You Don't Know What you Have Until it's Gone and Then it is Too Late: The Benefits of a Data Management Audit.

CYNERGISTEK

Hunterdon Healthcare
Your full circle of care.
www.hunterdonhealthcare.org

Presented by:

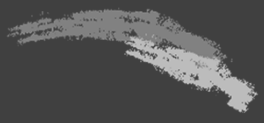
Marti Arvin
VP of Audit Strategy

Don Ahart
Internal Auditor

Agenda

1. What is a data management?
2. Steps to a data management audit
3. Auditing findings & addressing gaps identified
4. Value add in key areas
5. Wrap-up

What is a Data Management?



Data Management

- Processes to
  - Identify your organization's data
  - Where that data lives
  - How the data is stored
  - How the data is used internally and
  - Who data is shared with external to the organization

What Data Does the Organization Have?

- Identifying and categorizing the organization's data is the first step
  - Multiple ways to do this
    - By "protection level" with details within each level
      - https://security.ucop.edu/files/documents/uc-protection-level-classification-guide.pdf
    - By type of data
      - http://www.bu.edu/policies/information-security-home/data-protection-standards/data-classification-policy/

Data Protection Level

- Protection level 1
  - Given a description of the non-sensitive, non-confidential data
- Protection level 2
  - Data that requires some limited degree of protection but not sensitive or confidential information
- Protection level 3
  - Sensitive information but not highly confidential information
- Protection level 4
  - Highly confidential information that requires the highest degree of protection

Type of Data Categories

- Public
- Internal
- Confidential
- Restricted

Where Does the Data Live?

- This is driven by the type of data and the nature of the obligation to protect the data
  - Legal obligations
    - HIPAA
    - FISMA
    - FERPA
  - Other obligation
    - PCI
    - Contractual

How is the Data Stored?

- This ties to the various modalities of storage.
  - Modalities
    - Servers
    - Mobile devices
      - Personal
      - Company owned
    - Cloud
    - Third-party storage

How is the Data Stored?

- It also ties to the way in which it is stored.
  - Encrypted
  - Unencrypted
  - Password protected
    - Individual user account
    - Generic user account

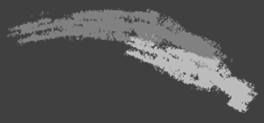
How is the Data Used Internally?

- Who has access?
  - Departmental
  - Central IT
- Who controls who has access?
  - ID management
  - Departmental
- What are the limitations on access?
  - Role based
  - Function based

How is the Data Shared Externally?

- Who has access?
  - Vendors
  - Affiliates
- Who controls who has access?
- How do they get access?
  - VPN
  - File share
  - Cloud file share
- What are the limitations on access?

Steps to a Data Management Audit



Purpose of the Audit

- Data Management vs. Data Governance
  - Data Management is the logistics of the data and Data Governance is the strategy of the data
- This presentation is about data management

Purpose of the Audit

- The purpose of the audit is to determine if an organization maintains data management processes with assigned internal controls that provide reasonable measures in maintaining the integrity, confidentiality, and availability for PHI, PCI, GDPR, and confidential information.

Audit Checklist

- ✓Review policies and procedures
- ✓Review roles and responsibilities
- ✓Review data asset inventories
- ✓Review data access processes
- ✓Review data life cycle processes

Policies and Procedures

- Verify that they are current and accurate and that they are being followed accordingly
- Verify that they contain the roles and responsibilities of the organization's data management program

Roles and Responsibilities

- Data Owners
  - Defined business owner(s) of the data. Normally a business leader(s)
- Data Custodians
  - Responsible for ensuring the integrity, confidentiality, and availability of the data. Normally an Information Technical member(s)

Roles and Responsibilities

- How are the roles assigned?
  - What is the criteria
  - Is it documented and available for the necessary staff
  - Process for data ownership changes
  - Separation of duties (business owner and data custodian)
  - Emergency situations

Roles and Responsibilities

- One owner to multiple systems
- Multiple owners to one system
- Multiple approvals
- Does every system need a dedicated owner
- How often is ownership reviewed

Roles and Responsibilities

- Sample chart
- Concerns and pitfalls

System	Bus. Owner	System Owner	Tech Owner	PHI	PCI	Location	Vendor	Classification
ED EMR System	Bob Smith Betty Vine	Mary Tom May Fog	Jen Dunn Sam Topp	Y	Y	On-prem Server A	Lynx Inc.	Confidential
Donation System	Sue Hill	Van	Al Strong	N	Y	On-prem Server B	Hound Inc.	Confidential
Café Menu	Simon	-	-	N	N	Cloud Vendor A	Fox Inc.	Public
HRIS System	Any HR Director	Mike Allen	Mike Allen	N	N	Cloud Vendor B	Raven Inc.	Internal

Data Asset Inventories

- Data Discovery (light)
  - Sedentary assets (Servers, network devices, copiers, PCs)
  - Mobile assets (Laptops, smartphones)
  - Clouds services and software (SOCs, data analytic systems, storage)
  - File hosting websites (Dropbox, Onedrive)

Data Asset Inventories

- File transfer protocols (FTP, SFTP) and Virtual private networks (VPN)
- Data maps
- Virtualization (multiple systems on the same hardware)
- Classification of data (public, private, confidential, top secret)

Data Asset Inventories

- Review asset documentation
  - Commission and decommission process
  - Physical controls
- Mobile assets
  - MDM controls
  - Review bills

Data Asset Inventories

- File hosting sites
  - Why is this needed
  - What is being shared and is it protected
- File transfer protocols (FTP, SFTP)
  - Review port 22 and port 23 traffic
  - Check what is going out as well as what is coming in

Data Access

- Who can approve/revoke access? Data Owner(s)
- Who can enable/disable access? Data Custodian(s)
- Verify that the approval process is being followed
- Verify the onboarding and off boarding of access

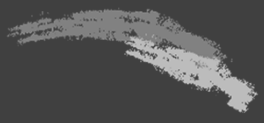
Data Access

- Consider view only, specific times, and temporary access
- Remember your Business Associates and vendors' access
- How often is data access reviewed by the data owners
- Separation of duties

Data Life Cycle

- Basics of data life cycle
  - Create and receive data
  - Process and utilize data
  - Store and transfer data
  - Archive and destroy data

Value Add in Key Areas



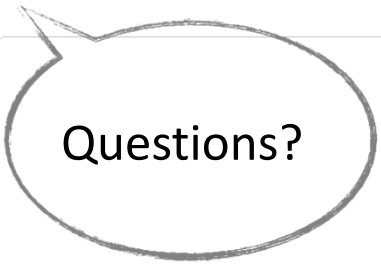
Future Improvements for Audits and Assessments

- Assist with the future Data Governance. With data identified, the organization can make decision on, “What do you want to accomplish with the data.”
- Assist with business continuity and disaster recovery plans as key systems, personal, and assets have been identified.
- Assist with developing a more targeted risk assessments (internal and external).
  - You cannot assess risk on things that you are not aware of

More Improvements…

- Assist with locating data and systems that have standards, regulations, or contractual responsibilities like HIPAA, PCI, and GDPR.
- Assist with incident response as key systems, personal, and assets have been identified.

Thank You!



Don Ahart
Hunterdon Health System
dahart@hhsnj.org
908-237-7059

Marti Arvin
VP Audit Strategy
Marti.arvin@cynergistek.com
512-402-8550 x7051