An Executive Summary

# Secure Document Workflows in Drug Development

FDA has increased scrutiny of the integrity of data generated by biopharmaceutical companies and their suppliers, focusing on analytical laboratory results, batch records, quality procedures, and other documentation related to the development, scale up, analysis, and manufacture of drug products. Three-quarters of the warning letters issued by FDA's Center for Drug Evaluation and Research between January 2015 and May 2016 cited data integrity issues noting problems with how data were recorded and authenticated. In April 2016, the agency issued a draft guidance on data integrity, Data Integrity and Compliance with CGMP, that included a section on electronic signatures for master production and control records.

In addition, as recordkeeping, reporting, and submission documents continue to migrate from manual to digital processes, and from internal operations to outsourced operations, the challenges of tracking the authenticity of documents and signatures becomes more complicated. Biopharmaceutical companies and organizations that support drug development and manufacturing—including contract research, development, and manufacturing organizations, API manufacturers, testing laboratories, and materials suppliers—need proven tools to authenticate documents and reports used in the development and manufacturing process and supply chain. Digital signatures are gaining more widespread acceptance as an effective tool.

An electronic signature is defined in 21 *Code of Federal Regulations (CFR)* Part 11, Electronic Records; Electronic Signatures as "a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." An electronic signature represents the sender's intent to sign but does not have strong forensics behind it, says Mollie Shields-Uehling, CEO of the SAFE-BioPharma Association, a collaboration of biopharmaceutical and healthcare organizations as well as digital document and security companies working to provide high assurance identity trust for cyber transactions.

A digital signature is defined in 21 *CFR* Part 11 as, "an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified."

A digital signature provides a more technically and process-reliable signature, says Shields-Uehling. "In a digital signature, the sender's or the signer's identity is very tightly and uniquely algorithmically linked to the

signature," she says. In addition, the signature can be stored as long as required; if the document is changed once it has been signed, that signature is invalidated.

Due to the technology behind the digital signature, the sender cannot claim that they did not intend to make the signature or it was not their signature. "It gives a very very strong forensic proof that that person intended to sign, did indeed sign, and there is a reason for signing," says Shields-Uehling.

Digital signatures have applications beyond regulatory requirements. Signatures can be used for internal compliance and quality assurance issues, for standard operating procedures, and for work with external partners. They are used increasingly by companies looking to improve workflows and are used in regulatory, discovery, and compliance applications, says Shields-Uehling.

For example, GlaxoSmithKline, which outsources IT operations in India, uses digital signatures for compliance-related standard operating procedures. Pfizer uses approximately 10,000 digital signatures per month globally with e-lab notebooks, e-chemical notebooks, and e-bio notebooks.

FDA requires either a scanned signature or a digital signature for electronic submissions.

The European Medicines Agency, however, requires a digital signature with specific requirements. The identity must be uniquely linked to the signer, has to be created using data that the signer has under his or her sole control, and has to be linked to the signed document so subsequent changes in the document are detectable. In addition, the signature must be issued from a certification authority that is certified by a European Union (EU) member state and be on that member state's trust list, explains Shields-Uehling.

The SAFE-BioPharma digital signature meets those requirements and provides a standardized identity trust that the signer can be recognized by every US government agency, by the EU, and the European Medicines Agency, says Shields-Uehling. "It becomes essentially an Internet passport, an identity and a signature that can be used with all partners across the ecosystem, eliminating usernames and passwords and the other proliferation of all of these different digital identities that are unique to only one enterprise," she says.

Digital signatures provide companies with assurances that the person who signed the document intended to sign the document, the date and time it was signed are valid, the document was not changed after it was signed, and the signature can be validated for years after it was signed. This additional level of trust in the integrity of bio/pharmaceutical documents and data can be crucial as FDA presses for enhanced data security.