Threat: Insider, Accidental or Malicious Data Loss

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Imagine this: An employee is asked to make a copy of a patient's information at a facility. The employee deliberately makes an extra copy to leave the facility and then be sold for financial gain. Patient security has just been compromised and the patient's information is now in dangerous hands.

Data loss can occur a few different ways, including malicious acts. A malicious data loss threat is loss or theft caused by an employee, contractor, other user of the organization's technology infrastructure, network, or databases, with an objective of personal gain, extortion, or inflicting harm to the organization or another individual. An accidental insider threat is not malicious and can be caused by honest mistakes, such as being tricked, procedural errors, or a degree of negligence.

This threat involves people who typically have legitimate access to your computer systems and network. If a user takes advantage of access provided, patient safety can be compromised over short or extended periods of time. This impacts patient's overall quality of care.

What can you do to protect your patients and organization to manage the threat of insider, accidental or malicious data loss?

You can:

Train staff and IT users on data access management procedures to mitigate social engineering or procedural errors.

Implement and use workforce access auditing of health record systems and sensitive data.

Implement and use data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads.

The best way to prevent attacks against insider, accidental, or intentional data loss is to maintain consistent communication with your organization's IT or cybersecurity professionals and implement up-to-date cybersecurity policies.

The Department of Health and Human Services, or HHS for short, and the public-private partnership known as 405(d) are committed to aligning health industry cybersecurity approaches by creating, managing, and leading all industry-led processes to develop consensus-based, industry tested guidelines, practices, and methodologies to strengthen the health sector's cybersecurity posture against cyber threats.

Insider, accidental or malicious data loss is one of the five threats identified in the HHS 405(d) publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), which aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector.

Each individual threat discussed in the HICP publication provides threat specific mitigation practices, such as those provided earlier.

Additionally, the HHS 405(d) Program has more resources like other publications, awareness products, and outreach-focused social media platforms and events to keep your organization cyber safe, which keeps your patients safe.

No matter what role you serve in your organization, the 405(d) website at 405d. hhs.gov has resources to help you protect your organization and its patients from cyber threats.

As healthcare industry professionals, the best way for us to stay vigilant is for everyone, including you, to play a part and remember that Cyber Safety is Patient Safety.

Produced by the U.S. Department of Health and Human Services at Taxpayer expense.