Good Practices for Archivist and Record Managers

Sylvia Gifty Appiah

MSc Cyber Security and Management

Archiving and Records Management
(Data Protection and Privacy)

What is Archiving

Why Archiving

Where do you start

What data/records do we currently have

Do we need to collect all this data?

Records Management

- Records management is the **systematic control** of an organization's records, throughout **their life cycle**, in order to meet operational business needs, statutory and fiscal requirements, and community expectations.

- Records management refers to a set of activities required for **systematically** controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions.

ISO 15489 – International standard for records management

Archiving

- What is Archiving

- Data archiving is the process of moving data that is **no longer actively** used to a separate storage device for **long-term retention**.
- It consist of older data that is still important to the organization and may be needed for future reference as data that must be retained for **regulatory compliance.**

Where Do We Start?

- Privacy by design (PbD)
- Data protection Principles (8 Principles)

1. Accountability
2. Lawfulness Of Processing
3. Specification Of Purpose
4. Compatibility Of Further Processing With Purpose Of Collection
5. Quality Of Information
6. Openness
7. Data Security Safeguards
8. Data Subject Participation.

Type Of Records Held

- Manual
  - Paper files
  - Original copies of documents
  - Correspondence
  - Invoices/receipts
  - Application forms etc
- Electronic/Digital
  - Videos/images
  - CCTV recordings
  - Online forms
  - Documents/files

Archiving and Retention Policies

Archiving and Retention Policies

- Embed into systems
- Have procedures in place
- Raise awareness

Considerations for Arching and Record Keeping/Retention

- Classification
  - Personal Data
  - Confidential Data
  - Personally Identifiable Information
  - Sensitive Data (special sensitive dataCollection/Volumes

Creating

- Storing
- Destructing (purge)
- Access (FOI/Subject Access Request)

Security

Encryption

- Data at Rest vs Data in Transit
- Access Levels

Capturing and Storage

- Digital
  - Cloud

    Data Centers/Data warehousing
- Manual
  - Electronic Data Records Management Systems (EDRMS)
  - Scanning and indexing (Manual records)

Benefits or Good Archival & Record Management System

- Know what records is held, and locate them easily to support decision making
- Cost reduction- savings in administration costs, both in staff time and storage
- Only actively used data is available for processing
- Speed in retrieval of information
- Regulatory compliance
- Best Practice/Accountability (Principle 1)
- Trust and Reputation

Poor Archival & Record Management System

- Difficult to know what records is held
- Can slow systems down
- Cost of physical storage
- Speed in retrieval of information
- Non compliance

What if You don't Comply

Fines

Negative Media Attention - Loss Of Reputation

Destruction

- NHS (Trust) in the UK was fined £200,000 July 2013
- by data regulators after losing sensitive information about 3,000 patients. The hospital didn't actually 'lose' data in the classic sense of misplacing and never finding it, nor was it a victim of a vicious malware attack.
- They actually failed to check that the data destruction company charged with getting the computers ready for recycling had properly destroyed the records. The data destruction company passed on data, believing that crushing hard drives was enough to permanently erase the NHS computers.


If I'd known they wanted me to use all this info – I would never have asked for it!