signature are and remain non-repudiable, tamperproof and uncompromised.

The first item outlined above is the single most essential aspect of electronic records and signatures (and paper-based ones as well!). Within every signature process “intent” must be displayed. An electronic signature must capture not only the signature but also the person’s intent to agree to, approve, and/or authorize the contents of the record being signed, whether those contents are transaction oriented or contractual. For companies to be certain that “intent” is captured, the process must be implemented such that the intent is clear. This can be accomplished through a thorough and documented process, as well as through the use of clear and unambiguous “I understand that I am...” statements. While in certain industries legal disputes occur over fraudulent signatures, changes after signing, etc., more often than not, it is the “intent” which is disputed, and the process of capturing that intent that is then scrutinized to determine that intent was indeed implied.

The remaining items require the “intent”, but are instead focused on the authenticity of the terms and conditions of the signed document. These subsequent items will determine the admissibility of the record

in a court of law, and should be “built in” to any solution used. If these items are not adhered to, or are implemented in an unreliable manner, the contract itself may be deemed unenforceable – and the company stands to lose money, a capital asset or more.

For Electronic Records or documents (defined here as any electronic record, form, transaction, contract or other) to be considered minimally compliant, there are two very basic yet very *key* requirements:

- the electronic record (document) whether or not it has an electronic signature, must remain verifiably accurate and unchanged for its retention life.
- The electronic record (document) whether or not it has an electronic signature, must remain available and accessible for the period of its retention life.

All regulations governing documents, electronic or otherwise, demand that the first criteria above be met. A document (electronic or otherwise) cannot be changed or modified without indicating that it was changed, by whom and when. This is, however, especially crucial in the electronic world, where courts can demand both proof of a document’s authenticity/originality and proof that it is unaltered/able. Since in a legal dispute, your corporate records are among the first things the opposing counsel will request, the authenticity of these records needs to be verifiable and demonstrable - the burden of proof is on you. Companies have lost cases solely on the lack of verifiable “proof” that their electronic records are authentic and unchanged. (*July 2003, Vinhnee vs. American Express.*)

The second item is equally as key, but is unique to electronic documents. It is a key component of any legally compliant electronic document/signature initiative – electronic documents, must remain available, accessible, viewable and printable over their retention life. (Retention life is defined as the period of time, by law, documents must be maintained, often as long as 10 years, or indefinitely in many financial contracts.) All parties to the record must be able to obtain a copy of the record upon request. Storing these records or signatures in a format that is not accessible or that is subject to change, will lead to significant difficulty in meeting these key criteria, and could render your electronic records and signatures inadmissible in a court of law.

Once the key criteria for electronic signatures and documents have been defined, the next, often most difficult step for businesses, is identifying the laws, guidelines and regulations that apply to them. While there are laws and guidelines that directly impact your electronic document and signature project (ESIGN, for example), there are also many that *indirectly* impact their use. (These may include Consumer Protection Laws, Privacy laws and more.) As privacy laws evolve, the Patriot Act implications are felt, and identity theft laws are put on the books, these compliances become only more difficult to define. In the following section we discuss the federal law (ESIGN), State Laws, banking regulations and specific rules regarding government-based commercial transactions.

Governing Law, State Regulations and more:

- **ESIGN.** Passed in 2000, this law enables the use of electronic records and signatures across the US and its territories for any business, consumer or commercial transaction, and interstate or foreign commerce. (Please note: ESIGN specifically DOES NOT apply to government transactions, which are regulated by OMB/GPEA, nor does it cover a contract in which there is a “security instrument” (such as equipment leasing or financing.) Contracts with security instruments (also referred to as “electronic chattel paper”) are governed by UCC Article 9-105, which is described later in this section.) ESIGN:
 - enables the use of electronic records and signatures where the parties involved agree to use electronic versions.
 - enables electronic transmission of mandated disclosures subject to consent (signing etc.) from the recipient.
 - defines an electronic signature as “a sound, symbol, or process attached to, or logically associated with, a contract or other record” and executed or agreed to by a human (person) with the intent to sign said record.
 - provides for the long-term electronic storage of all records as long as they are unchangeable and accessible to all entitled parties for the retention life of the document.
 - provides for the use of electronic signatures in the act of notarizing documents and records.
 - provides for the use of electronic promissory notes.

-
- **UETA.** Uniform Electronic Transaction Act. These are state laws that govern the use of electronic records and/or signatures in commercial transactions. They are similar in both form and provisions to E-SIGN, with certain state-specific consumer protection terms. UETA exists in most states, Washington DC, Puerto Rico, and the US Virgin Islands. (Several states have chosen not to pass UETA codes, including NY, Georgia, and Washington. They have instead passed their own state-specific Electronic Signature and Records Acts.)
 - **UCC Article 9-105.** This is a provision of UCC article 9 dealing with Security Instruments. It enables the use of electronic documents and signatures for equipment leasing and financing contracts. These “security instruments” are also often legally referred to as “chattel paper”, and with the passage of UCC 9-105, are now known as “electronic chattel”. Similar in wording to both E-SIGN and UETA, with additional definition of “electronic chattel” and electronic promissory notes.
 - **Federal Reserve Board Final Rules on Electronic Disclosures.** These rules govern banking, financial and credit transactions, and establish mandatory standards for electronic delivery of consumer finance disclosures under consumer protection regulations. Initial disclosures and subsequent changes may be delivered electronically provided that customer consent was obtained in accordance with E-SIGN regulations and consumer laws governing the date and time of such disclosures. These include:
 - Equal Credit Opportunity
 - Electronic Fund Transfers
 - Consumer leasing
 - Truth in lending
 - Truth in savings
 - **Office of Management and Budget (OMB) Guidance on the Implementation of E-SIGN.** This guidance applies only to federal agencies. It was published by the OMB to provide directives for agencies in their electronic transactions with the public. Agencies following this guidance include: the IRS (tax filings), Federal Student Aid programs for the Department of Education, Homeland Security for I-9 forms, passports and more. This directive applies only to external transactions. Internal or inter-agency electronic records are governed by GPEA terms.

Government Applications: State and Federal regulations and guidelines

The United States Federal Government has been amongst the biggest proponents of “paperless” environments, as a means of improving inter office efficiencies, cutting costs and reducing the overall government paper burden. In 1998, then president Clinton championed, and ultimately signed into law, the Government Paperwork Elimination Act, the sole purpose of which was to reduce the sheer volume of paper the government consumed on a yearly basis. This law led to agency interpretations and issuance of agency-specific guidelines.

- **Government Paperwork Elimination Act (GPEA)** This law, targeting the federal government itself, has a simple goal: eliminate paper to the extent possible. (agencies are responsible for the implementation strategy and outline.) To accomplish this, it outlines only a few major compliances that must be met:
 - electronic documents and signatures are recognized as legally enforceable when used in government applications.
 - specifies that all federal agencies must provide mechanisms for using and accepting electronic signatures and records.

To support federal agency implementations of the GPEA, numerous agency guideline papers have been written, including:

- **Office of Management and Budget Guidance on Implementing GPEA.** This outlines the procedures agencies should use for legally enforceable documents and signatures. It makes procedural recommendations as well as providing storage guidelines.
- **eGovernment eAuthentication Initiative Team Guidelines.** This document addresses the overall steps that should be implemented as well as the suggested techniques for authenticating government and other users who are interacting entirely electronically, including completing and signing electronic documents.
- **NARA – National Archives and Records Administration Guidance documents.** These guidelines are published under several titles, and encompass the broad aspects of implementing an electronic document and signature strategy while also providing guidance on the long term storage, accessibility and archiving of these records.
- **State Laws and Regulations.** Almost all states have passed the

UETA laws (see the UETA section of this document for more information), and those who have not have their own versions of that law. In many states, there is both a UETA law, as well as some type of electronic records/digital signatures act. These laws in general specify the types of signatures accepted (biometric, handwritten, digital) as well as where within government transactions they may be used and how. For more state specific information, please visit Orion's ESign Portal at www.orisys.com/infocenter.

- **County Laws and Regulations.** With the increased paperwork burden and reduced staffing now found at many county offices, many counties have turned to electronic documents, especially for real estate documents (which have been identified as the most time consuming by recorders!) to improve the efficiency and reduce recording time. Many states have passed laws allowing for the electronic recording of deeds, liens etc., and in some cases, where states have been slow to act, counties themselves have passed ordinances allowing for such recording. These laws vary in shape and scope, but all have a similar intent: to accept as legally valid electronically signed and filed documents. A movement is also underway to pass a UETA-type in each state that would make the process less individual and more similar from state to state and county to county. The Uniform Real Property Electronic Recording Act, (URPERA) was introduced by the Uniform Law Commissioners in 2004, and has now been passed in several states. Over time it will be reviewed in all 50 states and the US territories. For more information on URPERA, please visit the Orion ESign Portal, or the Uniform Law Commissioners' URPERA information center at www.nccusl.org/Update/uniformact_why/uniformacts-why-urpera.asp

INDUSTRY SPECIFIC COMPLIANCES

Industry-Specific Laws and Guidelines on the use of electronic signatures and records.

Regulations specific to particular industries have been passed at both the federal and state level. To date, the most widely known of these are in the medical/pharmaceutical industry which we will provide an overview of here. Additional regulations have been published by OSHA, FAA, and others, dealing with paperwork unique to those industries. (For more information beyond this overview, please visit the Orion ESign Portal.) The two most widely known "industry specifics" are:

- **HIPAA.** (Health Insurance Portability and Accountability Act) Most people are very familiar with this law, enacted in 1996, as they must sign a "privacy policy" explanation paper every time they visit a doctor or a dentist. The law is, however, much broader than simply outlining privacy policies. Its goal was to "simplify" the use and movement of medical records (hence the "portability" in its name!) through the use of electronic documents and signatures. In order to accomplish this portability, HHS (health and human services agency) adopted guidelines for electronic health transactions. These guidelines impact all aspects of health care – providers, insurers and the many clearinghouses used by both. While HIPAA specifically allows for the use of electronic records and signatures, it does demand strict adherence to the following two principles:
 - Patient data (using an all-encompassing definition of data as any information (records, results, billing) that may identify a patient in any way) must be protected logically and physically to ensure confidentiality and integrity, while remaining accessible at all times.
 - Electronic signatures used must include encryption technology such that created electronic records are non-repudiatable, secure and patient identities are authenticatable

For more specific information, please visit the Orion Esign portal and review the HIPAA law in its entirety.

- **FDA CFR 21 Part 11.** As its name implies, this impacts the electronic records (and signatures) of companies regulated by the FDA, most specifically biotech and pharmaceutical, although all-FDA regulated industries must adhere as well. This regulation has been in effect since 1997, and encompasses any and all FDA-regulated processes. It sets forth the following guidelines for the use of both electronic records and signatures.
 - electronic records: electronic records MUST be handled

in a secure environment utilizing audit trails to monitor their accesses, such that their integrity is maintained and the record is non-repudiable.

- o electronic signatures: electronic signatures must be secured with the electronic record, such that they are non-repudiable. It further states that any type of signatures may be used, including PINs and biometrics.

For additional information, please visit the Orion ESign Portal.

“INDIRECT IMPACT”
COMPLIANCES

Laws that may indirectly impact your paperless initiative.

Consumer Laws. In the consumer finance, insurance, and other industries, there are mandated disclosures that must be made, and regulations mandate when they must appear and the form they must appear in. (Font sizes, layouts, etc. are often regulated.) All of the electronic signature and records laws, while enabling electronic presentation, signing and storing of these records, DO NOT, in any way affect or remove the adherence requirements set forth in these consumer laws. When implementing a paperless solution, especially one that will interact with consumers, it is imperative that disclosure law adherence be maintained. In the leasing and insurance industries, for example, laws were originated when paper was the only option, so they still require that a paper original be provided to the consumer and that state guidelines on layouts, font sizes and wording be maintained as well.

Privacy and Identity Theft Laws. As increases in identity theft and “privacy” violations continue to occur, newer and more penalizing laws are enacted to prevent them and ensure penalties for violators. The Gramm Leach Bliley Act was the first of these, but many states now have, or are in the process of enacting similar, more stringent laws. GLB, and subsequent state laws, affect the use and storage of electronic records and signatures to the extent that the onus is placed on the business to prevent any electronic tampering, hacking or outright theft. Businesses that do not ensure that their records are secure, non-repudiable, and inaccessible to unauthorized persons face stiff fines and other penalties. The similar trend in all of these laws is that they require stringent security, audit trails, and clearly dictate that business must assume and prevent any inherent risk in electronic systems.

USA Patriot Act. While this law deals with all aspects of homeland security, contained within it are numerous provisions that businesses must adhere to. Among these is Section 326, which requires that financial institutions implement stringent account opening identity verification policies. While the Patriot Act applies to all transactions and records, not just electronic ones, it states that users of electronic ones must use appropriate techniques for verifying applicant identities, and they are required to authenticate an applicant using an electronic record and signature. Most businesses are impacted in some way – Homeland Security now controls the I-9 form all new hires must complete, and all electronic filers must have stringent security in place to ensure the security of this personal information. In addition, some

businesses are required to provide records to DHS under Patriot Act requests for information, with failure to do so resulting in significant fines and penalties. DHS often asks for records electronically where possible, as it allows them to verify the integrity of said information and the sender can guarantee its authenticity.

CONCLUSION

Electronic records and signatures are rapidly becoming the norm in most businesses. While the technology enjoys widespread adoption, when beginning a paperless initiative, implementers must pay careful attention not only to the laws that govern electronic records, but also privacy laws, ID theft laws, consumer laws and other industry specific guidelines. Orion has been providing a patented, highly secure, and compliant solution for companies in a broad range of industries, and our solutions have been designed and developed to adhere to and exceed the compliance requirements for all existing federal, state and industry specific regulations. As the industry evolves, Orion will continue to implement new technology that will help our customers both stay compliant and competitive, and we will continue to help spearhead new rules and guidelines that protect our customers and the public. In this paper we have provided a general overview of the laws that most often apply to electronic records and signature implementations, and the information is deemed accurate as of this date. As the legal landscape continues to evolve, please watch our Esign Portal pages for updates to electronic records, privacy, consumer etc. laws. (www.orisys.com/infocenter)

Orion Systems is a leading software developer of secure paperless solutions employing electronic signatures, fingerprints and other biometrics. Based on our fundamental patent, our software is the only solution that securely and irrefutably electronically binds your customer or employee's biometrics to your document, creating a legally enforceable, signed document. Our products, designed specifically to address key industry needs, can be viewed online at our website, www.orisys.com.

If you have feedback about this document, please send e-mail to: sales@orisys.com.

Boston Office

15 New England Exec Park
Burlington, MA 01803

Austin Office

9600 Great Hills Trail
Suite 150W
Austin, TX 78759

Tel: 1-877-OrionSign (674-6674)
www.orisys.com

©Copyright 2011, Orion Systems, Inc. All rights reserved. Registered or unregistered trademarks in this document are property of their respective owners. The products in this document are protected by one or more patents, US. Patent number 6,745,936 and 7,246,097. Specifications subject to change without notice.