Data Loss Prevention in Healthcare
The permanent and official location for Health Information Management Working Group is
https://cloudsecurityalliance.org/research/working-groups/health-information-management/
Acknowledgments

Lead Author
Imran Pirzada

Contributors
Jim Angle
Michael Roza

Reviewers
Satish Govindappa
Sarah Shafqat

CSA Staff
Alex Kaluza

Designer
Claire Lehnert

Special Thanks
Larry Hughes - Editor
# Table of Contents

Acknowledgments ...............................................................................................................................3  
Abstract ...............................................................................................................................................5  
Introduction .........................................................................................................................................5  
  Data loss prevention (DLP) in Healthcare..........................................................................................5  
  DLP Cloud is the predominant means of transferring data.............................................................6  
How DLP Works ...................................................................................................................................6  
DLP Types ............................................................................................................................................7  
DLP EDM/IDM ......................................................................................................................................8  
  False Positives ...............................................................................................................................9  
  Data Classification ........................................................................................................................9  
DLP & Threat Intel ..............................................................................................................................10  
Data Usage by Locale .........................................................................................................................10  
DLP Protect ........................................................................................................................................10  
DLP Best Practices Strengthen Data Security .....................................................................................12  
DLP Policy Rollout Best Practices .......................................................................................................13  
DLP In Real-Time ................................................................................................................................13  
Measuring DLP Maturity .....................................................................................................................14  
Conclusion .........................................................................................................................................16  
References .........................................................................................................................................16
Abstract

The rise of digital services in healthcare has made protecting medical data an ongoing challenge. Healthcare IT leaders need proper security controls and visibility into user behavior to monitor data loss. This requires a person-centric and monitoring of data movement approach to understand the intent and the safeguarding of the data. Connecting users to sensitive medical data and its movement across a secure channel is one piece of the puzzle. Healthcare process automation improves efficiency in hospital or clinical decision making, where there also arises the risks of data loss. The data loss may occur in several forms: (i) information theft, (ii) data leak, (iii) data manipulation, and (iv) unauthorized sharing of data with third parties. Therefore, Data Loss Prevention (DLP) in healthcare is proposed.

Introduction

This paper outlines how DLP (Data Loss Prevention) is utilized in the healthcare industry, especially regarding transferring patient information. DLP, a multifaceted security solution, is being considered by many organizations and medical industries to review data exfiltrations that are hard to detect, considering this data converging into the Cloud makes it even more obscure. Scenarios like ensuring compliance of patient information in all jurisdictions, healthcare data stored offsite not only increases the chance of data compromise, but also the cost of protecting this data from threat actors, considering that this industry is one of the most highly targeted for ransomware attacks. Organizations are finding out that more than protecting the contents alone is needed. Visibility into knowing whom are using and where they are moving must be clear to prevent and mitigate this loss. Therefore using several studies to assess the requirements for this technology is key in helping to bridge the gap between understanding the risk and protecting it.

Data loss prevention (DLP) in Healthcare

Data Loss Prevention refers to measures that prevent the accidental or unauthorized loss or exposure of sensitive information, such as patient records or personal health information (PHI). These measures are especially important in the healthcare industry, where the compromise of PHI can have serious consequences for patients, including identity theft and harm to their medical treatment. It is important for organizations to have a DLP strategy in place to prevent data breaches and ensure the security and integrity of healthcare data.

With cloud computing becoming increasingly popular in recent years, “[o]rganizations today are transferring and sharing data primarily through the cloud—a trend catalyzed by the COVID-19 global pandemic.” Allowing organizations to store and access data remotely introduces new risks to healthcare data, including the possibility of access by unauthorized individuals, or loss due to technical issues, such as unintended deletion of encryption keys.
DLP Cloud is the predominant means of transferring data

How do employees transfer and share data?
(Select all that apply)

<table>
<thead>
<tr>
<th>Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud storage apps (e.g., OneDrive, Box, Dropbox)</td>
<td>46%</td>
</tr>
<tr>
<td>Cloud to cloud</td>
<td>39%</td>
</tr>
<tr>
<td>Email</td>
<td>38%</td>
</tr>
<tr>
<td>Cloud collaboration and messaging apps (e.g., Slack, Teams)</td>
<td>31%</td>
</tr>
<tr>
<td>Endpoint devices</td>
<td>26%</td>
</tr>
<tr>
<td>Web download/ upload</td>
<td>16%</td>
</tr>
<tr>
<td>Private apps</td>
<td>7%</td>
</tr>
</tbody>
</table>

**Figure 1: DLP Cloud is the predominant means of transferring data**

How DLP Works

DLP employs a combination of security measures, including firewalls, endpoint detection and response tools, anti-virus software, artificial intelligence, and machine learning. These measures work together to identify anomalies, prevent data breaches, and provide contextual insights.

DLP delivers benefits depending on the type of solution chosen. Most use the following techniques:

1. **Rule-based matching:** Here, known patterns are used to find data that matches specific rules. For instance, in the United States a Social Security number is nine digits, which when encountered will be flagged for further review and analysis.
2. **Database fingerprinting:** Also known as Exact Data Matching, this technique looks for an exact match of structured data inside the file, e.g., for the precise string “Patient No. 123.”
3. **Exact file matching:** Here, matches are made against cryptographic hashes of file contents, rather than then entire file contents.
4. **Contextual Analysis:** This is used when considering various factors about data transmission, such as the user’s role, physical location, and the application used. This technique reduces false positives and improves accuracy of policy enforcement.
5. **Partial document matching:** This technique looks for files that partially match pre-set patterns, for instance, when different users have filled out multiple versions of a form.
6. **Statistical analysis:** Here, machine learning or other statistical methods are used, such as Bayesian analysis, to trigger violations.
7. **Pre-built categories:** Pre-built categories use rules based on the Healthcare Delivery

Organizations (HDOs) data classification which identifies data based on its sensitivity and security requirements.

8. **User behavior analytics**: This technique flags suspicious end user behavior.

## DLP Types

DLP solutions come in various types, each serving specific purposes within an organization's data security strategy. The three main DLP variations are described below. Due to the complexities of IT environments, many organizations use multiple solutions.

**Network DLP** monitors, detects, and blocks exfiltration when data is in motion, for example, when a malicious insider emails sensitive company information to a bad actor or sends intellectual property to their personal email when leaving the company.

**Endpoint DLP** prevents employees from copying confidential data to removable devices, e.g., USB drives. Another scans data at rest via a local agent, where file and network shares are scanned to capture sensitive data based on endpoint data loss policies that perform local detection.

**Cloud DLP** protects against data exfiltration or accidental file sharing. “Organizations must remain constantly vigilant, preparing for and defending against potential cloud and web attacks. Attackers frequently attempt to target personal or sensitive data that can be used for their financial gain. The result for businesses can be quite extensive, including the loss of intellectual property, reputational damage, legal liability, and regulatory fines. For these reasons, data loss was ranked as the top outcome organizations are concerned about with cloud and web attacks.” In transforming from a perimeter-based network to a user- and application-centric network, on-premise DLP solutions are gradually replacing Cloud-based ones. This allows the inspection of outbound data and eases deciding whether to block the traffic without negatively affecting user experience.

![Figure 2: Types of cloud applications organizations are most concerned about being attacked](pfpt-us-eb-cloud-and-web-attacks.pdf (proofpoint.com) Page 7)
DLP EDM/IDM

Healthcare industries must also incorporate periodical changes to their medical classifications managed and published by the World Health Organization (WHO). Tracking and blocking document transfers containing FDA-recognized drugs, Current Procedural Terminology/International Classification of Diseases (CPT/ICD-10 codes), and medical diagnostics terms require frequent ingestion of medical terms into DLP. These terms can be injected via features such as Exact Data Matching (EDM) and Indexed Document Matching (IDM).

EDM fingerprints structured data, allowing the monitoring of data in row and column (or CSV) format. IDM fingerprints unstructured data by content matching indexed documents and images.

“IT organizations need better visibility into potential risks of data leakage with granular control and actionable outcomes,” said Steve House, VP of product management, at Zscaler. “With the addition of EDM, our customers, in real time, can more precisely identify and protect sensitive information that could potentially leave their network — keeping the good things in, and the bad things out.”

<table>
<thead>
<tr>
<th>PHI Data - Exact Matching</th>
<th>IDM - Indexed Document Matching</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Protects “unstructured” documents - PDF, Word, Powerpoint, etc. by looking for a 10-90% match in text content</td>
</tr>
<tr>
<td>Health Plan Beneficiary Numbers</td>
<td>Can protect images or other files with 100% binary file match</td>
</tr>
<tr>
<td>Addresses</td>
<td>Most common healthcare policies:</td>
</tr>
<tr>
<td>Device Identifiers and Serial Numbers</td>
<td>Billing forms, patient registration forms, other common patient correspondence templates - usually broken down by department or subsidiary</td>
</tr>
<tr>
<td>Dates (death, birth, admission, discharge or elements indicative of age)</td>
<td>Patient data (scans, medical images - usually very tactical and not global)</td>
</tr>
<tr>
<td>Certificate/license numbers</td>
<td>Intellectual Property - designs, procedures, etc.</td>
</tr>
<tr>
<td>Phone and Fax Numbers</td>
<td></td>
</tr>
<tr>
<td>Account Numbers</td>
<td></td>
</tr>
<tr>
<td>Email Addresses</td>
<td></td>
</tr>
<tr>
<td>Vehicle Identifiers</td>
<td></td>
</tr>
<tr>
<td>IP Addresses</td>
<td></td>
</tr>
<tr>
<td>Website URLs</td>
<td></td>
</tr>
<tr>
<td>SSN</td>
<td></td>
</tr>
<tr>
<td>Full face photos</td>
<td></td>
</tr>
<tr>
<td>Medical Record Numbers</td>
<td></td>
</tr>
<tr>
<td>Biometric Identifiers</td>
<td></td>
</tr>
</tbody>
</table>

DLP deployments are universally impacted by false positive incidents, which generally result from stringent policies that require tweaking. When resources allow, it helps greatly to have people train the DLP system by marking incidents as either true or false positives. The use case for these false positives normally fall under blank forms that contain specific keywords within your policy, for example blank patient requisition forms that contain words like “Patient ID”, “DOB”, “SSN”, or actual numerical values that mimic Credit card or Social Security Numbers that DLP flags in result of.

Data classification is critical to data security. It bridges the gap in identifying, tracking, and safeguarding sensitive information, especially in conjunction with DLP solutions. One of the primary success factors of any business is protecting sensitive data to achieve operational excellence. “Many DLP vendors rely on data classification services to enhance their native data security solutions. This is typically offered through either a native product or third-party integration. Data classification standards are foundational to a successful DLP program. These standards define the confidentiality of company data and are the basis on which data risk is measured. Properly labeled and tagged data simplifies the DLP process, as organizations can easily distinguish sensitive data from non-sensitive data (see Improving Unstructured Data Security With Classification), improving DLP performance. As a result, data classification is increasingly becoming an integral component of a DLP program and comes bundled with many DLP products.”

Data Classification

Data classification is critical to data security. It bridges the gap in identifying, tracking, and safeguarding sensitive information, especially in conjunction with DLP solutions. One of the primary success factors of any business is protecting sensitive data to achieve operational excellence. “Many DLP vendors rely on data classification services to enhance their native data security solutions. This is typically offered through either a native product or third-party integration. Data classification standards are foundational to a successful DLP program. These standards define the confidentiality of company data and are the basis on which data risk is measured. Properly labeled and tagged data simplifies the DLP process, as organizations can easily distinguish sensitive data from non-sensitive data (see Improving Unstructured Data Security With Classification), improving DLP performance. As a result, data classification is increasingly becoming an integral component of a DLP program and comes bundled with many DLP products.”

4 https://www.gartner.com/doc/reprints?id=1-2AMORDJ1&ct=220720&st=sb
Classifying in-house data provides greater transparency about its use and movement. DLP has the ability to configure how a file should be transmitted externally, thereby preventing costly data leaks. Once the data owner classifies a file, the data classification solution sets an identifier on the file to tag its disposition, e.g., confidential, internal. The tag can then be added to a DLP policy to either block, encrypt or quarantine the file.

DLP & Threat Intel

This would be a great area to collaborate with your Threat Intel team as their tasks encompass the analysis of user behavior, which can achieve the means of recognizing the movement of data that can eventually be flagged before any exfiltration. DLP policies can be established that list departing or risky users to monitor and alert on an insider threat. Actions such as auditing or blocking their transfer of data externally can be monitored. A file size limit can also trigger an alert if a user exceeds a threshold, or a pattern of file exfiltration by a single user is recognized.

Data Usage by Locale

This opens another challenge that impacts data usage according to location. Several local and international regulations govern location-based data transfer, e.g., CPA GDPR, FDBR. Although next generation DLP solutions might automatically classify and track this data, it will still require us to understand the importance of data protection and compliance for all types of personal data, including that of specific regions based on their policies, since there are hefty ramifications for leakage.

As a reminder, not all data should be shared. However, when data sharing is required, the organization responsible for the data must ensure its security. As with data use, IAM is critical for data security. At a minimum, a Data Loss Prevention (DLP) solution should be employed to monitor the use of data. DLP is used to ensure sensitive data is not lost or misused. DLP software classifies regulated and confidential data and identifies violations of policies defined by organizations or within a predefined policy pack, typically driven by regulatory compliance such as HIPAA, PCI-DSS, or GDPR. In addition, the organization should consider an Information Rights Management (IRM) technology. IRM is a security technology that protects documents that contain sensitive information from unauthorized access.5

DLP Protect

DLP vendors provide solutions ranging from basic content filtering at the network gateway to complex network- and host-based monitoring solutions. Companies must monitor, discover, and implement policies to protect sensitive information resources. Means of exfiltration include, email, web-browsers, cloud file sharing, instant messaging, social media, portable storage devices, and screen captures.

5 https://cloudsecurityalliance.org/artifacts/healthcare-big-data-in-the-cloud/
DLP directly conflicts with encryption strategies or requirements as it inspects plaintext packets and requires data to be unencrypted for inspection. This can actually create a threat point if the DLP is implemented at the wrong layer or if it is configured improperly.

1. **Encrypt data:** Encrypting data makes it unreadable to anyone who does not have the proper decryption key. Encryption can help prevent unauthorized access to sensitive information as there are other techniques that are gaining traction in the cloud for real-time searchable encryption.
   - **Symmetric Encryption** - Uses one key to both encrypt and decrypt.
   - **Data shredding in Cloud** - Makes data unreadable by deleting the encryption keys needed to decrypt the data.
   - **Tokenization, Partial Homomorphic (PHE)** - Sensitive data elements are replaced by surrogate values, or tokens.
   - **Polymorphic Encryption** - Encryption of data in multiple forms that are protected by multiple keys.
   - **Homomorphic Encryption** - where encrypted data can be manipulated and searched without needing to decrypt it.

---

**Figure 3: A systematic review of homomorphic encryption in Healthcare**

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

---

2. Access Controls - Such as user authentication and permissions to prevent unauthorized data access.
3. User Behavior Analytics - Utilizes user behavior analytics to detect unusual or suspicious data access patterns, thereby helping to identify potential insider threats.
4. Conducting Regular Audits - Regular audits can help to identify vulnerabilities and potential areas for data loss.
5. Data Monitoring and Analysis: Implement real-time data monitoring and content analysis to identify and prevent data breaches.
6. Training - Training employees on security best practices can help to prevent accidental data loss. For example, issuing template emails to users informing them of their activity, and quarterly security awareness training that targets repeat offenders with specific messaging about the risks of releasing data externally.
7. Secure Communication Channels - Secure channels, such as encrypted email for messaging systems, or SSL for Web traffic, can help prevent unauthorized interception of sensitive information.
8. Reputable Cloud Provider - Choosing a reputable provider that implements strong security measures.

DLP Best Practices Strengthen Data Security

Best practices in DLP combine technology, process controls, knowledgeable staff, and employee awareness. Below are guidelines for developing an effective DLP program:

1. **Implement a single centralized DLP program** - Implementing a single centralized DLP program ensures consistent data monitoring and provides better visibility into data assets, strengthening data security across the organization.
2. **Evaluate internal resources** - To implement a DLP plan, HDOs need experienced personnel, including DLP risk analysis, data breach response and reporting, data protection laws, and training and awareness.
3. **Conduct an inventory and assessment** - Evaluating data types and value is important in implementing a DLP program. The evaluation involves identifying the data, the compliance (HIPAA, PCI, PII), and business (IP) sensitivity, how the data is processed and protected, how it is transmitted and protected, and where it is stored and protected.
4. **Implement in phases** - DLP is a long-term process. Implementation is best in stages.
5. Create a classification system – HDOs must create a classification framework before creating and implementing DLP policies.
6. **Establish data handling and remediation policies** - After creating the classification framework, create (or update) policies for handling different categories of data.
7. **Educate employees** - Employee awareness and acceptance of security policies and procedures is critical.
DLP Policy Rollout Best Practices

Below are some best practices to help HDOs maximize their DLP investment and ensure the solution aligns with the company’s existing security strategy and existing measures:

1. **Determine the primary objective.**
   For many HDOs, DLP is adopted so that the HDO can meet complex and evolving compliance standards, such as HIPAA. While this is one important feature, a comprehensive solution provides other assistance to the HDO, including data protection, incident prevention, visibility, and incident response capabilities. Flexible solutions allow the HDO to customize for their priorities.

2. **Ensure the DLP aligns with the HDO’s security architecture and strategy.**
   When designing and implementing a DLP solution, HDOs must carefully assess legacy security technology, such as firewalls and monitoring systems, to determine compatibility to ensure a cohesive and integrated security architecture.

3. **Create a regular cadence of security review.**
   HDOs should continuously evaluate the performance of their DLP solution. They often add new features and capabilities which should be evaluated when they reach the market.

4. **Establish change management guidelines.**
   HDOs need an agreed-upon configuration among stakeholders, requiring uniform approval before implementation.

5. **Test.**
   Regular audits and comprehensive testing are critical to ensure that the DLP solution performs as intended, and identifies and addresses any potential vulnerabilities or gaps in measures.

DLP In Real-Time

The below illustrates how data might flow through the DLP solution and handle exceptions.

1. **Real-Time Data Monitoring:** The DLP solution continuously monitors the data in real-time as data flows through the HDO’s networks and systems. For example, it monitors file transfers for sensitive data and blocks the transfer. It can intercept data at different points, such as at network egress points, user endpoints (e.g., laptops, desktops), or cloud applications.

2. **Content Inspection and Analysis:** The DLP solution performs content inspection and analyzes the data passing through it. Upon discovering sensitive data, it the data from passing. It uses various methods such as keyword matching, regular expressions, data fingerprinting, and machine learning algorithms to identify sensitive data based on defined policies and classifications.

3. **Contextual Analysis:** The DLP solution avoids false positives and ensures accurate policy enforcement by considering the context of data transmission or access. If it discovers transmission of sensitive data, the solution blocks it. The solution analyzes factors such as the user’s role, location, device used, destination, and application being used.

4. **Policy Enforcement:** When the DLP solution identifies or potentially identifies policy violations, it enforces them in real time. Policies can trigger various actions depending on
configuration settings, such as blocking the transmission of sensitive data, encrypting the data, alerting the user or administrator, or logging the incident for further analysis.

5. **Incident Response**: The DLP solution triggers an incident response workflow if a policy violation occurs. The response can include notifying security personnel, escalating the issue, and taking necessary steps to mitigate the risk and prevent further data exposure.

6. **Reporting**: The DLP solution can generate detailed reports, including policy compliance reports, incident reports, and trend analysis reports. These reports provide insights into data protection activities, policy violations, and the organization’s overall data security posture.

7. **Continuous Updates and Improvement**: DLP solutions need updated databases and algorithms to stay current with new patterns, emerging threats, and regulatory changes. Regular updates ensure that the solution effectively identifies and protects against evolving risks.

---

## Measuring DLP Maturity

To understand how effective the HDOs’ DLP programs are, they should self-assess maturity. One way to determine maturity is to define categorical pillars and then apply a maturity level. The following is an example of [Critical Elements of Data Loss Prevention Program Maturity from an HCLtech blog](https://www.hcltech.com/blogs/understanding-data-loss-prevention-dlp-program-maturity).

**CE1 – Program Governance** - Program Governance is the series of hierarchies, processes, and policies that provide the enterprise with strategic and tactical decision-making guidance on DLP business uses, implementations, and organizational policies.

**CE2 – Enterprise Coverage** - Enterprise Coverage is the breadth of DLP protections across the enterprise's network, user, and data spaces.

**CE3 – Policy Coverage** - Policy Coverage describes the depth of DLP detection and protections across the entire scope of data types relevant to an enterprise.

**CE4 – Incident Remediation** - Incident Remediation maturity encompasses the processes, personnel, training, and sub-programs that define our organizational response to user, data, and network actions that violate validated DLP protection policies.

**CE5 – Security Awareness** - Security Awareness, as defined for this definite purpose, defines end-user employee awareness of security policies, data security considerations, security organizational awareness of DLP tooling, its necessity, its value, and the security-related internal uses of DLP metrics and tools.

**CE6 – Metrics and Reporting** - Data Loss Prevention programs need to have trackable and reportable success metrics to ensure a data-driven road to provable ROI and demonstrable security improvement.

---

After identifying critical elements, the next step is to apply a maturity rating. The blog’s author uses CMMI (Capability Maturity Model Integration), developed by Carnegie Mellon University and registered with the US Patent and Trademark Office. This model can be modified to meet the needs of the HDO.

The five CMMI maturity levels are:

1. Initial - Processes are seen as unpredictable, poorly controlled, and reactive. Businesses in this stage have an unpredictable environment that leads to increased risks and inefficiency.
2. Managed - Processes are characterized by projects and are frequently reactive.
3. Defined - Processes are well-characterized and well-understood. The organization is more proactive than reactive, and organization-wide standards provide guidance.
4. Quantitatively Managed - Processes are measured and controlled. The organization uses quantitative data to implement predictable processes that meet organizational goals.
5. Optimizing - Processes are stable and flexible. The organizational focus is on continued improvement and responding to changes.

<table>
<thead>
<tr>
<th></th>
<th>Initial</th>
<th>Managed</th>
<th>Defined</th>
<th>Quantitatively Managed</th>
<th>Optimizing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program Governance</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprise Coverage</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Policy Coverage</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Incident Remediation</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Awareness</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Metrics and Reporting</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

The table above shows the HDOs immediately where they are in reference to maturity. Regardless of how you measure maturity, the HDO must incorporate this into its DLP program.
Conclusion

Data protection is crucial to every individual and organization, especially with various communication channels. It is key to establish a firm platform for recognizing your data and the challenges around it. The healthcare industry being one of the targets, especially while digitalization is at the forefront, can either benefit the industry by expanding the treatment roadmap or pose threats if the proper security tool sets and awareness are absent. Monitoring the boundaries of your data and interfacing with the owners continuously will broaden the preventative measures and curtail the attack surface, leading to data loss.

References

Cloud is the predominant means for transferring data -


CPT Codes - CPT Codes | American Medical Association (ama-assn.org)

ICD Codes - ICD - ICD-10 - International Classification of Diseases, Tenth Revision (cdc.gov)

DLP False positives - [New Research] Data Loss Prevention & Data Security Survey Report | The Inner Circle (cloudsecurityalliance.org)

EDM Extension - Zscaler extends cloud DLP service with inline exact data match for massive data sets covering users globally | VanillaPlus - The global voice of Telecoms IT

Data Classification: Market Guide for Data Loss Prevention -
https://www.gartner.com/doc/reprints?id=1-2AMORDJ1&ct=220720&st=sb

Healthcare Big Data in the Cloud | CSA (cloudsecurityalliance.org)

A systematic review of homomorphic encryption and its contributions in healthcare industry - PMC (nih.gov)