Healthcare Data Breaches of 2022:

Types, Causes, and Prevention

Jenna Cousino, University of Toledo, jenna.cousino@rockets.utoledo.edu

THE UNIVERSITY OF TOLEDO

Definitions

- The US Dept. of HHS defines a data breach as, "the illegal use or disclosure of confidential health information that compromises the privacy and security of it under the privacy rule that poses a sufficient risk of financial, reputational, or other type of harm to the affected person."
- HIPAA defines a data breach as, "the procurement, access, use or expose of confidential health information illegitimately, which compromises the privacy and security of that confidential health information."

Data Breach Types

- *Internal* – incidents that occur with the help of an internal agent. Examples include: privilege abuse, inauthentic access/disclosure, improper disposal, loss or theft.
- *External* – incidents cause by any external entity or source. Examples include: malware and ransomware attacks, phishing, spyware, or fraud in the form of stolen cards.

Methodologies

- Figure 1 shows the number of healthcare data breaches from 2009-2022 of 500 or more records. The year 2022 ranks as the second worst year ever in terms of the number of reported breaches.
- Figure 2 shows the number of data breaches at HIPPA-regulated entities from 2009-2022. In 2022, the highest number of data breaches involved business associates (BA).
- Figure 3 shows the number of breaches in 2022 by classification: improper disposal, loss/theft, unauthorized access/disclosure, and hacking/IT incident. Hacking incidents accounted for 555 of the 707 reported breaches (71.4%).
- Figure 4 shows the number of data breaches in 2022 by the location of the breached protected health information.

Figure 1

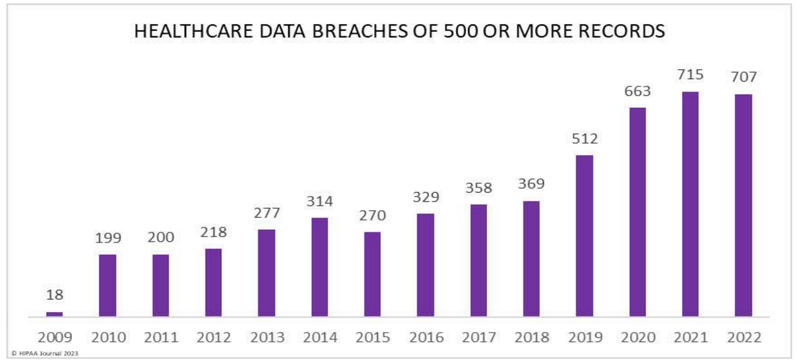


Figure 2

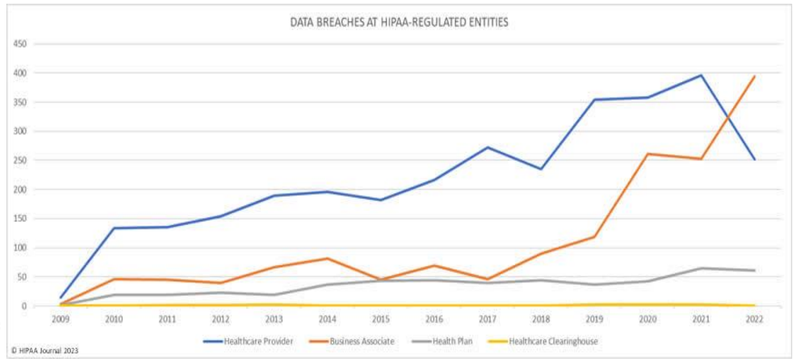


Figure 3

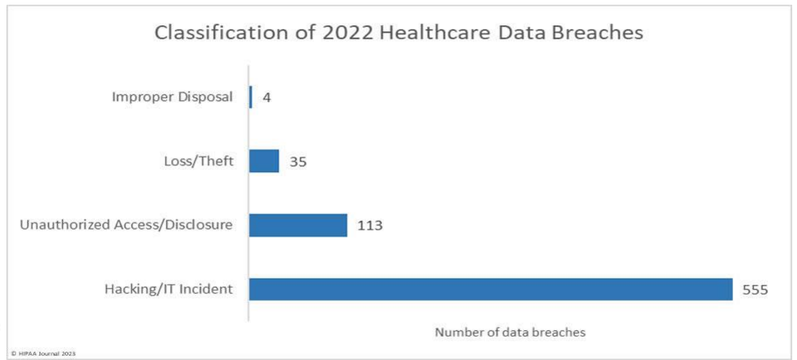
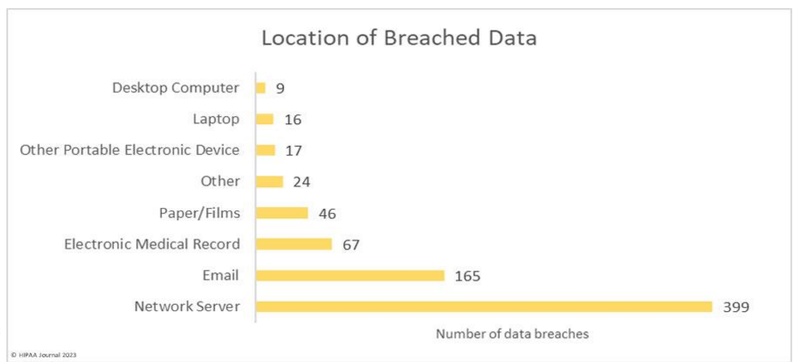


Figure 4



HIPAA Journal, 2023[3]

Prevention

The ONC suggests a seven-step approach to privacy and security of electronic health information:

1. Lead Your Culture, Select Your Team, and Learn
2. Document Your Process, Findings, and Actions
   - Documentation shows how you did the security risk analysis and implemented safeguards to address risk
3. Review Existing Security of ePHI (Perform Security Risk Analysis)
   - Assesses potential threats and vulnerabilities to the confidentiality, integrity, and availability of ePHI
4. Develop an Action Plan
   - Components of action plan: administrative safeguards, physical safeguards, technical safeguards, organizational safeguards, and policies and procedures
5. Manage and Mitigate Risks
   - Implement your Action Plan
   - Prevent Breaches by Educating and Training
   - Communicate with Patients
   - Update your BA Contracts
6. Attest for Meaning Use Security-Related Objective
   - Legal statement that you have met specific standards, including that you protect electronic health information
7. Monitor, Audit, and Update Security on Ongoing Basis
   - Your control audits and capabilities should be scaled to your organization's size

References

1. Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Khan, R. A. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2), 133: 2-18. https://doi.org/10.3390/healthcare8020133
2. The Office of the National Coordinator of Health Information Technology. (2015). Guide to Privacy and Security of Electronic Health Information. *HealthIT.gov.* Version 2.0: 1-62. https://bit.ly/healthitgov
3. Alder, S. (2023). 2022 Healthcare Data Breach Report. *HIPAA Journal*. https://bit.ly/3Ime2qV