Background

Maybe your company had plans to move to an electronic signature capability prior to the world going into quarantine. Many businesses in the regulated industry may need to have employees work from home or in some cases shelter in-place for what could be several weeks. While many large regulated companies may have validated an e-signature solution that was implemented before the COVID-19 worldwide pandemic, it is possible that small pharma, support organizations, contract research organizations (CROs), and virtual regulated companies had yet to implement such a solution. If you find yourself in the latter camp in the early stages of a work-from-home strategy, it may last for several weeks. So, what are your options for getting documents authorized or signed? The Computer Validation and IT Compliance (CVIC) Specialty Section would like to provide the following points to consider for an emergency implementation or approach to help organizations and personnel in this situation. You will have to review your triage plans to determine if deviations or variances need to be filed. It’s also a good time to review your business continuity and disaster recovery plans to see if they need to be updated to address work-from-home situations.

Points to Consider:

Obviously, if your company finds itself in this predicament, it is not likely that it has the time to:

- Initiate a vendor procurement
- Conduct a vendor assessment or audit
- Prepare a contract
- Validate an implementation plan
- Submit a letter of intent to utilize electronic signatures by your company
- Train staff on signature expectations and then provision the signatures to staff with identity verification.

A company in this situation needs to have a solution that helps it be efficient and not compromise the integrity of any authorization approvals by signature that are executed on documentation. So, it is recommended that the company initiates a triage in the following ways.
Triage:

1. Review what is already available.
   - Do the people who are working from home use a virtual private network (VPN)? Can they access document management systems or other systems that need approval (or rejection) signatures? Urge your IT or technical group to update or upgrade the remote working capabilities so that people can access critical systems in a secure manner from outside the physical confines of the company locations.
   - Investigate utilizing your document management system to manage forms online. For example, can a form be filled out electronically instead of by hand, then reviewed and approved using the approval functionality of the document management system? Most document management systems will also allow you to upload scans or PDF documents and then approve those using the document management system’s approval workflow. This approach could be an option for when multiple individuals must review and approve documents when they are no longer co-located.

2. Consider your company’s processes and determine what exactly needs to be signed. Not every document requires a signature, and it is important at this time to streamline processes for document approval to just those where signatures are required by regulations. Even if you need to draft a deviation because your organization has a procedurally required signature, it would be best to document that deviation from procedures impacted by COVID-19 and note that during the health emergency you are utilizing an electronic signature signing process just for certain documents.

3. Wet Signatures
   a. Ideally, a quick and reliable process can be the use of wet-ink and scanning of the signature to provide an electronic record of the signed document. In this case, it is recommended that the wet-ink document be retained as the original with the scan serving as a working copy until the signed original can be provided for files as original record documentation. While not ideal to have to retain paper, since this process would be a manually intensive option, it reduces impediments to any compliance implications. Don’t forget that those original paper documents with wet-ink signatures will have to be gathered and collated for retention/archive.
b. Another option could be to sign in wet ink and then take a photo with the camera on a mobile phone or device, providing photographic copy evidence of the signature as a working electronic copy. In this case, it would also be recommended that the paper copy be retained as the original source.

4. Document your decisions and the process you will follow, and document your communication of the process to all staff who will be following it. Leverage existing policy and procedure documents such as an Acceptable Use policy and Records Retention Policy to address privacy and security concerns.

5. There are a number of electronic and digital signature solutions on the market that can be secured (e.g., AdobeSign, DocuSign).

   a. Generally, it would be recommended that these go through an assessment process and that they are validated for your intended use. Given the nature of the situation in which we find ourselves, these tools have been validated and used by others in the industry and found to be effective. It could be relatively easy for a company to contact these vendors and ask them to implement their Part 11-compliant modules and secure enough licenses to allow for staff to move into this approach and later retrospectively qualify and validate the vendor and their product. Each company should evaluate and document any compliance risk of using an unvalidated electronic signature application and the retrospective validation approach (note, both OECD-17 and the Pharmaceutical Inspection Co-operation Scheme (PIC/S) indicate retrospective validation is not an acceptable approach).

   b. It will be helpful if you define the intended use of these products because there are many options available. For example:

      • Do you need signatures just from your internal staff, or do you need signatures from external entities like CRO staff? If external entities will be included, how will you identify those people who will electronically sign? Will you need to buy licenses for them, or can you send passwords via a separate email? Limiting contact to people with company-issued emails may provide more confidence.

      • Do you already have a document management system, or will you need a repository to store the electronic documents? Will your document management system support the verification of the electronic signature?
c. You will need to document any deviations for practices that exist and for use of electronic signatures not defined in company procedures. If you do choose to go this route, it will still be important to utilize the vendor's provisioning processes for users with licenses and provide some training on the expectations for appropriate use (e.g., don't share passwords) and the equivalency of the electronic signature to handwritten signature when approving documentation. As noted, while not ideal, it is believed that the risk of documentation being completed fraudulently or lacking integrity is low with this approach. And it is important to have a plan for the retrospective validation to be completed on the project. Otherwise, your company risk assessment may determine that when using commercial off-the-shelf (COTS) software, verification of intended use may be sufficient as discussed in ISPE GAMP®5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems.

d. Another approach is to conduct a risk-based, high-level validation with minimal documentation. The requirement to validate is firmly established; however, the level of detail, documentation, and amount and detail of testing is left solely up to the company. Testing and documentation could be very high level initially and supplemented later, if desired. Leveraging vendor testing would also be encouraged. Deviations to current procedures would need to be documented.

6. If your company has not already done so, do prepare and send a certification letter to FDA as required by 21 CFR 11.100. It is likely that over the course of the coming months, as things settle down, you will want to implement a more permanent electronic or digital signature solution. The letter is a very simple step. The required text and address are below.

(Company Name) hereby certifies to the agency that the electronic signatures in our systems, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

**Address:** Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857
Conclusion

These are extraordinary times that call for creative solutions that still provide for the best attempt at signature authenticity and accuracy. As noted previously, while not ideal, these options, with effective deviation documentation, can allow for efficient electronic signature processes that will need to be validated and completed. If you choose the approach to use e-signatures, be sure to document your deviations and your plan for remediation along with a timetable for compliance.

References


Additional Resource on a Related Topic

CVIC Technical Article: Alternatives to Performing On-site Software Vendor Audits (Using Other Technologies) Points to Consider