



d-wise™

Accelerate to the Speed of Life

Regulatory Scrutiny on Data Integrity: Are you safe?

Chris Decker, d-wise
Jon Horton, d-wise

Who Is Responsible for Data Integrity?



Keep them Raised If...

You Have Complete/Comprehensive Understanding Of



Health Authority Data Integrity Regulations

Lastly, Keep them Raised If...

You Have Complete/Comprehensive Understanding Of



Your Organization's Data Integrity Strategy and Policies

Now, Imagine...

You Receive a Call from Your Security Desk



Now, Imagine...

And the FDA is Here to Inspect Your Systems!



Which One Are You?

Can you provide a record of the first write for X, and all changes with evidence of who did it, what they did, when, and for what purpose?

Uh Oh!

Show me the exact dataset that was submitted to the Agency



Does the system prevent deletion of original data?

Has every cGMP workflow been validated for its intended use?

Can you provide evidence of PAR to ensure only authorized users continue to have access?

We've Got This!

Who had access to these folders/files on dd-Mmm-yyyy?

What data produced this report?



What encryption standards are followed for data in transit and at rest?

The Reality Is...

Drug Manufacturing Data Integrity Warning Letters



Quick Reminder!



- Inventory of Potential Violations
- Descending Order of Significance
- Not Final Determination of Violation
- Does Not Require Your Response
- Considered Public Information



- Issued After Agency Review of 483 and Your Written Response (if provided)
- Determination That Violation Occurred
- Written Response Is Required
- CAPA Is Required

Data Integrity Regulation (Computerized Systems)



- VALIDATION
- RECORD GENERATION
- RECORD RETENTION
- AUDIT TRAILS
- AUTHORIZED USERS ONLY
- SYSTEM CHECKS
- DEVICE CHECKS
- TRAINING
- SYSTEM DOCUMENTATION
- DIGITAL SIGNATURES

ALCOA +



contemporaneous



legible

attributable

original



accurate



Can Regulators Keep Pace With Industry?



Leveraging Electronic Service Providers



DATA SECURITY SAFEGUARDS



VALIDATION DOCUMENTATION



ACCURATE AND COMPLETE COPIES OF RECORDS



ARCHIVING CAPABILITIES AND RECORD RETENTION



ACCESS CONTROLS

DATA SECURITY SAFEGUARDS



AUDIT TRAILS FOR USER ACTIONS AND CHANGES



ENCRYPTION OF DATA AT REST/IN-TRANSIT



DATA CONFIDENTIALITY AND SECURITY



PERFORMANCE RECORD OF ELECTRONIC SERVICE PROVIDER



MONITORING OF PROVIDER'S COMPLIANCE

DATA SECURITY SAFEGUARDS



VALIDATION DOCUMENTATION

Ensure Vendor Has Established and Acceptable Validation Standard

Ensure Vendor Has Demonstrable Evidence of Validating System Per Standard

Ensure Vendor Has Established and Acceptable Change Control Standard

DATA SECURITY SAFEGUARDS

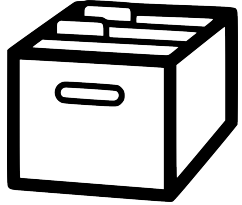


ACCURATE AND COMPLETE COPIES OF RECORDS

Ensure Vendor Has Documented and Tested Backup/Restore Process

Ensure Vendor's RTO/RPO Capabilities Meet Your Requirements

DATA SECURITY SAFEGUARDS



ARCHIVING CAPABILITIES AND RECORD RETENTION

Ensure Vendor Has Documented and Tested Backup/Restore Process

Ensure Vendor's Retention Period Can Be Configured to Meet Your Compliance Obligations

Ensure Vendor Has an Approved and Tested Disaster Recovery Plan

DATA SECURITY SAFEGUARDS



ACCESS CONTROLS

Ensure Vendor Can Demonstrate Ability to Restrict Access to Only Authorized Users

Ensure Vendor Can Restrict File/Folder Access to Only Authorized Users (if required)

Ensure Vendor Has Evidence of Testing Access Controls in Validation Package

DATA SECURITY SAFEGUARDS



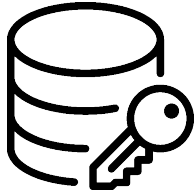
AUDIT TRAILS FOR USER ACTIONS AND CHANGES

Ensure Vendor Can Provide Secure Date/Time Stamped Audit Trails

Ensure Vendor Can Demonstrate Who Performed an Action and Why as Part of the Audit Trail

Ensure Vendor Can Demonstrate Original/Previous Values are Maintained and Not Overwritten

DATA SECURITY SAFEGUARDS



ENCRYPTION OF DATA AT REST/IN-TRANSIT

Ensure Vendor Employs Controls to Encrypt Data In-Transit and At Rest

Ensure Vendor's Encryption Standards are Appropriate to Maintain the Integrity of Your Data

DATA SECURITY SAFEGUARDS



DATA CONFIDENTIALITY AND SECURITY

Ensure Vendor Provides Appropriate Segregation to Ensure No Comingling of Data

Ensure Vendor Employs Appropriate Network Firewall Configurations to Allow Only Traffic From Your Org Access

DATA SECURITY SAFEGUARDS



PERFORMANCE RECORD OF ELECTRONIC SERVICE PROVIDER

Ensure Vendor Meets Your Requirements by Qualifying Them in Accordance With Your Process

Ensure Vendor Has Qualified Their Data Center Partner (if applicable)

Ensure SOC2 Type 2, ISO27001, or Other Similar Documentation is Available for Review

Ensure Vendor Has Appropriate Standards for Key Processes

DATA SECURITY SAFEGUARDS



REGULAR MONITORING OF PROVIDER'S COMPLIANCE WITH CONTROLS

Ensure Vendor Supports Regular Due Diligence Inspections

Ensure Vendor Provides Updated SOC2 Type 2 (or Other Similar) Reports for Review When Updated

Ensure Vendor Complies With Established SLAs

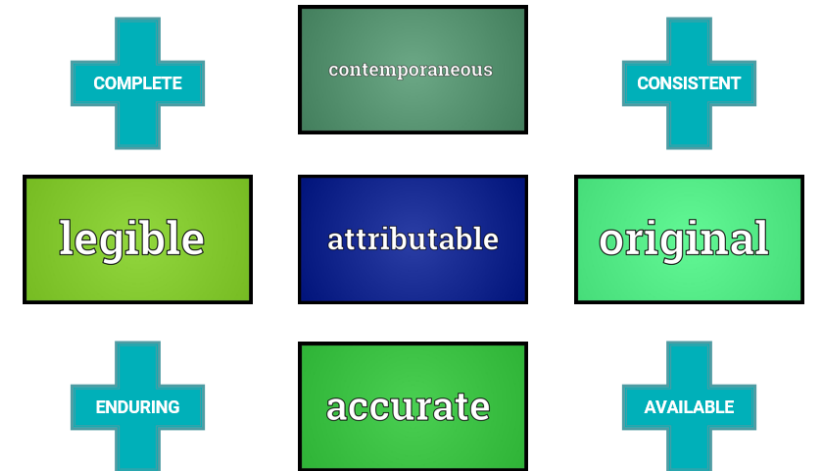
MAINTAINING COMPLIANCE



DATA SECURITY



SAFEGUARDS





Be afraid, very afraid...

Mirage of Quality



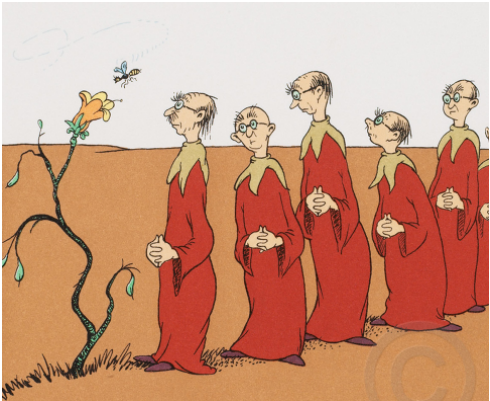
Variable Name	Variable Label	Type	Controlled Terms or Format	Origin	Role	Core	Source Domain	Source Variable	Derivation
STUDYID	Study Identifier	Char		Protocol	Identifier	Req	AE	STUDYID	
DOMAIN	Domain Abbreviation	Char	AE	Assigned	Identifier	Req			DOMAIN = 'AE'
USUBJID	Unique Subject Identifier	Char		Derived	Identifier	Req	AE	STUDYID SUBJID	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
CDISCPLOT01	01-701-1015	VERBATIM_0995	2014-01-03	1 AE	E07		APPLICATION SITE ERYTHEMA	GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS
CDISCPLOT01	01-701-1015	VERBATIM_1126	2014-01-09	3 AE	E06		DIARRHOEA	GASTROINTESTINAL DISORDERS
CDISCPLOT01	01-701-1015	VERBATIM_1219	2014-01-03	2 AE	E08		APPLICATION SITE PRURITUS	GENERAL DISORDERS AND ADMINISTRATION SITE CONDITIONS
CDISCPLOT01	01-701-1023	VERBATIM_0300	2012-08-07	1 AE	E08		ERYTHEMA	SKIN AND SUBCUTANEOUS TISSUE DISORDERS
CDISCPLOT01	01-701-1023	VERBATIM_0300	2012-08-07	4 AE	E08		ERYTHEMA	SKIN AND SUBCUTANEOUS TISSUE DISORDERS
CDISCPLOT01	01-701-1023	VERBATIM_1549	2012-08-07	2 AE	E09		ERYTHEMA	SKIN AND SUBCUTANEOUS TISSUE DISORDERS
CDISCPLOT01	01-701-1023	VERBATIM_1650	2012-08-26	3 AE	E10		ATRIOVENTRICULAR BLOCK SECOND DEGREE	CARDIAC DISORDERS



Does this
deliver quality?



Real World Disasters

(1) That the applicant has failed to establish a system for maintaining required records, or has repeatedly or deliberately failed to maintain required records or to make required reports under section 505(k) or 507(g) of the act and 314.80, 314.81, or 314.98, or that the applicant has refused to permit access to, or copying or verification of, its records.

User who left the company accessed data three months later

Hacked together scripts for moving data contained clear text passwords

Users who were supposed to be blinded accessed sensitive data

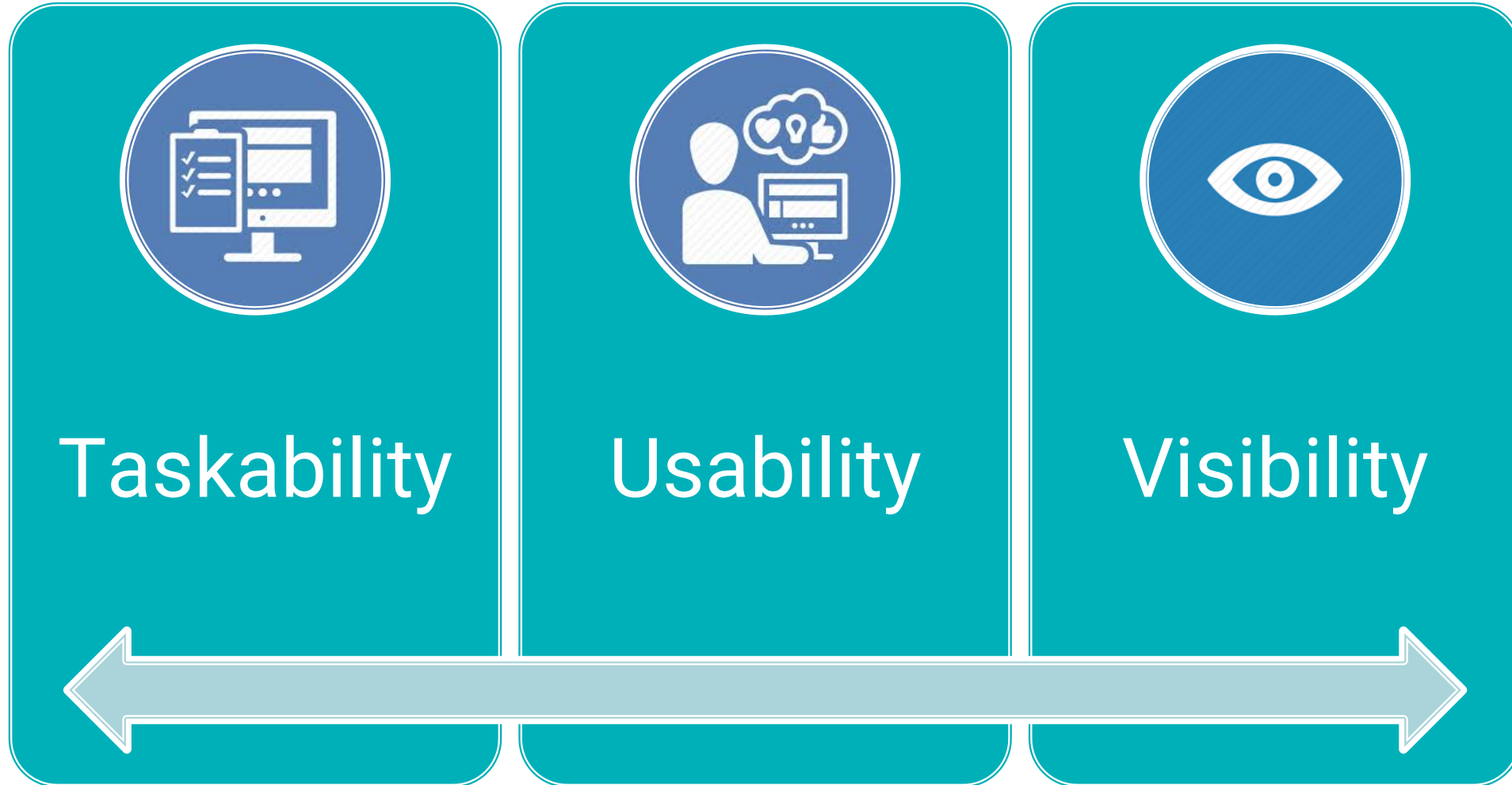
Can't identify which version of the raw data was used for the analysis

Don't know which user ran the final TFLs that were produced

Don't know which security groups a user is in and what studies the groups can access

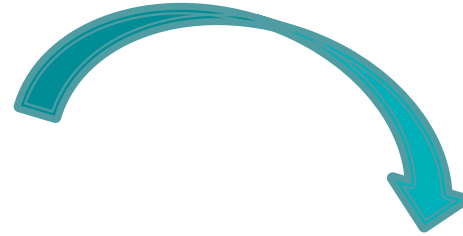


Compliance Themes



Taskability

Move from “The system shall...”



To “The user needs to take this step...”

~~“I need to version!”~~

NO

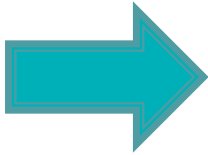
“I am ready for my code to be validated”

And behind the scenes...

- ✓ Code is moved
- ✓ Code state is changed
- ✓ Code is versioned
- ✓ Audit trail is generated

YES

Usability



PARKING SCHEDULE			
	M-F	SAT	SUN
7am	(P) FREE	(P) FREE	(P) FREE
8am	(R) [Red Hatched]	(P) 1 HR	
8 ³⁰ am	(R) [Red Hatched]	(R) [Red Hatched]	
		(P) 1 HR	
4pm	(P) 1 HR		
7pm	(P) FREE	(P) FREE	

Compliance doesn't have to be painful

Focus on integrating human centered design with the required compliance needs

Visibility

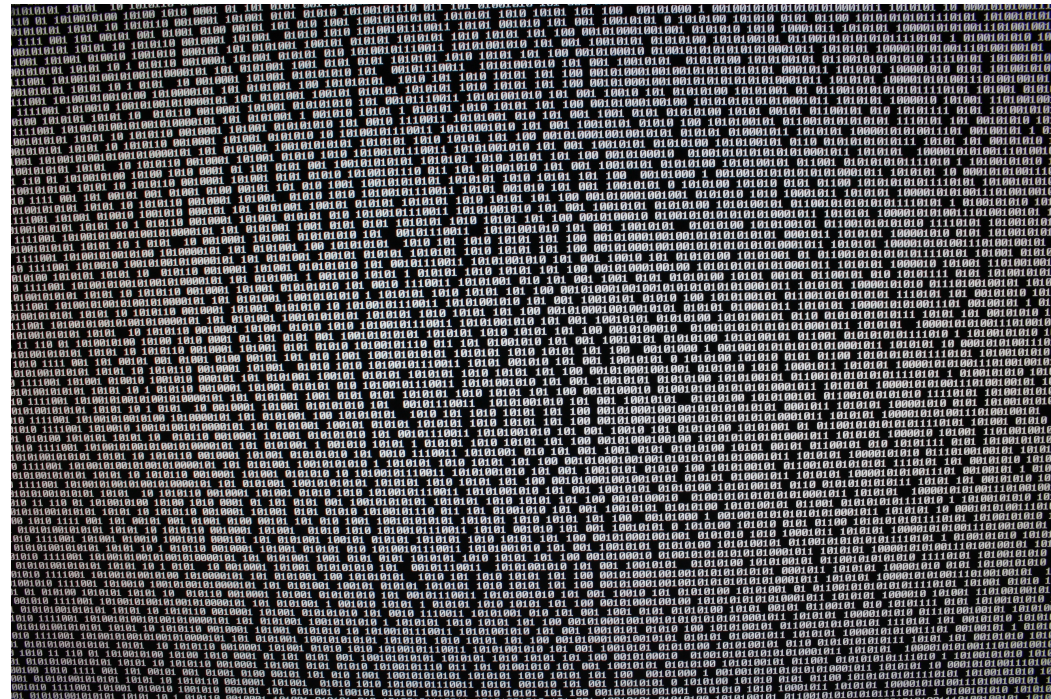
Install
Software



Turn on
Auditing



Collect
500,000
records a day



Case Study: Building Systemized Compliance

Security and Folder Structure Model

- Develop a simplified and standard folder and permissions model
- Automate application of folders and permissions to eliminate human mistakes

User/Group Management

- Develop a group based model aligned with access needs
- Implement tools to allow end user management of users and groups

Workflow

- Control the movement of files through the system based on specific tasks
- Develop task service that will manage file movement through the clinical data flow

Auditing

- Monitor user activities and maintain information about user/file changes and workflow task activities
- Provide simple access to audit records so you can provide traceability of your files and workflow

Conclusion

What you should know...

- Regulations
- Company's data strategy
- Current processes

What you should do...

- Challenge your current processes
- Focus on the tasks (human centered)
- Focus on pragmatic compliance