Paper SA07

Regulatory Scrutiny on Data Integrity: Are you safe?

Chris Decker, d-wise, Morrisville, NC, USA
Jon Horton, d-wise, Morrisville, NC, USA

ABSTRACT

Over the past decade we have helped dozens of life sciences clients identify, design, and implement their statistical computing environment (SCE) leveraging the best of breed technologies and optimizing their processes. During the past few years we have noticed a higher level of scrutiny by regulatory authorities around the clinical data lifecycle relative to an SCE. Our clients have been given formal warnings around topics such as unauthorized access, lack of traceability, and overall data integrity. These issues and how the regulatory authorities choose to enforce them could cause significant issues for pharmaceutical companies and delays in submission costing millions of dollars. This presentation will provide an introduction to why we should care about 21 CFR Part 11, what and how Food and Drug Administration (FDA) issues warnings, the issues d-wise has seen across our clients, how your company can be ready for the increased focus on data integrity, and a summary of the solutions we have implemented to address these challenges.

INTRODUCTION

Over the last five years d-wise has observed an increase in rigor of regulatory audits on the processes and systems biometrics uses to deliver their work. This scrutiny is causing sponsors to worry and assess their level of compliance and whether they might have an issue. Within this paper we will first provide an overview of the FDA audit and enforcement process, why 21 CFR Part 11 is important, and the challenges regulatory and sponsor companies are having in addressing these gaps. Then we describe a case study in delivery a solution that closes those gaps and describe what the key components of compliant framework look like.

In January of the year major sponsor had to pull back their application due to data integrity issues and the inability to provide traceability for their primary analyses. Companies need to wake up and be diligent about assessing their internal processes and technology.

FDA ENFORCEMENT

The primary objective of the Food and Drug Administration (FDA) is to assure compliance with the Federal Food, Drug, and Cosmetic Act. As such, the FDA has several enforcement tools available to correct/prevent violations, remove non-compliant products from the marketplace, and punish organizations that violate regulatory requirements within the space they operate.

While there are many enforcement options available to the Agency, including Form 483s, Warning Letters, seizures, injunctions, consent decrees, and criminal prosecutions, the most common and well known to most in the pharmaceutical industry are the 483 and the Warning Letter. However, while the names 483 and Warning Letter may be well known, it's been surprising how little is typically known about the details of each.

Below is a summary of both the FDA Form 483 and the Warning Letter, how they are related, and what to do in the event you are the recipient of one.

FDA Form 483

The FDA Form 483, also known as "Inspectional Observations," is an inventory of potential violations, listed in descending order of significance, provided to site management at the conclusion of an inspection. The Form 483

represents the judgement of the inspector at the time of the inspection and is not a final determination as to whether a violation of documented FDA requirements has occurred. It should be noted, however, that Form 483s are considered public documents and available to any individual upon request.

In the event you are the recipient of a Form 483, while not required to respond, it is highly recommended to provide a written response to the District Director and Lead Investigator within 15 calendar days. Any written response received after 15 days is not required to be included in the decision process which determines whether subsequent actions are required.

Warning Letter

After the inspection, the inspector completes an "Establishment Inspection Report" which, in addition to the site's written response to the Form 483, is reviewed by other FDA officials. If, after review, it is determined that a violation of regulatory significance, with the potential to lead to an enforcement action has occurred, the agency may issue an FDA Warning Letter.

A written response, detailing corrective and preventative actions that will be implemented to reduce the likelihood of issue recurrence, is required for all FDA Warning Letters.

WHY 21 CFR PART 11?

21 CFR Part 11 (Part 11) is a well-known regulation, even if only by name, for anyone who's used computerized systems in the pharmaceutical industry during the past two decades. At its core, Part 11 establishes the requirements for recognizing electronic records as equivalent to paper records and electronic signatures as equivalent to hand-written/we-ink signatures. But, as you'll see in this presentation, adherence to these requirements, and associated data integrity requirements, has been put somewhat under a microscope in the past few years, with the number of data integrity findings increasing steadily year over year. So, what are the requirements of Part 11 and how did we arrive here?

In the early 1990's, the Life Science industry, an industry that once gave preference to paper records over the adoption of electronic records, began to increase its reliance on computerized systems. In response, the FDA published the final rule on electronic records and signatures, 21 CFR Part 11, in 1997, with the final guidance, Computerized Systems Used in Clinical Trials, being published in 2007.

As mentioned above, Part 11 establishes criteria that must be met by Life Science companies, where applicable, to recognize electronic records as equivalent to paper records and electronic signatures as equivalent to wet-ink signatures. The criteria are:

- **Validation**
  Demonstrable evidence created in accordance with an approved process to ensure the accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.
- **Record Generation**
  The system must 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.
- **Record Retention**
  The system must protect records to enable their accurate and ready retrieval throughout the records retention period.
- **Audit Trails**
  The system must employ the use of secure, computer-generated, time-stamped audit trails to independently record the date and time of entries and actions that create, modify, or delete electronic records. Additionally, record changes must not obscure previously recorded information.
- **Limit System Access to Authorized Users**

The system must employ authority checks to ensure only authorized users may access the system and perform only the operations allowable for said user.

- **Operational System Checks**
  Where appropriate, the system must employ operational system checks to enforce permitted sequencing of steps and events.
- **Device Checks**
  Where appropriate, the system must employ device checks to determine the validity of the source of data input or operational instruction.
- **Training of Users**
  Demonstrable evidence that that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.
- **System Documentation**
  The establishment of, and evidence of adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures. Additionally, there must be demonstrated control over the access and use of documentation for system operation and maintenance.
- **Digital Signatures**
  Must contain the printed name of the signer, the meaning of the signature, and the date/time when the signature was applied.

With computerized systems now integral to nearly every aspect of drug development, including systems related to the manufacture of drug product, testing, clinical analysis, trending of safety events, product complaints, Corrective and Preventative Actions (CAPA), among others, it is critical to ensure the records produced by these systems are of the highest integrity which, in part, is accomplished through adherence to the requirements set forth in 21 CFR Part 11.

To most, compliance with Part 11 is viewed as a daunting task. And, while electronic service providers and other vendors exist today to help support that compliance path with software, platforms, and infrastructure via a Software/Platform/Infrastructure as a Service (SaaS/PaaS/IaaS) model, the early days of adoption saw most organizations creating and maintaining in-house developed systems.

There is no question the rise in adoption of computerized systems to support drug development brought a wealth of benefits, e.g. streamlined business processes, reduced turnaround times for key processes, and reduction in process costs to name a few, but it also brought with it complexity and costs required to develop and maintain compliant systems in a validated state. Pharmaceutical companies and Contract Research Organizations (CROs) quickly became both Life Science AND technology companies, with the expectation that the technology components also be built to support all relevant regulatory requirements. This was, and is, a complex and challenging task to accomplish.

In the 2000's and 2010's, the emergence of Life Science focused SaaS/PaaS/IaaS electronic service providers became the miracle drug for an industry facing extreme pricing pressures due to patent cliffs, over-burdened IT organizations, and multi-year/over-budget deployments of specialized in-house developed solutions. Simply put, the emergence of Life Science focused SaaS/PaaS/IaaS solutions provided cheaper, faster, and better alternatives to in-house developed and maintained specialty systems.

CAN HEALTH AUTHORITIES KEEP PACE WITH INDUSTRY?

While the FDA recognizes sponsors and other regulated entities are increasingly choosing to outsource electronic services to SaaS/PaaS/IaaS providers, the Agency has not published significant formal guidance on the implementation of 21 CFR Part 11 since May 2007, well before the use of hosted electronic services for regulatory/GxP purposes was considered commonplace.

There is, however, recent evidence to suggest the Agency is ready to weigh in on the transformation happening in the Life Science industry that is being driven by advancements in technology. In June 2017, the FDA published a draft guidance "Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 –

Questions and Answers." While this guidance is considered draft and is being distributed for comment purposes only, it still provides insight to the current thinking of the Agency regarding the use of outsourced electronic services.

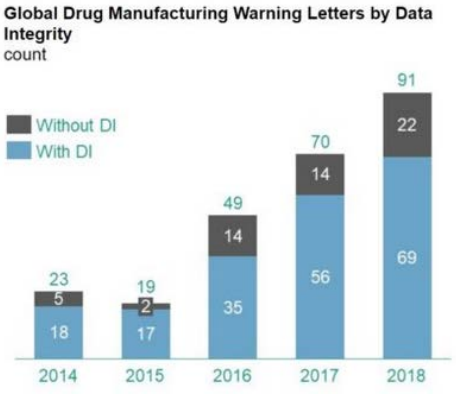
Specifically, when electronic services are used to process data for Health Authority regulated activities, the FDA recommends confirming adequate controls are in place to ensure the integrity and confidentiality of the data. Recommended factors, with our proposed controls to evaluate against, are included in Table 1 below:

TABLE 1

Data Security Safeguard	Recommended Controls Implemented by Vendor
Validation Documentation	1. Ensure the vendor has an established validation standard that aligns with industry best practices 2. Ensure there is documented evidence which shows the vendor's system/application was validated in accordance with their approved standards 3. Ensure the vendor has a change control standard, assuring changes made to the system are done so in a state of control and, if applicable, allow for client engagement in the event additional testing (e.g. User Acceptance) is required prior to production use
Ability to generate accurate and complete copies of records	1. Ensure the vendor has documented and tested backup backup/restore capabilities 2. Ensure the vendor's Recovery Point Objective (RPO) and Recovery Time Objective (RTO) capabilities meet your requirements
Archiving Capabilities/Availability and retention of records for FDA inspection for as long as the records are required by applicable regulations	1. Ensure the vendor has robust and tested backup and restore capabilities? 2. Ensure the retention period of backups can be configured to meet regulatory commitments required of you, the vendor's client 3. Ensure the vendor has an approved Disaster Recovery Plan 4. Ensure the vendor's Disaster Recovery Plan been tested and has a defined test frequency that is acceptable
Access controls	1. Ensure the vendor can demonstrate ability to restrict system access to only authorized users 2. If required, ensure the vendor can demonstrate ability to restrict access to specific locations within the application/system based on established permissions 3. Ensure there is evidence of these controls being defined and tested in the vendor's validation package
Secure computer-generated time stamped audit trails of user actions and changes to data	1. If required, ensure the vendor's system/application can provide secure date/time stamped audit trails 2. If required, ensure the audit trail identifies who performed an action and the reason for the action 3. If required, ensure previous values/entries are maintained and not overwritten or deleted
Encryption of data at rest and in transit	1. Ensure the vendor employs controls to ensure data is encrypted at rest and in transit 2. Ensure the encryption method employed by the vendor is sufficient to protect the integrity of your data
Data Confidentiality and Security	1. Ensure the vendor provides appropriate segregation (e.g. private LAN and hardware) to ensure your data is not co-mingled with other client's data

Data Security Safeguard	Recommended Controls Implemented by Vendor
	2. Ensure the vendor employs appropriate network firewall configurations to ensure only traffic from your network can attempt access to the deployed system/application
Performance record of the electronic service vendor and the electronic service provided	1. Ensure the vendor allows for on-site audits to be conducted at their office location and, when applicable, the data center where your system/application will be hosted 2. Ensure the vendor has qualified their partner data center, if applicable? 3. Ensure SOC2 Type 2, ISO27001, or other similar reports/certifications available for review 4. Ensure the vendor has approved procedures in place to govern the completion of activities related to the development, deployment, and maintenance of client systems/applications (e.g. policies, procedures, training, validation, security, change control, support, CAPA, auditing, document control, etc…)
Monitor the vendors compliance with electronic service security and data integrity controls	1. Ensure the vendor implements industry standard physical and logical security controls 2. Ensure SOC2 Type 2, ISO27001, or other similar reports/certifications available for review

ARE YOU READY FOR INCREASED FOCUS ON DATA INTEGRITY?



For decades the FDA has identified data integrity issues during inspections, with the number of findings steadily increasing as the industry continues to embrace the use of computerized systems and new technologies.

When considering the safety and efficacy implications, however, it should be of no surprise that the FDA and other Health Authorities are placing such importance on the integrity of the data being produced, stored, analyzed, and reported out of these systems. Its important to remember that, at the end of every clinical data point, there is a patient. A mom, a dad, a brother, sister, son, daughter, aunt, uncle, grandma, and grandpa who are placing their trust, and possibly their life, in the hands of a Life Science company's research, protocols, processes, and computerized systems…all with the hope that their involvement can lead to improved quality of life for themselves or future mankind.

To ensure the people, processes, products, and systems that contribute to the release of approved medicines do so in a way that ensures the safety, efficacy, and integrity of the medicines, Health Authorities like the FDA define regulations, e.g. 21 CFR Parts 11, 210, 211, and 212, that must be followed.

However, despite the identification and creation of data integrity related regulations, regulators initially struggled with the transition from a paper-based industry to a computerized industry. In recent years though, regulators have received the training necessary to inspect systems with an eye for data integrity gaps and to appropriately challenge perceived deficiencies.

The scarcity of data integrity related findings pre-2014, followed by steadily increasing rates of data integrity findings since is a clear signal that Inspectors are both trained and mandated to search out data integrity gaps associated with the creation of data, storage of data, analysis of data, and reporting of data. Examples of recent data integrity related findings illustrating this point can be found in the FDA's December 2018 publication of "Data Integrity and Compliance With Drug CGMP Questions and Answers, Guidance for Industry:"

- *§ 211.68 (requiring that "backup data are exact and complete" and "secure from alteration, inadvertent erasures, or loss" and that "output from the computer … be checked for accuracy").*
- *§ 212.110(b) (requiring that data be "stored to prevent deterioration or loss").*
- *§§ 211.100 and 211.160 (requiring that certain activities be "documented at the time of performance" and that laboratory controls be "scientifically sound").*
- *§ 211.180 (requiring that records be retained as "original records," or "true copies," or other "accurate reproductions of the original records").*
- *§§ 211.188, 211.194, and 212.60(g) (requiring "complete information," "complete data derived from all tests," "complete record of all data," and "complete records of all tests performed").*
- *§§ 211.22, 211.192, and 211.194(a) (requiring that production and control records be "reviewed" and that laboratory records be "reviewed for accuracy, completeness, and compliance with established standards").*
- *§§ 211.182, 211.186(a), 211.188(b)(11), and 211.194(a)(8) (requiring that records be "checked," "verified," or "reviewed").*

HOW DO YOU MEET DATA INTEGRITY REGULATIONS?

The ALCOA + requirements, a central tenet of the FDA's CGMP practices, outline the nine (9) core attributes of data integrity:

A – Attributable: Data collected or generated must be able to be attributed to the one collecting or generating the data

L – Legible: All required data must be readable and permanent

C – Contemporaneous: The record of an activity must be documented at the time the activity takes place

O – Original: The first write, or data source, including its full content and metadata

A – Accurate: Data is free from errors, complete, and a truthful representation of the activity or observation that took place

the above definitions represent the original five (5) attributes

the below definitions represent the four (4) attributes that comprise the "+"

C – Complete:	Data is complete; nothing has been deleted or overwritten and is verifiable through the audit trail
C – Consistent:	Data is recorded chronologically and is verifiable through the audit trail
E – Enduring:	Data is stored in a manner that ensures its durability and readability for at least as long as the required record retention period
A – Available:	Data is accessible throughout the life of the data

While the 9 data integrity attributes listed above seem simple in nature, the implementation of disparate, standalone systems that lack the integration capabilities necessary for seamless data sharing have made achieving compliance challenging and complex.

However, regardless the complexity or challenge associated with achieving compliance, compliance is nevertheless required to compete in this space. In our opinion, the fastest, least expensive, and best path forward for achieving compliance is to leverage the available Life Science SaaS/PaaS/IaaS offerings that meet your organization's needs, qualify the vendor in accordance with considerations listed in the FDA's 2017 draft guidance (Table 1 above), validate the use of the vendor's product within the framework of your processes and workflows, and ensure ALCOA + attributes are accounted for when activities performed are governed by regulatory requirements of a Health Authority.

QUALITY MIRAGE AND INDUSTRY GAPS

EMPEROR'S CLOTHING (DECKER)

In the famous story by Hans Christian Andersen, "The Emperor's New Clothes", two weavers convince the Emperor that he is wearing an invisible set of clothes that only the most privileged can see. However, he is naked and embarrassed in front of his whole kingdom.

This feels very similar to how our industry has been convinced they have implemented compliance through documents, processes, and checkboxes. We develop processes with significant manual intervention and human interpretation and expect it to lead to a high-quality deliverable at the end. We throw out many acronyms – SDLC, IQ/OQ, UAT, PQ, SOP, etc. – and expect that if we just write all these documents and check all the associated boxes then poof – we have quality!

The reality is that this is mirage. We end up creating a myriad of hidden issues despite all this documentation and checkboxes. There are so many examples of this within our clinical data lifecycle from the installation and qualification of a system to the development of code to generate the data to the review of our analysis results. Let's use one example.

The figure below is a picture of our process for generating data. A person develops a spreadsheet that attempts to describe the rules and algorithms that must be used to generate a derived data set and someone else (most likely people of a different native tongue) reviews it - CHECKBOX. Then two different people, again most likely people who write in a different native language program it separately, so we have 'matching' data – CHECKBOX. Then another person checks the final data set – CHECKBOX. All this independent work and checking must lead to a high-quality product – right? NO! While introducing these steps might provide us more opportunity to catch problems, it gives us a false sense of traceability and compliance because we are checking the box that we have specifications we have

better quality data and not focusing on the real need. We have spreadsheets and checkers and checkboxes and it doesn't actual mean better quality as we still rely too heavily on people to interpret and follow overly complicated processes.

Variable Name	Variable Label	Type	Controlled Terms or Format	Origin	Role	Core	Source Domain	Source Variable	Derivation
STUDYID	Study Identifier	Char		Protocol	Identifier	Req	AE	STUDYID	
DOMAIN	Domain Abbreviation	Char	AE	Assigned	Identifier	Req			DOMAIN = 'AE'
USUBJID	Unique Subject Identifier	Char		Derived	Identifier	Req	AE	STUDYID $UBJID	USUBJID=strip(STUDYID)||'-'||strip(SUBJID);
SUBJID	Subject Identifier for the Study	Char		CRF Page 1	Topic	Req	DM	SUBJID	
SITEID	Study Site Identifier	Char		CRF Page 1	Record Qualifier	Req	DM	SITENO	
AESEQ	Sequence Number	Num			Identifier	Req			Sort records by STUDYID, USUBJID, AEDECOD, AESTDTC and assign AESEQ to 1 for the first record, increased by 1 for each record.
AEREFID	Reference ID	Char		CRF Page 112	Identifier	Perm	AE	AESEQ	
AETERM	Reported Term for the Adverse Event	Char		CRF Page 112	Topic	Req	AE	AETERM	Keep only records with AENONE = ''.
AEDECOD	Dictionary-Derived Term	Char	AEDICT_F	Assigned	Synonym Qualifier	Req	AE	AEDECOD	Keep in mixed case.

STUDYID	USUBJID	AETERM	AESTDTC	AESEQ	DOMAIN	AESPID	AEDECOD	AEBODSYS
CDISCPILOT01	01-701-1015	VERBATIM_0995	2014-01-03	1	AE	E07	APPLICATION SITE ERYTHEMA	GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS
CDISCPILOT01	01-701-1015	VERBATIM_1126	2014-01-09	3	AE	E06	DIARRHOEA	GASTROINTESTINAL DISORDERS
CDISCPILOT01	01-701-1015	VERBATIM_1219	2014-01-03	2	AE	E08	APPLICATION SITE PRURITUS	GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS
CDISCPILOT01	01-701-1023	VERBATIM_0300	2012-08-07	1	AE	E08	ERYTHEMA	SKIN AND SUBCUTANEOUS TISSUE DISORDERS
CDISCPILOT01	01-701-1023	VERBATIM_0300	2012-08-07	4	AE	E08	ERYTHEMA	SKIN AND SUBCUTANEOUS TISSUE DISORDERS
CDISCPILOT01	01-701-1023	VERBATIM_1549	2012-08-07	2	AE	E09	ERYTHEMA	SKIN AND SUBCUTANEOUS TISSUE DISORDERS
CDISCPILOT01	01-701-1023	VERBATIM_1650	2012-08-26	3	AE	E10	ATRIOVENTRICULAR BLOCK SECOND DEGREE	CARDIAC DISORDERS

In my favorite Dr. Seuss book "Did I Ever Tell You How Lucky You Are?' there is a scene where the bee watcher is not watching hard enough so he needs a bee watcher-watcher to watch him – our version of that scene is below. This is the irony of our quality processes today.

"Oh, the jobs people work at! Out west near Complianceville there's a compliance watcher, his job is to watch. Is to keep both his eyes on the manual compliance process, a process that is watched will get better you see. So he watched and he watched, but in spite of his watch that compliance process didn't get any better. So then somebody said "Our old compliance watcher just isn't compliance watching as hard as they can, he ought to be watched by another compliance watcher! The thing that we need is a compliance-watcher-watcher!". Well, the compliance-watcher-watcher watched the compliance-watcher. He didn't watch well so another compliance watcher had to come in as a watch-watcher-watcher! And now all the compliance watchers who live in Complianceville are watching on watch watcher watchering watch, watch watching the watcher who's watching that compliance. You're not a Compliance Watcher you're lucky you see!"

INDUSTRY GAPS

As described above, the scrutiny of regulatory audits has increased significantly within the Biometrics space over the last 5 years. This has led to a plethora of findings that sponsor companies have had to address to ensure compliance. In the past clients have attempted to close those gaps through a mixture of implementing siloed technology and defining processes that are supposed to be followed. Unfortunately, gaps in technology, staff turnover, and stress filled deadlines have led to shortcuts and errors in following these processes.

Recently, a d-wise client was issued a 483 observation from the FDA which identified significant findings within the biometrics data flow space. These issues led to delays in submission, millions of dollars of remediation, and a lack of confidence internally and from regulators. Through our compliance assessments across a range of client we have identified a set of findings in key areas. A sample of those findings are summarized below.

User Management	Manual processes to set up and manage users led to errors over 25% of time
	Cannot reliably determine when a user was given an account and access
	Users flagged as accessing content after leaving the company
Content Access	Manual processes to protect blinded data not always followed or error prone
	Overcomplicated security models that are unmanageble and inaccurate
	Cannot ensure the most important data is controled and not modified
Workflow	Can't determine where and when 'final' outputs are generated
	Users unblinded incorrectly leading to invalid results
	Inabiity to understand the flow of artifact through the sytem
Traceabiity	Inability to follow the raw data through the system
	Inability to review who and when a file was moved or generated
	Can't ensure a file was not 'touched' after being reviewed

Most of our client are surprised and sometimes shocked when they are informed of the gaps they have in their technology and processes to ensure compliance and integrity.

CASE STUDY: BUILDING SOLUTIONS TO INCREASE DATA INTEGRITY

Sponsor companies are exploring options to support data integrity and ensure they have end to end compliance. Below is an example of a solution one of our client recently implemented to support this gap.

EXAMPLE CAPABILITIES

Recently, one of our clients implemented the solution where the highest priority was to ensure data integrity and compliance. In collaboration with the key business stakeholders, the solution was designed, built, and deployed with the following key components.

Study Setup	• Capability: Controlled creation of compounds, study and user groups to support a standard folder and user rolemodel • Value: Automated and controlled creation of studies and users eliminates human mistakes and standardizing
User Management	• Solution: User and Group management controlled through integrated and configured COTS solution • Value: user interface allowing the right users to add and remove users based on role and acess requirements
Code Promotion Workflow	• Solution: Controlled and audited movement of files through the development, validation, and production workflow • Value: Ensure the right user role can move and access files and audit all movements to capture traceability
Production Execution	• Solution: Controlled execution of code and generation of outputs in a read only production envirionment • Value: Ensure the programs executed have not been updated and are traced to the outputs being generated
File Sharing	• Solution: Delivery of raw data from external system to the platform with read only access and audit trails ; Controlled packaging of content to be delivered outside the system • Value: User interface, controlled, and audited file sharing

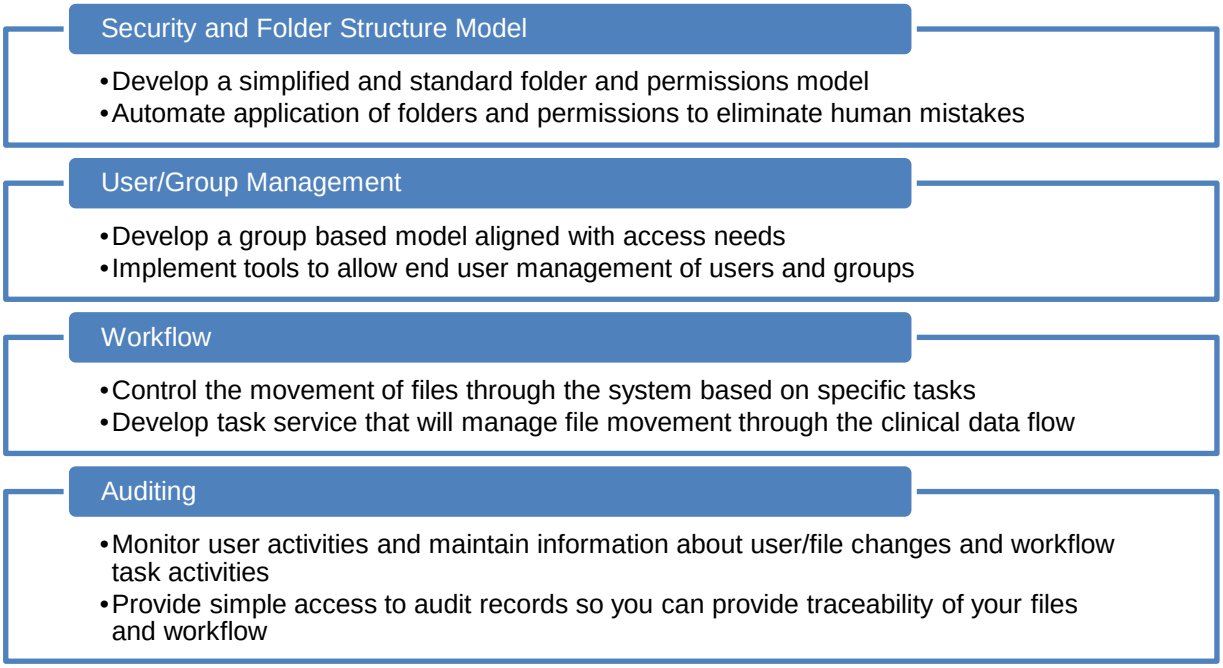
The solution minimized the disruption to the business by making it accessible within an environment very familiar to the end user and hiding the technology plumbing under the covers (versioning, auditing, etc.). There are many approaches to implementing fir for purpose solutions that can control and manage compliance by using COTS and open source technologies that can be integrated and configured.

COMPLIANCE FRAMEWORK

Another key to implementing solutions to address compliance are to balance the need for controlling the process while ensuring you focus on user experience and don't overburden the end user with technology that makes it so difficult to do their job they look for ways around the rules. There are many factors in designing and implementing a compliance framework, but they all need to consider three simple concepts:

- **Usability:** Implementing compliance doesn't mean also introducing a painful process for the end user. Focusing on the user experience through user centric design can help balance the need for compliance with the end user experience.
- **Task Focused:** Most clients develop requirements such as "System must have versioning" or "System must have audit trails" with no real context of why or when these activities must occur. The need for compliance should be based on a task "The code is ready for validation" or "I need to send a package of data to FDA" and based on those tasks certain compliance activities are activated
- **Visibility:** Implementing compliance is one step. Being able to have visibility into the compliance capabilities you have implemented is even more critical. For example, turning on auditing for everything in the system is great – check I have auditing – but then having to troll thousands of audit records a week to try to track down what happened does not meet your end game

Below are the key components to develop and maintain a compliant framework



The key to implementing the components above is to focus on simplifying your overall needs and developing and/r configuring tools that can automate and provide a robust framework for compliance.

CONCLUSION

The FDA is becoming more sophisticated in identifying and enforcing data integrity gaps. As technology advances and continues to be adopted it's imperative that you understand how to engage properly with 3rd party vendors to have a complete and holistic solution. We also need to understand the regulatory drivers behind the adoption so we can implement compliant solutions that can ensure integrity of our most important asset – our data.

We must evaluate whether our current quality paradigm is actually focused on the right thing and leading to the quality we expect. Technology exists today that can solve these issues if we just understand and adopt it. It is possible to build a compliance framework that balances ability for users to get the job done with the data integrity checks that must be in place to ensure you have compliance required.

REFERENCES

FDA Form 483 Frequently Asked Questions: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/inspection-references/fda-form-483-frequently-asked-questions

RECOMMENDED READING

21 CFR Part 11 Regulations: https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Chris Decker
d-wise
Email: Chris.Decker@d-wise.com

Jon Horton
d-wise
Email: Jon.Horton@d-wise.com