How to Implement Data Classification

Data Classification for Small/Medium/Large Healthcare Organizations

HHS 405(d)
Aligning Health Care Industry Security Approaches

What is Data Classification?

Data classification is based on understanding where data resides, where it is accessed, and how it is shared. An organization needs to identify the types of data files and types of records relevant to each category of classification such as sensitive, internal use or, public use, which in turn can help your organization decide how it should be protected.

Why is it important?

There is a vast amount of data in healthcare environments. Data can range from PII to ePHI (i.e., treatment information, SSNs, insurance numbers, billing information) to research information. Data in healthcare environments can also include business sensitive information such as strategies and development plans, financial data, HR information, and corporate board materials. These data elements need to be accurately secured based on the likelihood of a breach causing damage to the organization's reputation.

How will this keep my organization safe?

Electronic Protected Health Information (ePHI) is any information that can be used for identity theft, financial fraud, or damage the patient's reputation. Therefore, having a solid data classification process will ensure your data is protected with the proper security controls and will not jeopardize the safety of your organization and its patients.

Threats Data Classification Mitigates:

- Ransomware attack
- Loss or theft of equipment or data
- Insider, accidental or malicious data loss

Implementation Tips:

Control access to highly sensitive ePHI data. Data access should be controlled to only those users who need it to perform their job or patient treatment as well as requiring proper authentication at login. This data must be managed in compliance with applicable regulatory requirements. Data examples include Social Security Numbers, credit card numbers, behavioral health information, substance abuse information, and other patient treatment information.

Train employees on how to handle information based on its classification. Most healthcare employees work with sensitive data daily, so it is easy to forget how important it is to remain vigilant about data protection. Organizational policies should address all user interactions with data that has been classified as sensitive data and reinforce the consequences of lost or compromised data.

Consider data integrity and availability. When determining data classifications, consider not only confidentiality but data integrity and availability as well. For example, what if you can no longer trust the data is accurate because it has been damaged? What if you can never have access to that data again because you can never retrieve or restore it? It is important to ensure that your organization's data classification policy allows for easy access to information needed for employees to complete their work. This will prevent staff from having access to restricted information.

Ensure data is labeled based on its classification. It is important to label information properly to facilitate restriction implementation related to its usage and disclosure. At a minimum, the labeling process should ensure that labels are readily apparent when users view information. Use techniques like placing the classification in the footer of the document. Collaborate with your marketing and communication departments to create document templates based on data classification levels.

Establish a data classification policy. Ensure that it categorizes data by its criticality and sensitivity. Examples of data classification are Sensitive, Internal Use, or Public Use. An organization needs to identify the types of data files and types of records relevant to each category.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our website at 405d.hhs.gov and our social media pages: **@ask405d** *on Facebook, X, LinkedIn and Instagram!*