Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Designing Secure IT Environments for Pharmaceutical Clinical Trial Data Systems

Pharmaceutical companies are subject to regulations imposed by the FDA (Food and Drug Administration). Key elements of these regulations are rules governing the information technology space in drug production and research organizations. The requisite security infrastructure by these systems is sufficiently different from the security requirements in other IT areas because of these FDA regulations. Security professionals need to be educated in the rules and the unique challenges they present. This paper details the rele...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Designing Secure IT Environments for Pharmaceutical Clinical Trial Data Systems

Paul Drapeau

GSEC Practical Assignment Version 1.3

Abstract:

Pharmaceutical companies are subject to regulations imposed by the FDA (Food and Drug Administration). Key elements of these regulations are rules governing the information technology space in drug production and research organizations. The requisite security infrastructure by these systems is sufficiently different from the security requirements in other IT areas because of these FDA regulations. Security professionals need to be educated in the rules and the unique challenges they present.

This paper details the relevant regulations for security professionals and the special concerns they pose. Vendor neutral infrastructure component examples are given which could be used to develop a secure environment for FDA regulated systems. By learning about the requirements placed on systems by the FDA security professionals will be better equipped to aid in vendor selection and secure system implementation. Full compliance with FDA regulations will require the work and input of many people within the pharmaceutical company.

Introduction:

Computer systems that store or manipulate data involved with many aspects of pharmaceutical research, development and manufacture are subject to regulations published and enforced by the Food and Drug Administration. These regulations were developed originally to encompass paper data on drug development, clinical trials, and pharmaceutical production. As time and technology progresses and the regulations change, classical IT areas such as networking and security infrastructure in pharmaceutical companies are being affected by the regulations and must change the way they do business to comply.

While compliance with all FDA regulations pertaining to pharmaceutical data systems is a project that will likely include many groups within the company, several key technology responsibilities may fall into the IT department. Since the general requirements set forth in the regulations are designed to maintain the confidentiality, integrity, and availability of computer systems, IT security professionals will often be at the forefront of this effort.

The requirements of the FDA regulations are often simply codified examples of "best practice" network and security principles, but there are several instances where the FDA has put special restrictions on technologies in these realms. This document is meant to serve as a guide to IT networking and security engineers who are tasked with designing the systems and networks involved. By participating in vendor selection, technology evaluation, system design and deployment for FDA regulated data systems these

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

employees will likely perform critical roles in the overall compliance process of pharmaceutical and biotechnology companies.

Background and Relevant Regulations:

The FDA is tasked with the protection of consumers' safety and heath surrounding medical and food products. Pursuant to that goal, the agency has published and enforced regulations placing restrictions on pharmaceutical clinical trials, which are used to determine the safety and the efficacy of drugs. These regulations are designed to allow FDA inspectors to recreate studies and trials performed with a newly designed drug or a drug that has been on the market for some time. The specific regulations covering computer systems and IT security practices were developed to ensure that computer data is as trusted as paper data.

The traditional policy surrounding FDA regulated systems security covers best practice elements of their design, deployment and life cycle. Part of the constraint is that IT departments maintaining systems covered under FDA regulation are required to have well documented standard operating procedures (SOPs). These SOPs cover system installation, function, maintenance, backup and continuity planning, security, and change control. System and configuration validation is also central to the FDA rules. A data system covered under FDA regulations must be shown to be fully functional for its intended purpose and the initial configuration must be completely documented. Changes to the system must be thoroughly evaluated and documented to show they will have no adverse effect on the current validated state of the system. This restriction obviously includes operating system and application service packs, patches and security fixes. The FDA also requires that data produced by pharmaceutical companies regarding products be stored for long amounts of time. The data is relevant to the FDA and subject to inspection, in some cases, throughout the entire lifecycle of FDA regulated products (and often after they have expired or are no longer produced).

With the institution of the FDA regulation 21 CFR Part 11 "Electronic Records; Electronic Signatures" (often referred to as simply 21 CFR 11 or 21 CFR part 11) the security requirements for computer systems involved in data collection for drug research and clinical trials vastly changed. The regulation was made effective August 20, 1997 and governs methods in which the FDA would allow electronic signatures to be used on records submitted to the agency and how companies could use electronic records. 21 CFR part 11 also requires that all systems involved in the electronic signature and electronic records process are validated. This newer regulation has been a source of much debate in the pharmaceutical industry, as it imposes very strict data integrity requirements and lends no relief to legacy systems or large companies with several hundred or even thousands of systems to validate. It has been estimated by industry groups that the cost that a major pharmaceutical company would incur to comply with the requirements of 21 CFR part 11 alone may reach above one hundred million dollars.[1]

[1] Goldhammer, p.1.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

21 CFR part 11 states every electronic record stored on regulated systems that may be used in FDA submissions must be electronically signed. The FDA requires that all electronic records be reproducible in a human readable form, include a printed name of the signer, incorporate the meaning of the signature, be accompanied by a time stamped audit trail, and enforce non-repudiation requirements. Electronic signatures on data must be equivalent to paper signatures in that they are verifiably authentic, not reused, and not assigned to multiple individuals. 21 CFR part 11 comments state that electronic signatures may be composed of usernames and passwords, unique codes or biometrics. The rule reads that all electronic signatures not based on biometrics "must employ two distinct identification components." [2] While access controls may be entered only once for multiple signatures during a single session, they must be unique and constructed so that only the named signer can produce an electronic signature on a record with his or her access method. The FDA rule does make a distinction between *electronic signature* which is defined by the rule to be "a computer data compilation of any symbol or series of symbols executed, adopted, and authorized by an individual to be legally binding equivalent of the individual's handwritten signature" and *digital signature* which is defined by the regulation 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."[3]

21 CFR part 11 is sufficiently vague to cause some bit of confusion as to what the FDA actually considers a compliant record or compliant system. Often it is left up the individual inspectors sent by the FDA to determine if an infraction to the rule has taken place. Companies have already received FDA warning letters (termed "483s" in the industry) for non-compliance with 21 CRF part 11 and electronic signatures requirements. These warning letters can have severe effects on a an organization receiving them including bad press, more intense future regulatory scrutiny, and may even be business or product ending if the violations are serious and frequent enough.

Special Information Security Requirements:

The obvious requirement placed on IT security infrastructure enforced by regulation 21 CFR part 11 is that every "record" on a computer system must be electronically signed in a method stated above. A record is created on a computer system, according to the FDA, when data is stored to non-volatile media. This record may be a data file, word processor document, CAD drawing etc. or a database entry of clinical trial or experiment results. All systems storing this type of information must have their access limited to authorized individuals and these individuals must be issued a method of electronically signing documents and records according to the FDA requirements.

The configuration stability and integrity requirements of standard FDA computer validation procedures must also be taken into account. Software and systems used to store data relevant to FDA regulated products or submissions must be documented, tested, and validated before they are put into production. Changes to these systems during their

[2] Department of Health and Human Services, 21 CFR part 11. p.13466.
[3] Department of Health and Human Services, 21 CFR part 11. p.13465.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

service life and especially while they are actively being used in clinical studies must be strictly limited to absolutely necessary changes which have been tested and validated to have no measurable effect on the system stability or data reliability. While clinical and FDA submission data systems represent the most crucial information systems assets in pharmaceutical research and production organizations, they will not be readily upgraded, patched or reconfigured to remove newly discovered security vulnerabilities. Patches, hot fixes, service packs, and configuration changes will have to be delayed on production systems for a period of time as they are validated on test systems. In an increasingly threatening era of fast spreading worms and rapidly scanning exploit tools this requirement will be taxing to security personnel and system's administrators.

The records retention requirements of FDA rules put new challenges on disaster recovery systems. Pharmaceutical companies are required to maintain data and systems for long amounts of time. Traditional hardware, software, and media lifetimes measured in a few years are not often adequate enough to satisfy the requirements that at a later date the FDA may require a company to reproduce human readable copies of all records pertaining to a particular inspection. Backup rotations and systems must be constructed with these long retention periods in mind and media that can be reliably stored for long periods of time must be used. The retention period also puts restrictions on the types of technology and procedures used to create the electronic signatures on these records. Key or certificate expiration dates, account deletions, infrastructure upgrades etc. may not create a situation where an electronic signature cannot be validated as authentic at a time far in the future from when the record was signed. This is a special concern, as authentication methods, encryption keys, biometric information and other components of electronic signatures must be maintained for employees that may have left the company long ago. This may be contrary to a security professional's instinct and training that all inactive logins, keys, tokens etc should be deleted or rendered useless to the previous owners.

The "internal attacker" problem is a very real threat to FDA regulated computer systems and the infrastructure supporting them. Even well meaning, non-malicious users could create a situation where a system is out of compliance. Users may fail to follow written procedure in such a way as to destroy critical data, audit logs, or stable validated configurations. Malicious insiders will have access to the most vital data and systems owned by their company and could do vast amounts of irreparable damage if given the ability to do so. This is more relevant than in non-regulated environments because of the nature of the data. A company suffering loss from an internal attacker will have its problems compounded by possible regulatory action for failure to comply with FDA requirements.

Designing a Security Infrastructure:

Complying with FDA regulations for information systems is not a job for one person or one department within a pharmaceutical company. The full compliance process will most likely involve legal, regulatory, clinical, and audit departments as well as the classic IT networking, security, and systems groups. Often IT and security engineers will work

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

closely with the groups setting policy and directly interfacing with the FDA. Security professionals will fill the important role of product selection and implementation. The most imperative thing for an information security professional to remember about FDA compliance is no single product can guarantee compliance. Vendors will sell products as "21 CFR part 11" compliant but these products do not stand on their own. True compliance will require far more than a single product or even simply the network infrastructure itself.

One of the most important guidelines to follow while designing a network and security infrastructure for FDA regulated computers is the fact that documentation of almost every aspect of the system is required. Working with auditors and those charged with direct interaction with the FDA the security professional must assist in the production of the SOPs required by the FDA. The security SOPs should set policy for all aspects of user and administrator behavior on the regulated systems. Procedures for adding new users, disabling the access methods of those who have left the company, training users in system security requirements, data backup and archive, and incident handling should be set into written policy as SOPs. Documentation and testing of the final security and network infrastructure implemented is also required. Companies such as Pharmacia (in January of 2001) have received warning letters from the FDA for failure to document their network and security infrastructure. In this specific incident the company was also cited for failure to maintain up to date WAN and LAN diagrams and failing to validate the network used to connect regulated computer systems.[4]

Physical security is required by the FDA regulations. Server and workstation consoles must be reasonably protected from unauthorized access. System installations will involve "installation qualifications" which should record the components included in a system, the environmental conditions around it and the physical install location. If any of these items can be easily changed by a user or any other unauthorized person there is a real danger of finding the system in a state which is not compliant at some time in the future. Regulated systems and network devices should be installed in locked cabinets and inside locked data centers that provide the environmental conditions specified by the manufacturer. Access to the system consoles should be limited to authorized administrators only and all direct interactions with the system console should be physically logged in a system specific maintenance log for each device.

Ideally the FDA regulated computer systems should be installed in a logically separate network segment from the general business-computing environment at the site. There is a need to log traffic coming in and out of the systems and to separately authenticate a specific group of users within the company that will be interacting with the regulated applications. The protection required by the FDA is sufficient to justify a separate security "zone" within the corporate network. This is a classic example of the requirements for defense in depth. Protecting the regulated data systems from unauthorized access or accidental change from inside employees is required but should the security perimeter of the site itself be compromised from the outside it is obvious that the FDA regulated systems require an additional layer of protection.

[4] McDowall, p.2.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Clinical trial and research data systems should be connected to a network segment that sits behind a specifically designed security perimeter within the network. The security professional tasked with designing this environment should think of the corporate network as a DMZ that, in the classic network security sense, sits between the network he or she is designing and the Internet. This corporate network will be filled with users who are unauthorized to access the regulated systems, several hundred or thousand computers with possibly looser security controls that could introduce viruses or malicious code into the regulated environment, and even hackers that have already penetrated the network perimeter. The end goal is to prevent any unauthorized change to these systems (accidental or malicious) and track all interactions with them in a time stamped audit log as required by the FDA. A very strong case should be made to management and regulatory compliance groups for deployment of a separate firewall between this regulated network and the non-regulated infrastructure.

The firewall deployed between the clinical data systems and the internal company network must have a policy that completely enforces the separation of the networks. The FDA regulations are unambiguous about the fact that all unauthorized access must be prevented and all users accessing the environment must authenticate specifically for that purpose. This is not a place for a loose and permissive firewall policy. The bare minimum of services should be permitted and all possible logging facilities should be enabled. No FDA regulated system should be permitted to access the Internet unless it is specifically needed for the particular application installed. Allowing these computers access to untrusted outside systems with protocols like FTP, HTTP, etc. would permit users to obtain software, applets, and data files which have not been through the rigorous quality assurance and validation processes required by the FDA and may introduce hostile code into the environment. Software and data transfers should be only allowed to originate from within the environment directly to a test environment where new software and configurations are validated. Ideally this test network environment would be a segment also protected by the security perimeter of the regulated environment so its general integrity could also be ensured.

Strong authentication and data integrity will be required on any connection originating from the outside of the regulated perimeter. 21 CFR part 11 requires encryption when regulated records are transferred into the environment from more open networks. A virtual private network device should satisfy this part of the FDA requirements. Most importantly, deploying a client-server style VPN access device will provide the ability to log the start and end of any user session into the environment. If the only method of access provided to users is the VPN server, policy should dictate they log on to the system only when required and terminate their connection to this VPN device as soon as possible. This will allow security administrators to reconstruct the group of users that were accessing the environment at any given time in the event of a problem or unauthorized change. Also using a VPN device as the only allowed method of access will provide another layer of protection to the environment. Unauthorized users would have to penetrate the authentication required by this device or circumvent the firewall rules, which should dictate all connections must come from it. The authentication method for

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

the VPN connections terminated in this device should be at least two factors or biometric based according to the FDA 21 CFR part 11 rules.

Using VPN connections into the regulated environment also ensures confidentiality of data across the corporate network. Pharmaceutical clinical trial data may be of a sensitive nature and transporting it to the regulated network environment via an encrypted VPN tunnel ensures it is protected in transit from eavesdroppers and modification.

With the firewall and VPN access devices considered we can formulate the parts of the security policy that will be implemented as the firewall rules:

1. The firewall will divide the corporate network, the test network, and the production regulated network.
2. The only access allowed inbound to the production regulated network will be via a VPN device configured to require strong authentication and providing encrypted tunnels. All other access should be expressly blocked by the policy.
3. The production network is allowed to pull software and configuration updates from the test network. The test network will be granted no inbound connection privileges into the production environment.
4. The production network should never access the Internet or other untrusted network (including the corporate network) for any reason.

While it may be sufficient to rely on implicit "deny-all" rules specifically implementing rules, which deny access, inbound to the production network might serve the purpose of documenting special access controls to the environment. In the event of an inspection by the FDA these rules can show that all unauthorized access is being prevented with technological controls. Admittedly this set of rules and security policy implement an "ideal" situation. In reality there might be business requirements that will require that this general policy be changed. For example clinical systems may be required to acquire information from other systems and networks. In all cases these changes should be carefully considered and compared with the regulations and security SOPs in place at a given site.

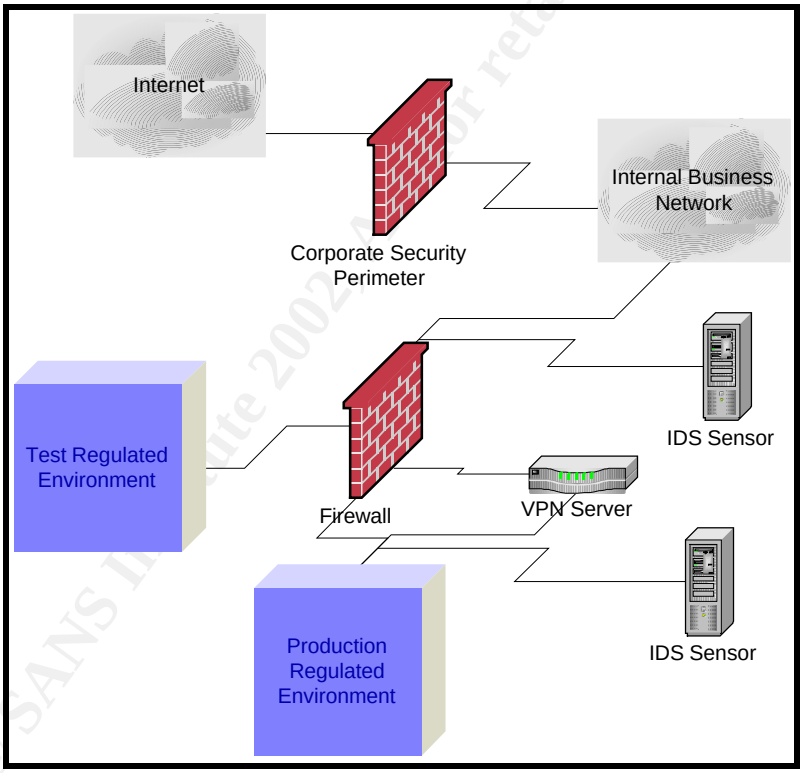
Network intrusion detection also has a role to play in the perimeter surrounding regulated systems. The rules implemented by the NIDS should be specifically tuned with the FDA regulations in mind. While the typical hacker attack is also a threat to these systems an element of change control and configuration integrity can be enforced or at least monitored by a NIDS.

With knowledge of the applications deployed on the regulated systems and their traffic patters information security administrators can craft rules, which detect undesirable or prohibited behavior. SOPs may not allow the direct change of records (good practices generally dictate records should be amended through a procedure which preserves the original content of the record). While this change could be detected after the fact with if the record was digitally signed, special IDS rules would alert administrators to unauthorized user behavior as soon as it happens. For example, if a particular application

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

stored data in a Microsoft SQL Server and SOPs for a given study dictated that data may only be entered into the system an IDS can be used to monitor this requirement and report on any violations. By implementing a pair of rules that search all traffic inbound to the server on TCP port 1433 (standard MS-SQL port) for DELETE or UPDATE queries the NIDS would alert the security administrator if any user or application attempts to deviate from the policy. Retraining the user on the relevant SOPs immediately can then minimize the damage. In this sense the NIDS cross checks the firewall and application controls for implementing the SOPs and FDA regulations, immediately reporting violations. A pager alert to a system administrator will cause far less headache to a pharmaceutical company than a warning letter from the FDA.

Deploying a NIDS will also improve the accuracy and completeness of the logging capability of the regulated environment. A carefully tuned NIDS could produce logs for the regulated environment that not only alerted administrators to prohibited behavior but also tracked all user interactions with the regulated systems at a level more detailed than most firewall logs.



High Level Diagram of Example Regulated Perimeter

Central to the 21 CFR part 11 requirements are electronic signature capabilities. The regulation reads almost as if public key cryptosystems were the desired goal for FDA compliant electronic signature infrastructure. The FDA will accept username and password for the electronic signature so long as the applications can still fulfill the other requirements (time stamped audit logs, signatures that include time, date, meaning etc.). Digital signatures are far more ideal. Classic cryptographic digital signatures will incorporate all of the required elements of the electronic signatures in 21 CFR part 11.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Signatures using cryptography can be configured provide for the "human readable form", user name, time stamping, integrity, and non-repudiation behaviors specified by the FDA.

PKI systems play very well in this space and the side benefits an organization will receive from a PKI implementation go well beyond regulatory compliance. Many vendors have released PKI implementations based on digital certificates, which can be used to fulfill many of the requirements of the FDA regulations.[5] When specifically considering the requirements of the systems regulated under 21 CFR part 11 there are unique requirements placed on any PKI or cryptographic solution put in place. While most asymmetric cryptosystems have integrity functionality and digital signatures as part of their feature set it is crucial that signatures be verifiable long after the records are signed. The fact that encryption keys that are lost, stolen, revoked, or expired can have no effect on the readability or verifiability of data at any time in the future. This requirement must be enforced while also maintaining the uniqueness of the private keys used to sign records. Escrow systems for private keys may draw scrutiny because of the keys availability to someone other than the intended owner. Implementing any cryptosystem in this space will be a difficult balance between two almost conflicting requirements in the regulations, the necessity to produce human readable copies of signatures and records at any time in the future and the desire to keep the elements of a given digital signature uniquely accessible to the owner. Private keys should be stored on a physical token and/or protected by pass codes to ensure that only the authorized owner of a key can use it to sign records. Thankfully, many commercial PKI solutions have taken these requirements into account and have technical solutions that address the issues, this should be a critical differentiating factor for any cryptography vendors considered.

PKI solutions must also be open and accessible via API interfaces for third party applications. Many applications are being developed with 21 CFR part 11 in mind. Any digital signature or key management package should be evaluated on its compliance with standards for digital certificates and programmer interface. X.509 certificates issued by PKI systems should contain the owner's name as required by 21 CFR part 11 but the software used for a particular record's generation and storage will have to include the other functionality made mandatory by the rule. Ease of integration between PKI systems and applications deployed in the regulated environment will be a key aspect to the success or failure of any given cryptography oriented solution posed to the electronic signature requirement.

Host based security and integrity tools should play into any implementation of an FDA regulated environment. Since configuration management and data integrity are so essential to compliance with 21 CFR part 11 and the predicate rules governing clinical, manufacturing, and research ensuring protections at the host level is very important. The two most useful (and in some cases mandated) tools are file system integrity checkers and anti-virus protection. Integrity checking software should be used to create configuration baselines when a system is installed. The baseline databases should be stored separate from the systems in question and used to verify the system state at regular, policy specified intervals during a study. Results should be printed and stored with the

[5] XCert, p.3.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

maintenance logs for each system. This will provide a good record that a system's software maintained the condition it was in during the installation qualification throughout the entirety of the computer's lifespan. Deviations detected can be dealt with when they are found which will give administrators and security officers an advantage in tracking down problems. Anti-virus software is specified in FDA configuration guidelines and companies have received warning letters for failing to protect their systems from viruses.[6]

Each system's configuration must also be carefully considered, checked and validated. The principle of least privilege holds very true in the arena of FDA regulated computer systems. If a particular privilege is not required for a particular user's job function, disable the user's access. System administrators must be trained to tread very lightly on regulated computer systems and should not use privileged accounts except when absolutely necessary. Changes made to the system through the use of privileged accounts should be immediately documented. The UNIX command "su" (and other operating system equivalents) is a double-edged sword in this area. It allows an administrator to use an unprivileged account and then switch context to the administrative user on a system only when necessary, but it also allows a root user to switch context to another user on the system. Care must be taken that administrators never impersonate a valid user for any reason. Ultimately any ability that any user has to alter data outside of the normal application interfaces can be seen as a violation of the regulations. Pharmaceutical companies have been cited for giving access to command prompts when this was not required for the duties of the user in question.[7]

The backup and disaster recovery capabilities of any FDA regulated systems infrastructure is perhaps the single most important requirement of any security infrastructure design. Retention times and sheer data volume make backup and recovery a challenge in the pharmaceutical environment. The SOPs, procedures, equipment, personnel, and media cannot be tested enough. The FDA expects to be able to completely recreate a study at some time in the future. Companies can only expect to be able to comply if they have well thought out backup, disaster recovery and data retention plans. While most backup media today is relatively durable testing of backups is critical. Tapes in storage should be tested often and copied to fresh media every few years to ensure that if required the data can be retrieved. Systems, software and storage devices must be maintained and older data stored in antiquated formats must be kept current with new technology to ensure that a lack of access to compatible hardware and software does not stand in the way of information recovery at a later date. Offsite storage is not left as an option; it is required because the loss of a facility cannot prevent data about a pharmaceutical study from being produced in a human readable format for FDA inspection.[8] Tapes and backup media that are kept on site should be physically secured and carefully controlled, as they will contain sensitive data about drugs in production and in clinical trails. Lastly any backup scheme must include the ability to backup and successfully restore all electronic signature information as well as audit logs. Recreated

[6] McDowall, p.3.
[7] McDowall, p.3.
[8] FDA Guidance for Industry, p.9.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

user accounts and passwords or digital certificates and keys may not be acceptable to validate electronic signatures created before a given disaster.

Conclusion:

Securing pharmaceutical data systems presents some unique challenges. Technology improvement and expected life cycle are at direct odds with the data retention and availability requirements posed in the rules. Systems are expected to be as secure as is possible but patches and configuration changes are prohibited or at least delayed by testing and validation requirements. The security administrators in this space will likely find themselves defending aging, unpatched systems with extremely critical data stored on them. Insider attack problems are vastly expanded to include accidental and seemingly innocuous changes to systems and data that would be very small comparative problems in other IT areas. The requirements are vague and meant to establish minimum requirements for security; organizations are left to interpret what exactly constitutes compliance.

The most critical thing to remember about security infrastructure design for pharmaceutical clinical trial systems is the differing interpretations of the regulations, and the sheer size and complexity of the task at hand. This will not be an endeavor security professionals take on alone. To create a successful, compliant infrastructure you must work closely with many departments and groups within an organization. This document was meant as an introduction to the special security challenges posed by FDA regulations on the pharmaceutical industry and potential solutions. The infrastructure guidelines made are one author's interpretation of the rules and guidance documents put out by the FDA. Requirements, SOPs, and interpretations of the rules may change company to company and the realities of user requirements may force security professionals into risk assessments that point to the need to deviate from what would be ideal from a security perspective. By keeping current with the FDA guidance documents and regulatory actions, security professionals will have a better idea of what the FDA inspectors are expecting to see and can therefore make more informed product and design decisions.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

Adams, Carlisle & Lloyd, Steve. "Core PKI Services: Authentication, Integrity, and Confidentiality." Understanding Public Key Infrastructure. 2002. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/prodtech/corepki.asp (March 18, 2002).

Department of Health and Human Services. "21 CFR Part 11Electronic Records; Electronic Signatures; Final Rule." Federal Register. March 20, 1997. URL: http://www.21cfr11.com/files/library/government/21cfrpart11_final_rule.pdf (March 18, 2002).

Einwechter, Nathan. "Preventing and Detecting Insider Attacks Using IDS." March 20, 2002. URL: http://online.securityfocus.com/infocus/1558/ (March 21, 2002).

Fields, Timothy. "Impact of 21 CFR Part 11 on Computer-Related System Validation." Journal of Technology Validation. August 2001. URL: http://www.ivthome.com/free/jvtv7n4pg311.htm (March 20, 2002).

Food and Drug Administration. "Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures Validation." August 29, 2001. URL: http://www.fda.gov/cber/gdlns/esigvalid.pdf (March 20, 2002).

Food and Drug Administration. "Guidance for Industry, Computerized Systems Used in Clinical Trials." April 1999. URL: http://www.fda.gov/ora/compliance_ref/bimo/ffinalcct.htm (March 18, 2002).

Goldhammer, Alan PhD. "Re: Proposed FDA Guidance on the Scope and Implementation of 21 CFR part 11." October 29, 2001. URL: http://www.fda.gov/ohrms/dockets/dockets/00d1541/c000001.pdf (March 19, 2002).

McDowall, R.D. "Qualification of Computer Networks and Infrastructure." American Pharmaceutical Review. 2001. URL: http://www.americanpharmaceuticalreview.com/past_articles/2_APR_Summer_2001/McDowall_article.html (March 19, 2002).

Xcert International. "Meeting the FDA's Requirements for Electronic Records and Electronic Signatures." URL: http://www.21cfrpart11.com/files/library/compliance/xcert_fda_white_paper.pdf (March 20, 2002).

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced