DIGITAL SIGNATURE COMPLIANCE

WITH

DOCUMENT MANAGEMENT SOFTWARE

Ademero software

FOR MORE INFO VISIT US ONLINE AT
WWW.ADEMERO.COM

DIGITAL SIGNATURE COMPLIANCE
WITH DOCUMENT MANAGEMENT SOFTWARE

Computers have completely transformed the way that we interact with the world around us. From the smartphones we carry to the latest office computers, ever-evolving technology continues to revolutionize our day-to-day lives. Of course, as technology continues to be embraced by businesses worldwide, rules and regulations are created to ensure that this adoption is done responsibly and for the benefit of all.

When it comes to using technology to manage your business' signed documents, these rules are ultimately centered around ensuring that electronic records and electronic signatures (ERES) are considered equivalent to old-fashioned paper documents and handwritten or 'inked' signatures. So, how do you ensure your ERES meets compliance within your document management software? Let's get started by first taking a look at some of the more prominent compliance regulations.

RULES AND REGULATIONS

Today, electronic records and digital signatures are used in nearly every industry around the world to better manage records and other content, reduce the risk of human errors, and to decrease operational costs by streamlining business processes and workflows. As a result, it takes multiple regulations to cover such a diverse range of needs. However, there are 4 main acts or guidelines to be aware of when considering your next e-signing software purchase:

1. The Uniform Electronic Transations Act (UETA)
2. The Electronic Signatures in Global and National Commerce Act (E-Sign Act)
3. The U.S. Food and Drug Administraion's (FDA) guidelines, 21 CFR Part 11
4. The Electronic Identification, Authentication and Trust Services (eIDAS), an European Union (EU) regulation

The guidelines for each one overlap somewhat, but since the regulations and guidelines above vary slightly from rule to rule, it's imperative to understand the requirements of each one before covering exactly what features to look for in your next document management software.

UETA & E-SIGN ACT

The Uniform Electronic Transactions Act (UETA) goes hand-in-hand with the Electronic Signatures in Global National Commerce Act (E-Sign Act), in that both were enacted to cover ERES concerns with business, commercial (including consumer), and government transactions. The UETA was approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) in 1999, prior to the E-Sign Act, to provide states with a uniformity and basic framework for determining legality of electronic signatures in transactions. The E-Sign Act was signed into law in June of 2000 to provide general rule of validity concerning ERES for transactions in or affecting interstate or foreign commerce.

With the UETA, digital signatures have the same legal effect as handwritten ones and any security procedure can be used to verify the digital signature (such as a telephone confirmation, PIN, etc.) in states and territories that have adopted the UETA. When it comes to additional requirements, digital signing software must:

1. Show that it was the intent of all parties to sign electronically
2. Include the signature on or linked to the contract or record
3. Include a timestamp/record that captures the process and date/time that the signature was created
4. Be able to retain electronic transactions
5. Include some method that confirms that the signer actually signed the contract/record

With the E-Sign Act, all the same elements are required as with the UETA, with two additions:

A

The consumer must consent to the use of electronic recordings

B

There is disclosure to the consumer that clearly and conspicuously discloses to the consumer that he/she has the right to have the contract/record in paper format and can withdraw consent to sign electronically

FDA - 21 CFR PART 11

In the early 1990's key groups in the pharmaceutical industry worked with the FDA to determine regulations that ensured best business practices with regards to electronic records and electronic signatures (ERES) for their industry. Over the next few years, these groups worked towards a goal to define criteria under which ERES are considered accurate, authentic, trustworthy, reliable, confidential, and equivalent to paper records and inked signatures.

These guidelines for the healthcare industry have had several additions over the years to help clarify intent with the latest iteration being released in 2014. In short, Part 11 requires the implementation of controls within the software to ensure the authenticity, integrity, and confidentiality of ERES. When considering the electronic signature functionality of the software, Part 11 requires two specific signature-related criteria:

1. That the system verify the identity for each signature.
    a. *"... subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual." —21 CFR Part 11, Subpart C, Sec. 11.200.*
2. That the signer prove their identity each time they sign with multi-factor authentication.
    a. *"... employ at least two distinct identification components such as an identification code and password." —21 CFR Part 11, Subpart C, Sec. 11.200.*

It's also important with regards to Part 11 compliance, that your document management system provide features for Access Controls, Confidentiality and Security, as well as Auditing and Logging Capabilities to ensure the signer cannot readily repudiate the signed record as not genuine.

eIDAS

The Electronic Identification Authentication and trust Services (eIDAS) is an European Union (EU) regulation established in 2014 (fully enforced in 2016) and applies to any person or business operating in the EU using electronic signatures for identity verification or electronic transactions. It was set out in order to give consistency to regulations and ultimately enhance trust in electronic transactions in the EU's internal market by providing a common foundation for secure electronic interactions across borders.

While any e-signatures that satisfy the UETA and E-Sign Act are sufficient, these do have the highest chance of being challenged successfully as determined by the EU. As a result, the EU has a list of about 200 qualified trust service providers, or Certificate Authorities, that provide and preserve digital certificates. While trust service providers not included on the list can be used by software vendors, using one that is qualified essentially ensures that the digital signature is irrebuttable and legally binding within all EU member states.

1

Level 1 - Standard E-Signatures

These satisfy the rules of UETA and E-Sign Act which, while legally binding under eIDAS, they are presumed rebuttable.

2

Level 2 - Advanced E-Signatures

These satisfy the eIDAS but are provided by non-qualified trust service providers, and as a result are still not 100% irrebuttable.

3

Level 3 - Qualified E-Signatures

These satisfy the eIDAS and are provided by qualified trust service providers, and as a result must be accepted and are irrebuttable by all EU memeber states.

In the end, the difference between levels 2 and 3 if you're not in or dealing within the EU is minimal. The eIDAS also introduced the recognition of Electronic Seals, pertaining only to legal persons and corporate entities and allowing organizations to sign documents as a department instead of having to use an authorized signer.

BEYOND MEETING COMPLIANCE WITH DMS

Even the more stringent of regulations are still worded vaguely enough so as to not commit to a certain type of technology or validation process. As a result, software vendors can tout digital signature compliance while giving you a slimmed-down or specialized tool that just doesn't satisfy the plethora of needs your business has. So, that means simply using a digital signature software to send a contract for signing still leaves you holding the bag for things like retention and security later, after the contract was signed.

When considering your businesses needs for compliance as well as just good business practices, it's important to ask yourself the following questions about your next software purchase:

1. Do I have needs in my organization that go beyond digital signing?
2. Where will I be storing my signed documents?
3. Are my records/documents/contracts secure and protected from tampering?
4. Do I have audit and access controls in place for these documents?
5. Would I benefit from automated workflows beyond routing for signatures?

With many industries, meeting a digital signature compliance is the least of their concerns. For example, if you're in the healthcare industry you're also worried about protecting ePHI and meeting HIPAA compliance. If you're in the education industry, you're also concerned about protection for all ERES related to student records in order to be FERPA compliant. Alternatively, you might just be looking for ways to use your next software purchase within your accounts payable and HR departments to streamline business processes saving your company time and money - you need a document management software (DMS).

KEEPING IT SIMPLE

In the end, a simple digital signature software just isn't going to hit the bar. Consider implementing a document management software instead to handle all of your electronic records and electronic signatures (ERES) needs, and then ask that provider if they meet FDA 21 CFR Part 11 and eIDAS requirements.

Ask them if they have features for Access Controls, Confidentiality and Security, as well as Auditing and Logging Capabilities like:

- Unique Multi-Factor User Identification
- Complete Electronic History of Documents
- System Event Logging for Auditing
- Data Encryption & Decryption
- Public Key Infrastructure (PKI) with a Level 2 or 3 Certification Authority

When it's all said and done, you're looking for so much more than a digital signing software. You're looking for a robust and simple solution that meets all your needs at one low price - one that's fast to implement, that's equipped with all the features you need, and that's easy to use and understand.

Content Central will keep your office moving with features that do more than just meet FDA 21 CFR Part 11 or eIDAS compliance. But don't just take our word for it, give it a try for yourself and see your customized solution in action today.

Sign Up For a Trial

Signup for a free trial of our Document Management Software today to see just how Content Central works for digital signing and more!

Schedule a Demo

Schedule a personalized demonstration to see exactly how Content Central can help you meet ERES Compliance today.

More to Discover!

Learn more about Content Central and the rest of our paperless office suite of products with videos, brochures, help articles, downloadables, and more!

Ademero
software

WANT MORE INFO?
VISIT **WWW.ADEMERO.COM**