cosign by arx
The Digital Signature Company

10 Questions: FDA Compliance Using Electronic Signatures — Part 2

Rodd Schlerf,
FDA Markets Manager, ARX

In the first part of this series, we discussed considerations for electronic signatures and FDA compliance. If you missed it, you can read Part 1 here. Part 2 discusses a few separate but related compliance issues, such as what types of electronic signatures are acceptable for HIPAA requirements.

6. What types of electronic signatures are acceptable for complying with HIPAA requirements?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) references electronic and digital signatures in a number of places: under the Privacy Rule, which protects the privacy of individual personal health information (PHI), and the Security Rule, which requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of an individual's PHI.

Under HIPAA, nearly all forms of electronic signature are acceptable. It is interesting to note that the initial HIPAA drafts called for the use of digital signatures only, but ultimately the language was softened to allow for any form of electronic signature.

There are specific compliance considerations around HIPPA and PHI when using a cloud service that uses electronic signatures (not digital signatures). It is common for cloud applications to route entire documents between individual computers and the cloud repository for signing purposes. This exposes a potential vulnerability to a document being intercepted and PHI being exposed. If the cloud service, however, is using standard digital signatures, then this would not be the case. Digital signatures only route an encrypted hash value (a mathematical expression of document contents), not the entire document.

The EU Electronic Signature Directives are Changing.

The EU's new Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS) regulation, which significantly revises the previous European Directive on Electronic Signatures 1999/93, was approved by the European Parliament on April 3, 2014. It was expected to be endorsed by the European Council in July, 2014. More details here.

7. Are there specific requirements for the use of digital signatures within the European Union?

The 1999/93/EC Electronic Signature Directive and the specific legislation in the different EU countries address two acceptable forms of electronic signature profiles. These defined forms are called "advanced electronic signatures" and "qualified electronic signatures," and can only be met by using standard digital signatures.

An advanced electronic signature is the same as a digital signature. A qualified electronic signature is a

10 Questions:
FDA Compliance Using Electronic Signatures - Part 2

digital signature that requires the signer to obtain his or her digital identity from a government-authorized certificate authority.

These requirements are mostly relevant in applications where government forms need to be signed, or with documents that need to be submitted to governments in Europe. There are subtle and sometimes major differences between the countries and regulators in the EU, so there is no one specific requirement. Because most life sciences companies tend to be very conservative, they have chosen to use standard digital signatures as a policy. There are smaller groups and pockets of employees who use electronic signatures in closed environments, but for GxP-regulated operations, digital signatures are prevalent.

"With digital signatures enabling us to sign off on experiments, we're able to enjoy the full benefits of our ELN solution and keep our documentation digital throughout its full lifecycle."

Peter Wagner, Senior Manager, Novozymes

8. What are some of the more common use cases for digital signatures in GxP-regulated operations?

Digital signatures are being used in many applications within life sciences enterprises today. One of the most common uses is within the core quality management system (QMS) of an organization. Most major document management systems and QMSs, such as Microsoft SharePoint, NextDocs, OpenText LiveLink, Alfresco, Adobe LiveCycle, Laserfiche, and Oracle WebCenter Content, have standard integrations for digital signatures.

Beyond back office business operations, digital signatures are commonly used in "middle office" applications. "Middle office" pertains to business processes where an organization needs 1) employees to sign documents that are then securely exchanged with or submitted to outside parties, or 2) outside parties to sign documents that need to be trusted by employees within the enterprise.

Because middle office applications are **open systems**, they should follow the FDA's recommendation for the use of digital signatures as specified in 21 CFR Part 11.30 — Controls for Open Systems. Examples of middle office applications where digital signatures are being used include Electronic Trial Master File (eTMF) essential documents (site monitoring trip reports, site regulatory packets, etc.); contracts, specifications, and other documents exchanged between BioPharmas and contract research and contract manufacturing organizations; Electronic Lab Notebooks used to support patent applications; and any other collaborative activities between multiple parties in the supply chain.

9. When using digital signatures, does the FDA or other regulatory authority require that digital certificates be obtained from a list of approved suppliers?

No. Most life sciences organizations use standard digital signatures and create their own digital certificates for their employees and other signers. This method is recognized as the most secure and natural way for an organization to issue digital identities and the best practice to leverage the technology.

An enterprise is naturally more qualified to issue digital credentials for its own employees than any third party performing this task. All organizations have well-established new hire policies and procedures,

10 Questions:
FDA Compliance Using Electronic Signatures - Part 2

including signed I9 forms or other HR forms, and new employees are added to the organization's MS Active Directory or LDAP, which defines the employee's digital signature privileges.

Also, most organizations already have screening policies, procedures, and databases in place for external parties such as customers, collaborators, or business partners. If an organization wants non-employees to sign documents, these policies enable medium- to high-assurance digital identities for signing purposes.

10. What type of digital signatures are accepted by the FDA's Electronic Submissions Gateway?

The FDA's website for Electronic Submissions Gateway mentions digital and electronic signatures for three purposes: to sign supporting documentation as part of a submission, to sign cover letters and associated forms, and to sign the submission transaction on the Gateway itself. The website makes it clear that the FDA will accept any form of electronic signature for the first two items. If a digital signature is used, a flattened PDF is preferred for submissions, so the signature is an image rather than an active component of the file. For "signing" during the submission transaction, however, the FDA provides specific instructions for how to create or acquire a digital certificate and how to use it to authenticate the submission transaction.

For the purpose of authenticating the electronic submission transaction, the FDA will accept digital certificates that are acquired from third-party vendors (listed in the Gateway User Guide Appendix C), certificates issued to a signer from his or her own organization, or self-signed certificates. A self-signed certificate is created by the same person who is signing, which is similar to a self-issued ID card.

Conclusion

Most users who sign documents electronically don't consider many of these issues, but it's important to take into consideration the topics discussed here prior using electronic or digital signatures.