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

Loss or Theft of Equipment or Data

What is Loss or Theft of Equipment or Data?

Every day, mobile devices such as laptops, tablets, smartphones, and Universal Serial Bus (USB)/thumb drives are lost or stolen, and they end up in the hands of hackers. Theft of equipment and data is an ever-present and ongoing threat for all organizations. In 2021, 713 major health data breaches (affecting more than 45.7 million individuals) were reported to the HHS OCR. Although the value of the device represents one loss, the consequences of losing a device that contains sensitive data are far greater. In cases where the lost device was not appropriately safeguarded or password protected, 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.

Real-World Scenario:

A physician stops at a coffee shop for a coffee and to use the public Wi-Fi with a secure Virtual Private Network (VPN) to review radiology reports. As the physician leaves the table momentarily to pick up his coffee, a thief steals the laptop. The doctor returns to the table to find the laptop is gone.

Impact

Loss of sensitive data due and impact to patient records was up in 18% in from 2021-2022, when a total of 50,406,838 patient records were compromised[1]. This has serious repercussions for the patients health and security, as well as the reputation of the physician and organization.

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 Loss or Theft of Equipment or Data

Heading out on a business trip or a personal holiday? You need to follow the same, and maybe greater, security procedures as you do in the office. Make sure you know your organization's policy on removing equipment from the workplace by asking:

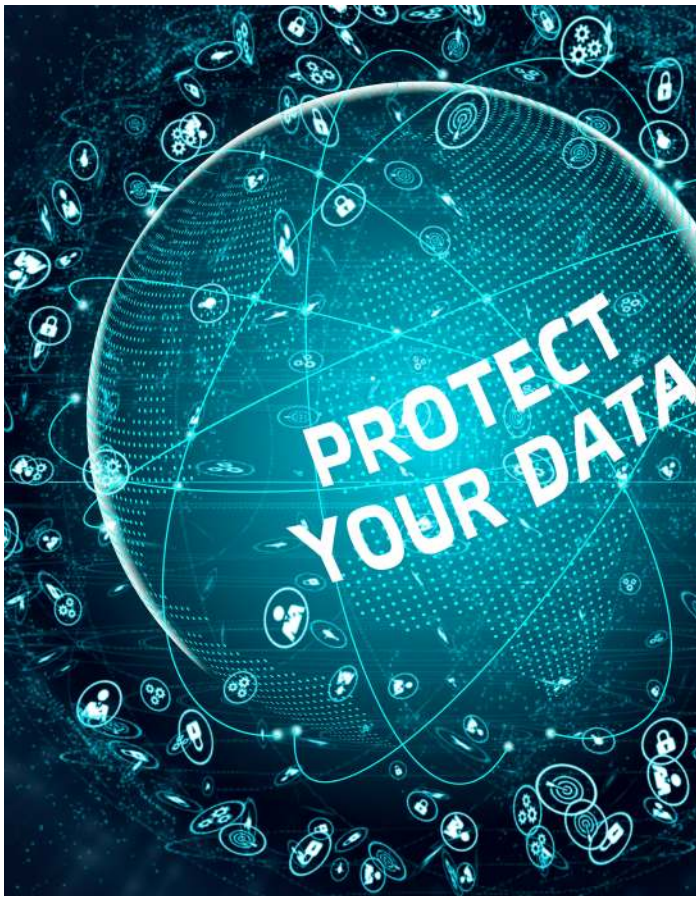
- Can I travel with my equipment?
- Can I take my equipment offsite to work remotely?
- Are USB or other portable storage devices allowed?
- Is the information on the computer or storage device encrypted?
- Is there a secure VPN that I can use, along with secure, password-protected Wi-Fi, to log into the network and work?

1 2022 Breach Barometer Protenus

When To Ask About Loss or Theft of Equipment or Data

As soon as you realize that your device or equipment has been stolen or misplaced, your supervisor and IT security professional should be notified immediately so appropriate measures can be taken to safeguard the data saved on your device or equipment.

Your IT security support staff or similar point of contact should be notified when a work device or equipment has been misplaced, lost, or stolen. The data saved on them are now compromised and susceptible to unauthorized access, dissemination, and use. This is a serious cyber breach and should be handled by trained IT security professionals.



How Can You Mitigate Loss or Theft of Equipment or Data?

Each individual threat discussed in the HICP publication provides threat specific mitigation practices. The table below lists the loss or theft 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 all others.

Loss or Theft of Equipment or Data Mitigation Practices to Consider
Encrypt sensitive data, especially when you store it and transmit it **(4.S.B, 4.M.C)**
Establish data backup processes with regular testing **(4.M.D)**
Acquire and use data loss prevention tools **(4.M.E, 4.L.A)**
Promptly terminate access when an employee or affiliate no longer requires it **(3.S.A)**
Maintain a complete, accurate, and current asset inventory to mitigate threats, especially the loss and theft of mobile devices such as laptops and USB/thumb drives **(5.S.A)**
Encrypt data at rest on mobile devices to be inaccessible to anyone who finds the device **(4.M.C)**
Process and identify clear accountabilities to clean sensitive data from every device before it is retired, refurbished, or resold **(5.S.C, 5.M.D)**

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!