Ryan Morlok
rmorlok2@uiuc.edu

Issues in Information Security and Verifiability for Biomedical Technology Companies

Introduction

Most people are aware of the existence of the Food and Drug Administration (FDA) and it affect on their daily lives. We all live with the security that the FDA is watching over companies that not only provide us with our daily food, but also the medical services and products that treat us for our regular and emergency physical needs. As part of this oversight, the FDA provides guidance and requirements for best practices during the research and evaluation testing of new drugs and medical products.

The medical research industry, along with every other industry in the world, has been undergoing significant changes throughout the last 20 years due to the proliferation of information technology (IT). Where previously all records were kept in paper, in modern times much information is available digitally, and with this transition to the new medium, a new set of problems has emerged. In response to these changes, the FDA has enacted regulations that apply to digital records. It now the responsibility of both medical providers (doctors serving patients) and medical researchers (doctors evolving the medical discipline) to comply with these IT policies. This paper will focus on the compliance issues for the latter, looking at regulations relating to taking a medical product from conception to the market.

The Medical Research Process

The medical research process can be broadly summarized by the following phases:

1) Product conception and pure scientific research
2) Initial product testing (animals, not human test subjects)
3) Clinical testing (human testing)
4) Product release

During the product development process, medical and pharmaceutical research companies are concerned with several things regarding records they must keep:

- *Intellectual property protection*
  The cost of developing new drugs has been estimated to be as high as $805 million [1] and the development costs of other medical devices and technologies can be similarly impressive. Due to this large investment in research, medical and pharmaceutical companies are anxious to protect their intellectual property developed through the research process until it can be formally protected by the legal patents. The ability to keep internal research records secure is vital to the businesses success.
- *Documentation demonstrating thorough product testing*
  Product testing is common to most any industry, however this process is much more formalized and regulated in the medical and pharmaceutical industries. Referred to as clinical testing, the products must be tested in animals, then in small groups of people, and finally a large, diverse sample of people prior to being released to the market. Obviously there is regulatory need to prove the safety and effectiveness of the product at each step before moving to subsequent, broader tests.
- *Traceability through the manufacturing process*
  As the product is manufactured, information must be maintained tracing which components went into which products. Again, this is common to other industries (the automotive industry, for example), however in most other industries the urgency is not as great. If a medical device manufacturer finds that some electrical component from a

certain lot of their supplier was defective, they must be able to quickly identify which of their products could be affected, in order to notify the potentially at-risk patients. This was the case with some defibrillator products offered by medical device maker Guident over the last year.

- *Documentation required for FDA approval*
  The need for this category of information is obvious. Before any new medical or pharmaceutical product can be released to the market, the FDA must approve it. It is important to note that the information required for the FDA overlaps much of the information already listed.

The areas of concern listed above are somewhat overlapping, however each requires formal documentation that could (at least potentially) be submitted to the government (when applying for a patent, when applying for FDA approval for a new product, etc.).

FDA Regulations

FDA regulations are released in the form of CFRs (Code of Federal Regulations). These regulations relate to all areas under the FDA's control, most of which have nothing to do with IT, however a small subset of the regulations deal Information Technology in regulated industries. The following is a list of such regulations that at least tangentially relate to IT:

- **21 Food and Drugs**
  - **21 CFR Part 11** – *Electronic records; electronic signatures*
    Of these regulations, 21 CFR Part 11 is by far the most influential. Much attention has been paid to it in terms of compliance and its impact on existing systems. Part 11 defines the way that all records are to be kept, as required by other regulations.
  - **21 CFR Part 21** – *Protection of privacy*
    This section deals with the rights to privacy of individuals contained in FDA records, as well as the procedures required in order to disclose private

information. Some information in this part is analogous to the privacy requirements of HIPAA.

- **21 CFR Part 820** – *Quality system regulation*

  This section covers a broad area relating to quality control. Things ranging from change management of designs of medical devices to controls that need to be put in place restricting access to manufacturing materials are addressed in this section. IT is not generally address specifically, however audit trails are required for many topics, which places requirements on any electronic systems used to keep track of this information. This once again feeds into the requirements laid out in 21 CFR Part 11.
- **21 CFR Part 821** – *Medical device tracking requirements*

  This part defines requirements for devices that must be tracked by their makers, as required by the FDA. Devices that could potential be harmful to the general public's health, or any device that will be implanted in a person for more than one year, must be tracked by the manufacturer. This is largely so that appropriate people can be alerted if a problem is found with the device. Again, this part does not specifically refer to IT requirements, however it impacts what information must be kept and stored by computer systems involved in device manufacturing.
- **21 CFR Part 1311** – *Digital certificates*

  This part defines requirement for a public-key infrastructure (PKI) used to place orders for controlled substances. The section describes restrictions on policy, authentication, and other areas related to such a system. The requirements of this section is not relevant to many medical or pharmaceutical companies, only those which much deal with controlled substances.

Of these Federal regulations, this paper will focus primarily on 21 CFR Part 11. This section provides the groundwork on which the documentation requirements of other CFRs are built.

21 CFR Part 11

Background

As IT began to evolve, and more laboratory equipment and administrative processes began to be computer based, the FDA recognized that it was important to put in place controls that would allow the benefits of this new technology to be realized, while at the same time maintaining the same safeguards of public health.

As such, the FDA released the draft guidances of 21 CFR Part 11 that went into affect around 1997. Unfortunately, as is the case with much new legislation after it is released, the scope of the rules were too broad and companies were scrambling to become compliant. It wasn't initially apparent the degree to which the FDA would enforce the rules, and obviously there was no way that companies could become compliant over night.

The guidelines laid forth in 21 CFR Part 11 are not unrealistic when one is designing a new system from the ground up. Rather, the difficulties come primarily when one is attempting to apply them to ones existing systems, which were simply not designed with the level of traceability required in mind. As with other new legislation when it is first released, attempting to comply with 21 CFR Part 11 was costing more money, and requiring more organizational focus than the FDA had initially envisioned.

To their credit, the FDA was both open and responsive to the concerns of industry, and went back to reassess the scope and applicability of the rules stated in 21 CFR Part 11. In 2003 the FDA released guidance for industry that described the agency's current thinking on the topic. While the guidance was not a binding document for either industry or the FDA, it did represent the current internal thinking of the FDA in relation to the rules that were going to be enforced. The guidance document significantly reined in the scale and scope of the records that fell subject to Part 11, limiting it to those documents that were required to be kept for the FDA as stated by the GxP[1] standards, whereas previously it had also included all supporting documents as well.

[1] GxP refers to the Good *blank* Practices. These are the accepted standards use for an area of industry. For example, GLP refers to Good Laboratory Practices; cGMP refers to current Good Manufacturing Practices.

Regulation

The following is an outline of the contents of 21 CFR Part 11:

- 21 CFR Part 11
  - Subpart A – General Provisions
    - 11.1 Scope
    - 11.2 Implementation
    - 11.3 Definitions
  - Subpart B – Electronic Records
    - 11.10 Controls For closed systems
    - 11.30 Controls for open systems
    - 11.50 Signature manifestations
    - 11.70 Signature/record linking
  - Subpart C – Electronic Signatures
    - 11.100 General requirements
    - 11.200 Electronic components and controls
    - 11.300 Controls for identification codes and passwords

In the general provisions section, the FDA lays out the scope for which electronic signatures and records can be used. Permission is given to use electronic signatures and records for any paper procedure that is in place, provided the signatures and records comply with the requirements laid out in Part 11. The only exceptions to this are regulations created after August 1997 (when Part 11 came into affect) that explicitly name the requirement of paper-based records.

The general provisions section also gives definitions for terms used throughout the regulation. These definitions will be discussed as associated with their appropriate topics.

Electronic Records

§11.3.b.6 *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

The controls that must be set in place for systems that generate electronic records are broadly classified into two categories: open systems and closed systems. Closed systems refer to any system in which access to the system is constrained (physically otherwise) to those individuals who are actually responsible for the content of the records in that system [7].

In closed systems, there must exist checks to ensure that only the appropriate people have access to the data. The system must be validated to make sure that it is reliable, and that it accurately maintains the information contained in the records. Beyond controlling simple access to the system, there must exist documentation for the system, and controls must be put in place to ensure that only those who should have access to this documentation do.

Change control must be employed in regards to any system that generates electronic records. There must exist an audit trail for any changes that were made to the actual system, or the documentation relating to that system. An organization should be able to produce a time-sequenced report of changes to given system.

Another major required component of systems that handle electronic records is that they maintain an audit trial of interaction with the system. Actions that create, modify, or delete electronic records within the system must be securely logged using a timestamps. Furthermore, this audit trail must kept at least as long as it is required to keep the actual electronic records, and the audit trail should be readily available if the FDA requires it for review.

While closed systems have a high degree of control over who could potentially have access to the data, in open systems things are obviously less secure. As a result further precautions above and beyond those used for closed systems must exist to protect the integrity of records. Open systems would include computers that are available for general use. For example, a common computer in a lab that is used to record data from a lab instrument, but is also used as a general email terminal would be considered an open system. In these systems, encryption and related cryptographic methods should be used to ensure the integrity of the records.

As is apparent from the definition, the term ‘electronic records’ as defined by the FDA is rather all encompassing for anything that is created on a computer. This broad definition was one factor that led to concern and confusion after the regulation was released. Under this definition, any Microsoft Word document or even any email is classified as an electronic record. When the regulation was first released, this created a lot of confusion and concern about the FDA’s expectations. Later guidance for industry helped clarify the scope for things that required full audit trails and other requirements specified in Part 11.

Another challenging component of the FDA’s requirements for electronic records was the mandate that the organizations be able to “generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency” (§11.10.b). The human readable component is the largest challenge in this statement. Raw digital data such as measurement voltage samplings from an instrument, or audio recording from a patient’s heart, do not have a clear way by which they can be placed in a human readable form. This type of data would simply appear to be continuous numbers, and making it human readable can in many cases only give as implied representation of the data. This again was somewhat clarified with industry guidance by the FDA.

A Background on Electronic Signatures

§11.3.b.8 *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and expected to be adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

§11.3.b.7 *Electronic signature* means 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 document can be verified.

In days before computers, and for a large part still today, a person's signature has been used as his or her method of conferring consent or seal to a document. By signing a document, a personal typically acknowledges that they have read the document, and agree with this contents. In essence, the signature places the individuals good name behind the validity of the document in question.

With the advent of computers, it is not apparent to the common person what should be the logical replacement to this process. It is naïveté to think that a scanned or touchpad[2] version of one's handwritten signature contains the same level of validating authenticity. Anything that has been entered digitally can be perfectly reproduced as many times as desired with no cost. Thus, if the supermarket wants to place the touchpad signature a customer that has just entered on the next ten purchases coming through the store, nothing is stopping them.

Before evaluating what can be done to create a somewhat analogous equivalent to handwritten signatures in the digital word, it is useful explicitly look at the services we wish a signature to provide. The following three items highlight the most important aspects of the use of signatures

1. *Authenticity*

   One of the primary uses for a signature is to show that a document has indeed come from a specific individual. Perhaps the best example of this is the written letter. In a world where most things are written on a word processor and then printed, the handwritten, personal signature at the bottom of the document provides the evidence that the alleged sender is in fact the true person. The same is true for the signing of monetary commitments (checks, credit card receipts, etc.). The signature provides proof that the appropriate person has authorized the transaction.

[2] As used in checkout lines around the country currently

2. *Integrity*

   The integrity of a document refers to the assurance that it has not been changed since it has left the original sender. This concern is often not raised for any but the most important documents in everyday life. For things like leases and loan commitments, however, individuals are typically required to initial each page or paragraph both as way to show that they have read that portion of the material, and to later prove that the document has not been changed after they have formally signed it.

3. *Non-repudiation*

   If conditions become unfavorable, an individual may wish to renege on a contract to which they have committed. To do so, they may claim they were not the person who made the original contract. In such cases, the use of the signature proves that it was in fact that particular individual who went into an agreement, as no one else would have been able to produce their signature.

With this understanding of the services that signatures provide, we can now look at how digital signatures are implemented. The workings of digital signatures rely on the use of public-key cryptography. Public-key cryptography is a mathematical technique in which two related numbers exists, such that one can be used to encrypt a message, while the other can be used to decrypt it. The number used to encrypt messages is referred to as the public key. It can be freely distributed to the world, without fear of compromising the encryption system. The number used to decrypt the message is referred to the private key, and it is kept secret to the world. The idea between the relationships between these two keys is that anyone who would like to send a secure message to the holder of the private key would encrypt the message using the public key. If secure, two-way communication is required, two key pairs would be used.

With digital signatures, the process of the public key cryptography is somewhat reversed. When one wishes generate a signature of a digital message, one first computes a hash of the message. A hash of a message is simply a deterministic way of computing a number that is representative of the entire message. The idea is that the hash value will be substantially smaller than the actual message, yet even a small difference between two messages will produce different hash values. A major reason hashes are used is because the digital signature techniques can be computationally intensive, and signing of the smaller hash value can be much faster than signing the original message in its entirety.

Once the hash of the message has been computed, the digital signature can be created. The digital signature is a number computed using the hash of the message and the private key of the user signing the message. The signature number is computed using the signature algorithm such that the signature can be verified, but not independently generated, by the public key. The private key can also not be deduced from the signature and the public key. The math behind cryptography is beyond the scope of this paper.

The final, signed, version of a message is simply the original message plus the number computed as the digital signature. To verify the signature, and individual would obtain a copy of signer's public key. The verifier would then compute the hash value of the message, in the same fashion that took place during signing, and then compare the hash value to the signature number using the public key. This would allow the user to verify that that signature was in fact valid for the given message.

The ability to verify the integrity of a message is an interesting property of digital signatures that does hold to the same degree in the physical world. Where a physical signature looks almost exactly the same every time it is given[3], the value of the digital signature is dependent on the content of the message. Thus, if the message for which the signature is given changes, the signature will no longer match the message, and the problem would be detected. One could think of this property as being roughly analogous to physically signing (in rather large letters) the entire page of a document rather than simply on the line at the bottom. If someone wanted to change the contents of the document, they would end up messing up your signature in the process, and thus the fraud could be detected.

While the abilities of digital signatures may seem like the panacea of determining the signer and integrity of the document, it must be understood that technology alone cannot solve this problem.

[3] In fact, it is this property that makes them useful. The ability to replicate the same writing pattern using a pen (not a photocopy) is what is used as the basis for verification of the signature.

If a user’s private key is stolen, the thief can then produce perfect digital signatures of any document. Thus, the security of a system using digital signatures rests in the hands of the policies in place regarding the proper use and storage of an individual’s private keys.

Regulations Regarding Electronic Signatures

Issuing of the Signature

Many of the regulations regarding electronic signatures are fairly intuitive. Before an electronic signature can be issued by an individual, the identity of that individual must be verified. This would likely include asking for standard forms of proof of identification, such as a drivers license or passport, and could possibly be as extensive as a background check.

Once the identity of the individual has been verified, the individual must confirm in writing that they intend to use the electronic signature in a legally binding way. This intention must be communicated to the FDA in paper form, containing the individual’s handwritten signature.

Finally, electronic signatures must be bound to a single individual. While this may seem elementary, this implies that an organization cannot assign a electronic signature to a role, and that any one taking on the role can use the electronic signature. Instead, the FDA wishes to bind any electronic signing to a single individual in order to enforce responsibility on that individual.

Signing of an Electronic Record

Prior to signing an electronic record a user must authenticate himself to the system. If biometric authentication is used, then this may be the sole form of identification, however if a non-biometric method is used, then the authentication must be two-fold (username and password, for example). Any form of biometric authentication must be properly verified to correctly identify users, and to not allow unauthorized users to access the system.

The act of signing an electronic record must be explicit as well. The user currently logged on to the computer is not sufficient, as this does not imply consent to signing the task at hand. Rather, for the first signing in a continuous series of tasks the user must use all forms of identification (type in their username and password, for example), however for later signings within that session, the user may optionally be only required to provide one form of identification (their password to carry on this example).

If usernames and passwords are employed within the system, protocols must be in place to properly deal with maintaining these elements. The system must maintain that all username/password combinations are unique (which would generally be handled by having no two users have the same username). Passwords must be periodically expired to reduce risks of passwords being discovered over time. There must be a procedure in place to handle cases where passwords are lost or stolen, and there must also be mechanisms to report unauthorized attempts to use signatures.

Signatures for Hybrid Records

Some organizations may wish to keep records digitally, but not employ electronic signatures. In these cases, in order to authenticate the validity of the document, an identifying portion of the recorded is printed to a paper form at which point a handwritten signature can be applied to the document. In a system such as this, it is vital that the printed portion of the record not only uniquely identify the record, but also contain enough information to later prove that the current state of the digital record has not changed since the handwritten signature was applied. To do this, methods such as timestamps and hash values are used.

If all information required by the predicate rules (GxP requirements) is printed to hardcopy before the handwritten signature is applied, the organization is considered to be using paper records, and the 21 CFR Part 11 rules do not apply.

A Risk Centric Approach to Compliance to 21 CFR Part 11

As stated previously, when 21 CFR Part 11 was initially released in 1997, it was unclear what direction the FDA would take in terms of enforcement. The scope of the regulation was broad and companies were unsure how to best utilize resources when focusing on compliance. Subsequently, in 2003, the FDA released a final guidance for industry that indicated the FDA would use a risk-based approach when enacting enforcement. As such, companies should take a similar approach when allocating resources to the compliance process.

The ultimate goal of the FDA, in all its regulations and efforts, is to protect the safety of the public. The FDA above all does not wish for unsafe drugs or devices to reach the market, whether they be unsafe from fundamental design, or simply flaws in the manufacturing process. As such, when one assesses ones systems for in terms of compliance, it is from this basis that one should evaluate risk. Companies need to look at each of their systems, and assess which systems and controls are the most critical in terms of maintaining product safety.

Part 11 is built on, and intended to enhance, the rules set forth in the GxP. As part of the GxP rules, companies are required to perform risk assessments of their products and processes, and put in place measures to manage that risk (be that a technical fix for something that can be improved through technology, a process if it risk can be mitigated by management of activities, or a warning label to the consumer if the risk is simply inherent to the product). As part of this risk assessment process, companies can asses whether the integrity of an electronic record is vital to safety. If so it falls under the restrictions of Part 11. If not, the company can handle it normally, as described by the applicable GxP. [3]

Several potential methods of risk analysis are suggested in [3] that could be used to work towards Part 11 compliance:

- *FTA (Fault Tree Analysis)*
  Fault Tree Analysis is top-down approach to analyze potential failures. One deductively selects potential top-level failures, and then analyzes potential lower level failures that could be the cause. The fault trees are typically modeled in a fashion similar to logic gates, using ANDs and ORs, to illustrate that the sequence of events that must happen for a top-level failure to occur.
- *FMEA (Failure Modes and Effects Analysis)*
  Failure Modes and Effects Analysis was first used in the 1960's and 1970's by reliability engineers to evaluate and document potential failures in a product or process. These analyses

were later used to try to reduce or eliminate these risks in the system. A fundamental assumption of FMEA is that all potential failures are predictable and preventable, thus this methodology is not designed to manage unavoidable risks, however it can be useful nonetheless.

- *FMECA (Failure Mode Effects and Criticality Analysis)*
  Failure Mode Effects and Criticality Analysis originally came from the military in the 1950's. It is a somewhat simple methodology in which one categorizes and ranks potential process failures and critical issues, and then targets effort to address those issues.
- *HACCP (Hazard Analysis and Critical Control Points)*
  Originally developed by Pillsbury in the 1960's, HACCP has always had a strong standing in the food and medicine area. At the core of HACCP, one determines the critical control points of a process, and establishes baselines against which the process or procedure can be checked to make sure things are running correctly. Additionally, actions are defined to deal with situations when the process is not functioning within expected limits. All of these procedures are documented.

Using one or more of these methods of risk analysis, organizations can effectively assess their current processes, controls, and systems to determine the areas of most risk to consumer safety. From there, companies can then determine where their compliance efforts would best be spent to maximize public health.

Conclusion

As medical and pharmaceutical companies continue to become more advanced in the technology used in the research process, efforts to understand and manage the risk introduced by this technology will become even more important. Already, the FDA has put in place rules that allow these companies to take advantage of these new technologies while still maintaining the same level of individual accountability that is essential to enforce public safety. Continuing focus on these issues in the future is important to balance the efficiency needs of corporations with the public good.

References

[1] DiMasi, J. Hansen , R. Grabowski, H. *"The Price of Innovation: New Estimates of Drug Development Costs"*. Journal of Health Economics: 151-185 March, 2003.

[2] http://en.wikipedia.org/wiki/Digital_signature

[3] Lander, V. *"21 CFR Part 11 and Risk Assessment: Adapting Fundamental Methodologies to a Current Rule"*. Pharmaceutical Technology Europe, May 2004

[4] http://www.21cfrpart11.com/

[5] Federal Register, Volume 68, No. 37. pp. 8775-8776. http://www.fda.gov/OHRMS/DOCKETS/98fr/03-4312.pdf

[6] 21 CFR Part 11. http://www.access.gpo.gov/nara/cfr/waisidx_04/21cfr11_04.html

[7] Federal Register, Volume 62, No. 54. pp. 13464-13466 http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf