Approval Processes, Security and 21 CFR Part 11

For anyone automating regulatory compliance document flows, there's clearly a challenge in defining what's required to conform to 21 CFR Part 11. When applying 21 CFR Part 11 guidelines to Institutional Review Board (IRB) and Grant approval processes, it's important that a vendor's technology can stand up to requirements. Click Commerce's portal-level security and product practices provide IRBs and Institutional Animal Care and Use Committees (IACUCs) a compliant, configurable product base that satisfies 21 CFR Part 11 requirements for a "closed" system. Though higher levels of add-on security technologies exist in the market today (e.g. biometric-based signatures), they far exceed the practical needs and budgets of today's IRBs: Click Commerce's eResearch Portal product, when combined with secured data transport such as Secured Sockets Layer (SSL) and your own Standard Operating Procedures (SOPs) for controlling physical access, are sufficient to meet 21 CFR Part 11's requirements.

21 CFR Part 11 Review

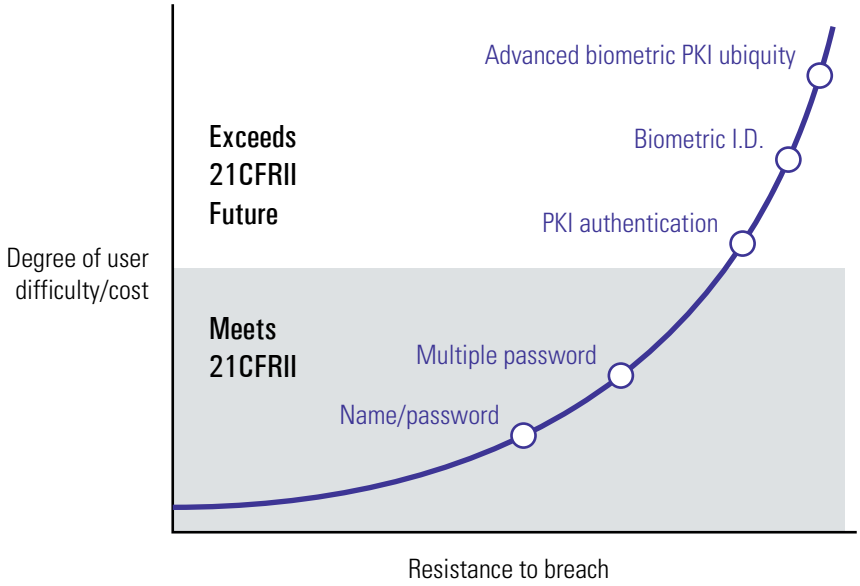
Verification and auditing capability (auditabilty) are at the core of every approvals system: institutions must be able to prove that any person taking action with the system is who they say they are. Furthermore, document submissions, reviews and approvals must be recorded reliably and cannot be changed without documentation: electronic signatures are the key to achieving this. The issues here really boil down to how much access security is satisfactory given the environment in which the system operates, whether "open" or "closed".

Closed System Policies and Access Security

A discussion about security should begin with the assumptions about the system operating environment. In the case of an approvals management system, the operating assumption is that the system is "closed": e.g. that the grant applications or research proposals and associated approval document data will be maintained within the same institution who is governing the process. Closed systems address some of the data integrity and confidentiality issues through an assumed level of trust among employees that is backed up with Standard Operating Procedures (SOPs.) For example, an SOP might forbid employees from writing down system passwords on notes near their workstations while, in parallel the automation system policy might require rotating to a new password every 90 days. Both work together to ensure data integrity and confidentiality.

With Internet technologies such as browsers and servers with extranet security, it's now possible for external companies, such as sponsors or commercial IRB personnel, to play a role in approval processes. Document and content security make it easily possible to accommodate external participants while hosting the system centrally within the Institution and still maintain a "closed" system context. But, exactly what should be the access security for such a system and how extensive must it be to meet the requirements of 21 CFR Part 11? Figure 1 introduces a model of cost/benefits for escalating levels of security that could be used to implement a closed system such as would be used for automating approvals.

Figure 1: Security Continuum for a "closed" electronic approvals portal



Different from an "open" system where 21 CFR Part 11 requires stronger authentication involving digital signatures, a "closed" system might use a combination of identification code (name/password) pairs and role-enforced access to specific electronic signature actions. Note the distinction between "digital signatures" and "electronic signatures"; some security technologies that implement the former present cumbersome usage and cost challenges. For practical purposes of IRB, IACUC and ancillary committee approvals, eResearch Portal implements name/password authentication and, additionally, role-enforced signature actions. eResearch Portal's standard approach for setting up system access rights by role and also workflow-specific access to review and approval activities meets the FDA's requirements for non-biometric electronic signatures that:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; 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.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

Reviewing each starting from the low end:

→ Name/password: the most widespread authentication scheme for electronic signatures, this scheme has the advantage of being familiar to anyone who has ever touched a computer. When abutted by SOPs that ensure proper password administration and conscientious employee use, name/password schemes provide an appropriate first-level of system access and operation. In addition, when combined with "strong" passwords (those involving both letters and numbers) and rotation schemes to force password changes every 90 days, resistance to breach becomes greater still and presents users with minimal password complexity. Finally, when combining this with an "electronic signature component that is only executable by, and designed to be used only by, the individual", the name/password approach achieves the FDA-required level of security for non-biometric signatures.

→ Multiple passwords: After signing-in with a system-wide password, certain creation, modification or approval actions can employ the use of the same passwords again before the system will record the user's action. This is more expedient and manageable than the addition of a completely separate, second password (note that a second password must be rotated on a similar basis to the conventional ones, but only to a select audience of users who, for their part, need to retain the confidentiality of a second key). The efficacy of any password system depends upon the diligence of the users and the responsiveness of the administrators; however, the value depends on the overall reduction in risk of fraudulent approvals that the institution perceives is gained through a second signing procedure (whether with the original password or with a second, separate password). Each approach's value must be compared to the administrative costs of gaining the signature.

→ Public Key Infrastructure (PKI) authentication: PKI document encryption with private and public \keys is arguably the most comprehensive and secure means of ensuring the identity of an author and tying it irrefutably to a singular edition of a document. However, PKI technology also complicates system design, performance and user experience. With digital certificates, users are typically tied to their workstations for signing operations, which eliminates the cost advantages of universal browser access: each time a user wishes to work from a different machine, a process to transfer the certificates to the new machine adds complications. In addition, like passwords, the loss or theft of a private key can result in impersonation. Finally, additional care must be used in determining the performance characteristics of a system where thousands of users are taking actions involving digital certificates: authentication traffic involving public/private key decoding can present significant computing overhead. Pilot testing the use of PKI on a small population of users would seem to be a prudent means of observing its characteristics (and costs) before widespread roll-out in a production setting.

→ Biometric identification: using physical data as an authentication means continues to raise legal questions as well as questions of efficacy. Fingerprints, facial scans, voice recognition technologies have repeatedly gained press for both for their difficulty to implement as well as for other privacy concerns. For a discussion of some of these concerns, consult the Electronic Freedom Foundation's web site: http://www.eff.org/Privacy/Surveillance/biometrics. Also, with the costs involved in adding hardware, it seems likely that biometric identification's adoption will be limited to applications where multiple layers of security and means of verifying identity are required (e.g. military or national security applications).

→ Future: the legal issues of collecting biological identity data aside, at some point in the future, hardware costs for effective biometric monitors may come down and PKI issues eased with the familiarity that comes from widespread exposure. At that time, the distinctions between authentication for closed and open systems may well blur at such time as costs and usage difficulty become insignificant.

Summary

An Institution must choose the right technologies that encourage automation system adoption by the constituents who need it most: the Principal Investigators (PIs), the IRBs and Department personnel. Security for any approvals system is a constant decision-making process that must balance SOPs for physical system access with the use of appropriate, available electronic technologies that resist breach, but encourage easy-to-use steady-state operation. In addition, every institution will have to weigh the documentation costs for fully validating their completed system against the benefits such validation might provide against future audits. Click Commerce's eResearch Portal product meets or exceeds the requirements in 21 CFR Part 11 for "closed" systems by providing manageable name/password administration, strong passwords with rotation options and electronic signature components that are only executable by, and designed to be used only by, specified individuals for specific approval actions.

[1] Code of Federal Regulations, Title 21, Volume 1; Revised as of April 1, 2005. CITE: 21CFR11.200
http://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?fr=11.200

Click Commerce

Click Commerce (Nasdaq: CKCM) eResearch Portal software has been configured to support institutions of all sizes and is backed by an experienced Professional Services organization with enterprise software deployment best practices.

Six of the top ten research institutions in North America, including Johns Hopkins, University of Washington, and the University of Michigan, use the eResearch Portal solution to automate regulatory compliance processes and manage research project approvals.

Contact us to find out how eResearch Portal can be licensed and configured to support your institution's process.

→ Find more online at research.clickcommerce.com or call, 1-800-590-5400