LAPTOP SECURITY

Laptop computer theft continues to be a significant risk exposure for healthcare organizations and represents more than just a property loss. Not only do you lose expensive technology, but you face a serious potential for lost data, including confidential patient information. The theft of a $1,500 laptop can translate into millions of dollars in liability, fines, and data breach notification costs.

In 2023, nearly 900,000 laptops and other portable devices were reported lost or stolen globally, with a large portion containing sensitive or regulated data (Verizon, 2024). A 2024 study revealed that laptops are involved in nearly 15% of all reported healthcare data breaches, often due to physical theft or unsecured remote access points (IBM Security, 2024).

For example, in 2022, a laptop containing the personal data of more than 125,000 patients was stolen from an employee's car outside a healthcare clinic in Chicago. The device was not encrypted, and the healthcare provider was required to notify all affected individuals and offer credit monitoring services, costing the organization over $2.5 million in response and legal expenses (HIPAA Journal, 2023).

Laptops and tablets are widely used in the hospice, home health, and telehealth sectors. While these tools improve information access and workflow efficiency, they also introduce security vulnerabilities. Their ubiquity has led some users to treat them casually, increasing the risk of negligent handling. Nearly every week, a healthcare-related laptop theft makes headlines. Our goal as healthcare providers should be to ensure our employees protect their assigned laptops—and the confidential information they contain—from theft or compromise.

Tips for Preventing Laptop Theft

- Store shipments of new or unassigned laptops and computers in locked closets or rooms with controlled access. Keep a full inventory from delivery onward, and conduct regular and random inventory checks.
- Engrave the company name or asset ID on all laptops. Record each laptop's serial number and store it securely. Some manufacturers and law enforcement agencies offer registry programs.
- Provide employees with inconspicuous, padded carrying cases. Flashy laptop bags attract attention and increase the risk of theft.
- Protect stored information with strong document passwords. Passwords should be at least 12 characters and include a mix of letters, numbers, and symbols. Consider passphrases for improved usability and security.
- Use advanced security features such as full-disk encryption and biometric authentication (e.g., fingerprint or facial recognition).
- If leaving a laptop in the office, lock it in a secure drawer or use a cable lock. Never leave it exposed.
- Do not leave laptops visible in vehicles. Store them in the trunk or out of sight if necessary.
- Ensure all important data on laptops is regularly backed up to secure, centralized storage.
- At meetings or conferences, keep laptops in sight at all times. Do not leave them unattended in public area
- Develop written policies outlining employee responsibilities for laptop security. Require signed acknowledgments of understanding and compliance.
- Maintain an up-to-date list of all laptops, assigned users, serial numbers, and software. Audit this list at least annually.
- Investigate all incidents of loss or damage. Report laptop thefts to law enforcement and publicize incidents as required by law and regulation.

Summary

It is important that healthcare providers make a concerted effort to educate employees about computer and device security in order to reduce financial losses and reputational damage. This information should be shared during new employee onboarding and reinforced through annual cybersecurity training and regular reminders. Creating a culture of security awareness can significantly reduce the risk of laptop-related data breaches (U.S. Department of Health and Human Services, 2024).

REFRENCES

HIPAA Journal. (2023, May 18). Unencrypted laptop stolen from parked car – 125,000 patients impacted. https://www.hipaajournal.com [hipaajournal.com]

IBM Security. (2024). Cost of a Data Breach Report 2024. https://www.ibm.com/reports/data-breach [ibm.com]

U.S. Department of Health and Human Services. (2024). Cybersecurity best practices for portable devices. https://www.hhs.gov [hhs.gov]

Verizon. (2024). 2024 Data Breach Investigations Report (DBIR). https://www.verizon.com/business/resources/reports/dbir/ [verizon.com]