CYBERSECURITY - DATA BREACH PRECAUTIONS FOR HEALTHCARE ORGANIZATIONS

In 2024, the healthcare sector experienced a significant surge in data breaches, with over 276 million individuals affected—a record-breaking figure . The healthcare industry accounted for a substantial portion of these breaches, highlighting its vulnerability to cyber threats .

Healthcare organizations handle a significant amount of personal information related to residents

and patients, as well as their own employees. Electronic files such as health information, billing information, Social Security numbers, and human resource records contain confidential information that must be secured. Electronic exposures that present a potential for loss, injury, or other damages are known as cyber risks and can significantly impact a healthcare organization and the customers they serve.

Activities that create cyber risk include:

- Patient care reports
- Credit card data collection and online payment processing
- Data storage(online and traditional shipping of paper records or back-up tapes)
- Housing private customer data on laptops
- Business partners and contractors that touch customer data (3rd party billing)
- Providing online content or media
- Cloud and outsourced computing
- Social media sites (Facebook, LinkedIn, Instagram, Twitter) that collect and display private information
- Human Resources activities

Causes of data breaches identified in 2024 include:

- 52% of data breaches were due to malicious attacks
- 26% of data breaches were due to human error
- 22% of data breaches were due to IT failures

Not all data breaches result in identities being exposed; however, the cause of the breach does impact the likelihood of this occurring. In 2024, breaches involving stolen or compromised credentials were among the most damaging, often leading to the exposure of sensitive personal information .

What are attackers looking for?

According to research, the more details someone has about an individual, the easier it is to commit identity fraud. Criminals are targeting insurance, government, and healthcare organizations to obtain complete profiles of individuals .

The following is a ranked list of the information pursued among data breaches occurring in 2024:

- Real names were the most commonly sought-after piece of information
- Home addresses, birth dates, government IDs (such as SSNs), medical records, and financial information

- Email addresses, phone numbers, insurance information, and usernames/passwords
- Credit card data remains a target, but its black market value has decreased since credit card companies and cardholders are quick to notice anomalous spending patterns, and stolen card data has a limited shelf life .

Cybersecurity Tips

There are several important steps that a public entity may take to help protect public and personal information

Here are 10 tips to help safeguard sensitive data:

Keep Only What You Need.

Reduce the volume of information you collect and retain to only what is necessary. Minimize the places you store personal data. Know what you keep and where you keep it.

Safeguard Data.

Lock physical records in a secure location and restrict access to employees who need to retrieve private data. Consider employee background checks. It may be beneficial for vendors/contractors (who handle your systems or data) to undergo due diligence regarding their own information security practices and to provide an insurance certificate that includes cyber liability coverage. Include language in service contracts for defense and indemnity in the event of a mishap that impacts your data. Specify that the contractor will notify you of any breach in a timely manner.

Destroy Before Disposal.

Cross-cut shred paper files before disposing of private information. Also, destroy CDs, DVDs, and other portable media. Deleting files or reformatting hard drives does not always erase data. Instead, use software designed to permanently wipe the drive or physically destroy the drive.

Update Procedures.

Using Social Security numbers as employee IDs or client account numbers is not recommended. If you currently do so, consider an alternative ID system.

Train Employees.

Establish a written policy about privacy and data security and communicate it to all employees. Educate them about what information is sensitive and their responsibilities to protect that data.

Control Use of Computers.

Restrict employee use of computers to business purposes. Consider blocking access to file-sharing peer-to-peer websites, inappropriate websites, and unapproved software.

Secure All Computers.

Implement password protection with a condition to re-logon after a period of inactivity. Train employees to never leave laptops or PDAs unattended. Restrict teleworking to company-owned computers with non-generic passwords that are changed regularly and not shared by systems administrators.

Keep Security Software Up-To-Date.

Keep security patches for your computers up to date and apply default settings on new servers. Firewalls and antivirus software are beneficial.

Encrypt Data Transmission.

Data encryption may be an option to consider. Try to avoid using Wi-Fi networks as they may permit interception of data.

Manage Use of Portable Media.

Portable media such as DVDs, CDs, and USB flash drives are susceptible to loss or theft. Encrypting laptops if sensitive data is housed on the device is also an option.

Conclusion

If a data breach occurs, it is important that the healthcare organization quickly reduces the potential damage and limits the flow and distribution of data. React immediately and carefully follow the breach incident response plan to determine the nature of the problem. Engaging outside forensic computer investigators and a privacy lawyer (also known as a Breach Coach) could be beneficial to the organization. Some forensic service vendors can also assist with data recovery and restoration.

REFRENCES

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

Identity Theft Resource Center. (2025, January 28). 2024 Annual Data Breach Report. https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/ [idtheftcenter.org]

HIPAA Journal. (2025, May 26). Healthcare Data Breach Statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/ [hipaajournal.com]

Varonis. (2024). 38 Must-Know Healthcare Cybersecurity Stats. https://www.varonis.com/blog/healthcare-cybersecurity-statistics [varonis.com]

Secureframe. (2025). 110+ of the Latest Data Breach Statistics [Updated 2025]. https://secureframe.com/blog/data-breach-statistics [secureframe.com]

UpGuard. (2025). 14 Biggest Healthcare Data Breaches [Updated 2025]. https://www.upguard.com/blog/biggest-data-breaches-in-healthcare [upguard.com]