Health Industry Cyber Security Practices:
Managing Threats and Protecting Patients (HICP)

Insider, Accidental or Malicious Data Loss

What is Insider, Accidental or Malicious Data Loss?

Insider threats exist within every organization where employees, contractors, or other users access the organization's technology infrastructure, network, or databases. There are two types of insider threats: accidental and intentional. An accidental insider threat is unintentional loss caused by honest mistakes, like being tricked, procedural errors, or a degree of negligence. For example, accidentally sharing Protected Health Information (PHI) with impermissible parties is an accidental insider threat. An intentional insider threat is malicious loss or theft caused by an employee, contractor, or other user of the organization's technology infrastructure, network, or databases, with an objective of personal gain or inflicting harm to the organization or another individual.

Real-World Scenario:

An employee with access to patient records begins to print multiple copies of patient records, putting a spare copy off to the side. When the employee gathers a considerable amount of spare patient records, that include sensitive information such as PHI, they then take the documents and sell them on the dark web.

Impact

Insider threats involve people who typically have legitimate access to your computer systems and network. Whether through negligence or maliciousness, insiders can compromise your patient and enterprise data over short or extended periods of time. This has serious repercussions for the patients, their security, and overall quality of care delivery.

How Can HICP Help?

The publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector. The material on this flyer is a section of the publication that examines cybersecurity threats and vulnerabilities that affect the healthcare industry.

Staying Resilient to Insider, Accidental or Malicious Data Loss

See something? Say something! Follow your instincts, and always report what does not look or feel right to you. Beware of social engineering techniques. Check to see whether your organization conducts enhanced employee and vendor screening to make sure that those gaining access to company data are who they say they are and they truly require access to the information. Are you limiting access to information to those who require it based on roles and responsibilities?

Always consult your IT security professionals when exposed to a situation of stolen data or employee misconduct. Every situation will vary so your IT security professionals will be able to guide you because a cyber-threat is not limited to hacking.

When to Ask About Insider, Accidental or Malicious Data Loss

Conduct regular security training sessions to further employees' education and awareness. Train and test your staff to make sure they understand the security risks and the consequences of falling victim to insider attack. When employees leave your organization, there should be established procedures, ideally automated, so that they no longer have access to accounts, files, or the facility. By doing so, you can lower the probability of such attacks happening in your organization.

Audit and Monitoring

Regular audits and monitoring on your network and systems can be the difference between stopping a problem or being surprised by one. What are some of the activities you should be looking for on your network and why? Look for things like too many login attempts or access from a different location. The same applies for access patterns in your patient record systems; don't forget to watch those too. If an insider's credentials are compromised or the insider is abusing their access, you should have a way to monitor and catch these anomalies before it becomes a problem.

How Can You Mitigate Insider, Accidental or Malicious Data Loss ?

Each individual threat discussed in the HICP publication provides threat specific mitigation practices. The table below lists the insider mitigations along with a quick reference key to help locate further information in the HICP documents. The mitigation practices are covered in greater detail in the technical volumes included in the publication: Technical Volume 1 for Small Organizations and Volume 2 for medium and large organizations.

Insider, Accidental or Malicious Data Loss Mitigation Practices to Consider
Train staff and IT users on data access and financial control procedures to mitigate social engineering or procedural errors **(1.S.B, 1.M.D)**
Implement and use workforce access auditing of health record systems and sensitive data **(3.M.B)**
Implement and use privileged access management tools to report access to critical technology infrastructure and systems **(3.M.C)**
Implement and use data loss prevention tools to detect and block leakage of PHI and PII via e-mail and web uploads **(4.M.E, 4.L.A)**

Key: 1-10 = Cybersecurity Practice | S = Small (Tech Vol 1) | M = Medium (Tech Vol 2) | L = Large (Tech Vol 2) | A-Z= Respective Sub-Practice

Example: "1.S.B Education": "1" refers to the cybersecurity Practice "Email Protection System" | "S" refers to Small size organization | "B" refers to the sub practice for small size organization within the Email Protection System – Cybersecurity Practice, which in this case is "Education"

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 at hhs.405d.gov or email us at CISA405d@hhs.gov. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram!