Transcript: Loss or Theft of Equipment or Data

HHS 405(d)
Aligning Health Care
Industry Security Approaches

Imagine this: A physician stops at a coffee shop for a midday refresher and to use the public Wi-Fi using a secure Virtual Private Network, also known as VPN, to review radiology reports.

As the physician leaves the table momentarily to pick up their coffee, a thief steals the laptop. The doctor returns to the table to find the laptop is gone along with all the patient data and system access information stored within it.

Loss and theft of equipment and data is an ever-present and ongoing threat for all organizations.

Every day, devices such as laptops, tablets, smartphones, and USB thumb drives are lost or stolen, which end up in the hands of threat actors.

However, it's important to remember that equipment loss is far less risky than the loss of sensitive data on that equipment.

In cases where the lost device was not appropriately safeguarded by strong passwords and multi-factor authentication (MFA), the loss may result in unauthorized or illegal access, dissemination, and use of sensitive data.

Even if the device is recovered, the data may have been erased and completely lost. Loss or malicious use of data may result in business disruption and compromised patient safety, and may require notification to patients, applicable regulatory agencies, and/or the media.

This is why physical security of our cell phones, computers, tablets, and other devices is such an important part of cybersecurity.

So, how can you be proactive in preventing and responding to lost or stolen equipment or data?

You can:

Make sure you know your organization's policy on removing equipment from the workplace;

Encrypt sensitive data, especially when you store it and transmit it;

Maintain a complete, accurate, and current asset inventory of mobile devices;

Require MFA to log into devices;

And establish data backup processes with regular testing.

Don't be afraid to report a lost device; far more damage can be done by not reporting the loss.

The best way to prevent loss or theft of data and equipment 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.

Loss or left of equipment or data 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.