3/11/2024

Data retention and data archiving, data destruction/disposal

Big question for data retention: how long do you keep it?
Month? A year? A decade? Forever?

Data archiving is the intentional preservation of data that makes it easy to refer back to.

Differentiate between data archives and data backups
They are not the same
Don't want to configure your archive in such a way that it produces a single point of failure

- Don't make your archive an afterthought
- Regulators may impose severe penalties on loss of archived data

Establish clear policies about what data should be stored and in which tier of storage (security, time of retention, etc.)

Don't treat all data the same
Take steps to automate lifecycle management
Don't underestimate the importance of security – especially in the cloud
Consider the benefits and risks of storage solutions
What purpose does your data retention policy serve?
How long do you need different classes of data?

- What data is for internal use only?
- What uses does the data have (including reuse cases)?
- What regulations apply?

https://www.the-ies.org/sites/default/files/documents/retention_archiving_policy.pdf

https://www.healthit.gov/playbook/pddq-framework/platform-and-standards/historical-data-archiving-and-retention/

https://www.oecd-ilibrary.org/environment/guidance-document-on-good-in-vitro-method-practices-givimp/storage-and-retention-of-records-and-materials_9789264304796-15-en;jsessionid=Qm2SVRUIbY7hEzuI-b9d1QtH.ip-10-240-5-112

data destruction/disposal

why?
Data isn't valuable forever, and there are not unlimited resources to preserve/retain all data collected

Safe data destruction may be the subject of regulations

Methods:

- Overwrite the data – overwriting with new data or assigning random values to the sectors so that the old data can't be retrieved
- Degaussing—erasing magnetic data with a magnet – destroy the medium in the process
- Disposal/destruction of the physical mechanism -- breaking the device so that it can't be physically used

Maintain a log of device that have been destroyed and how (including the methods) and dates

Should have a policy about data disposal (with retention and archiving), and when and how will the data be destroyed

States have different regulations and disposal and in what circumstances
Some companies exist to facilitate compliance

Resources:

1. https://www.the-ies.org/sites/default/files/documents/retention_archiving_policy.pdf
2. https://www.healthit.gov/playbook/pddq-framework/platform-and-standards/historical-data-archiving-and-retention/
3. https://www.oecd-ilibrary.org/environment/guidance-document-on-good-in-vitro-method-practices-givimp/storage-and-retention-of-records-and-materials_9789264304796-15-en;jsessionid=Qm2SVRUIbY7hEzuI-b9d1QtH.ip-10-240-5-112
4. https://www.ironmountain.com/resources/whitepapers/d/6-dos-and-donts-for-data-archiving
5. https://www.techfino.com/blog/data-retention-best-practices
6. https://www.intradyn.com/data-retention-policy/
7. https://www.smartsheet.com/content/data-retention-policies-plans-templates
8. https://www.atlanticdf.com/blog/2019/10/31/safe-data-destruction-101-why-data-disposal-is-necessary/
9. https://www.cisecurity.org/insights
10. https://kirkpatrickprice.com/blog/secure-data-destruction-guide/
11. https://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws

Extended commentary:

Data retention and data archiving are two concepts related to managing data over its lifecycle.

Data retention refers to the process of storing data for a specific period of time as mandated by laws or regulations, or as per the organization's policies. The retention period may vary depending on the type of data, industry, and country. During this period, the data must be stored securely and should not be altered or deleted, as it may be required for legal or audit purposes.

Data archiving, on the other hand, refers to the process of moving inactive data from primary storage to secondary storage to free up space, improve performance, and reduce costs. Archived data is not accessed frequently, but it must be stored for long-term retention as it may be required for future reference or legal reasons. Data archiving can also help in complying with data retention policies.

In general, data archiving is used for managing data that is no longer needed in the short term, while data retention is used for managing data that is still required for legal or regulatory reasons. Data archiving is also used to optimize storage resources and reduce storage costs, while data retention is used to ensure that data is not deleted prematurely.

Effective data retention and data archiving policies and practices require careful planning and implementation to ensure that data is managed efficiently and effectively throughout its lifecycle. Organizations must develop a clear understanding of their data requirements, legal and regulatory obligations, and business needs to establish effective data retention and data archiving policies.

Data destruction or disposal refers to the process of permanently erasing or destroying data that is no longer needed or has reached the end of its lifecycle. Proper data destruction is important to prevent data breaches, protect sensitive information, and comply with data privacy regulations.

There are several methods of data destruction, including:

Physical destruction: This involves physically destroying the storage medium, such as shredding or melting hard drives, flash drives, or optical media.

Degaussing: This is a process of erasing data from magnetic storage media by exposing it to a powerful magnetic field that permanently erases the data.

Overwriting: This involves overwriting the data with random data multiple times to make it unrecoverable. This can be done using specialized software tools.

Cryptographic erasure: This involves encrypting the data before deleting it, making it unreadable and unrecoverable.

It is important to follow proper data destruction procedures to ensure that data is not accidentally or maliciously leaked or accessed after it has been deleted. This can include creating a data destruction policy, ensuring that all data is properly backed up before destruction, and verifying that all data has been successfully deleted or destroyed.

Data archives and data backups are both important aspects of data management, but they serve different purposes.

Data backups are used to create a copy of data at a specific point in time, typically for the purpose of restoring that data in case of data loss or corruption. Backups are typically made on a regular basis, often daily or weekly, and stored separately from the primary data to ensure that a copy is available in case of disaster or failure.

Data archives, on the other hand, are used to preserve data that is no longer actively used but still has long-term value. This could include data that is required for regulatory compliance, historical records, or other information that must be retained for legal or business reasons. Archives are typically created by moving data from primary storage to a separate archive system, often with additional measures such as encryption or access controls to ensure the security and privacy of the archived data.

In summary, while data backups are used to protect against data loss or corruption, data archives are used to preserve data that is no longer actively used but still has long-term value.

A data retention and disposal policy typically includes the following elements:

Purpose and scope: The policy should clearly state the purpose of the policy and the scope of the data it covers.

Roles and responsibilities: The policy should specify who is responsible for implementing and enforcing the policy.

Data retention requirements: The policy should outline how long data should be retained and under what circumstances data can be deleted.

Data disposal methods: The policy should specify how data should be disposed of when it is no longer needed, including any methods for securely erasing data.

Legal and regulatory requirements: The policy should comply with any relevant legal and regulatory requirements, such as data protection laws or industry-specific regulations.

Training and awareness: The policy should include provisions for training employees on how to comply with the policy and raising awareness about the importance of data retention and disposal.

Monitoring and auditing: The policy should establish procedures for monitoring and auditing compliance with the policy, including regular reviews of retention schedules and disposal methods.