Cybersecurity in Healthcare

Protecting Patients in the Digital Age

Celeste Meraz-Luna

CYSE 201S

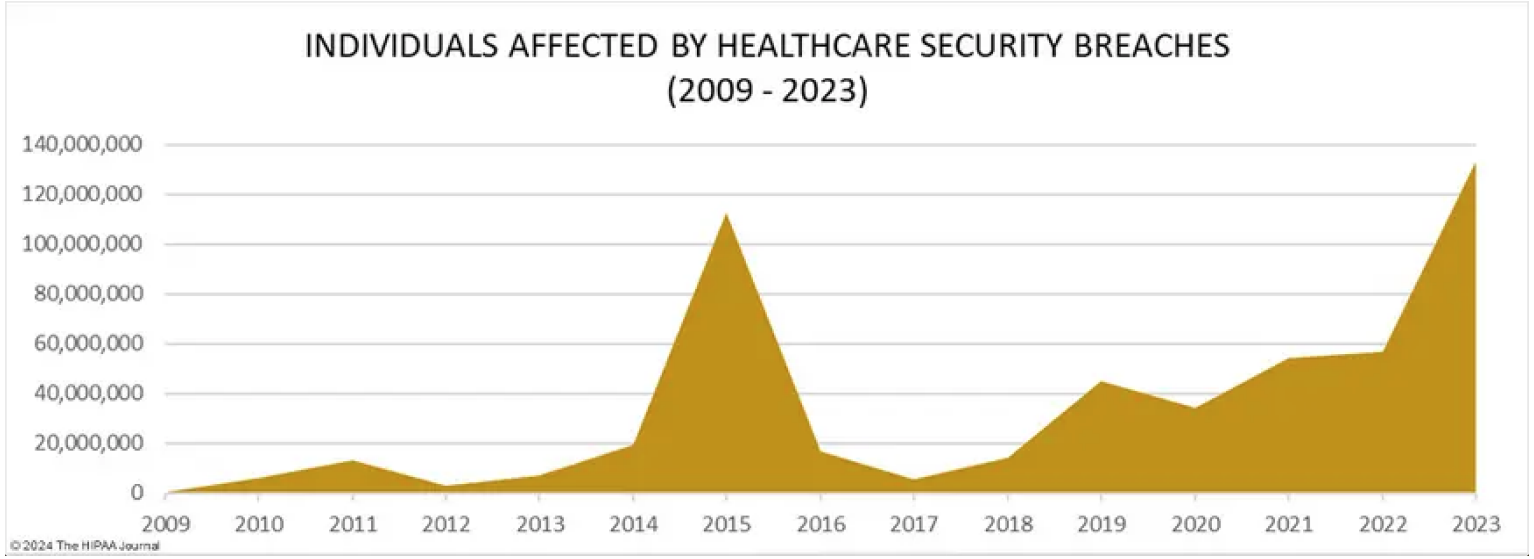
April 18, 2025

Introduction

- Cybersecurity is critical in healthcare, where breaches can disrupt patient care and compromise sensitive data.
- We will explore the intersection of cybersecurity and social sciences, focusing on data protection, ethics, and the broader public health impact.

Cyber Threat Landscape in Healthcare

- Common threats: ransomware, phishing and breaches.
- Example: 2017 WannaCry attack on the NHS (UK National Health Services.
- Healthcare's vulnerabilities: outdated systems and high-value data.
- Sources: Wired (2025), Reuters 2025), AP News (2024)



Social Science Lens

- Privacy and trust are foundational ethical concerns.
  - Patient data includes deeply sensitive information.
- Human behavior: untrained staff and insider threats.
  - One of the greatest vulnerabilities in healthcare cybersecurity stems from human error.
- Disproportionate impact on vulnerable populations.
  - Cyberattacks tend to harm marginalized groups more severely.
- Source: NIH (2021), Synoptek

Policy & Legal Frameworks

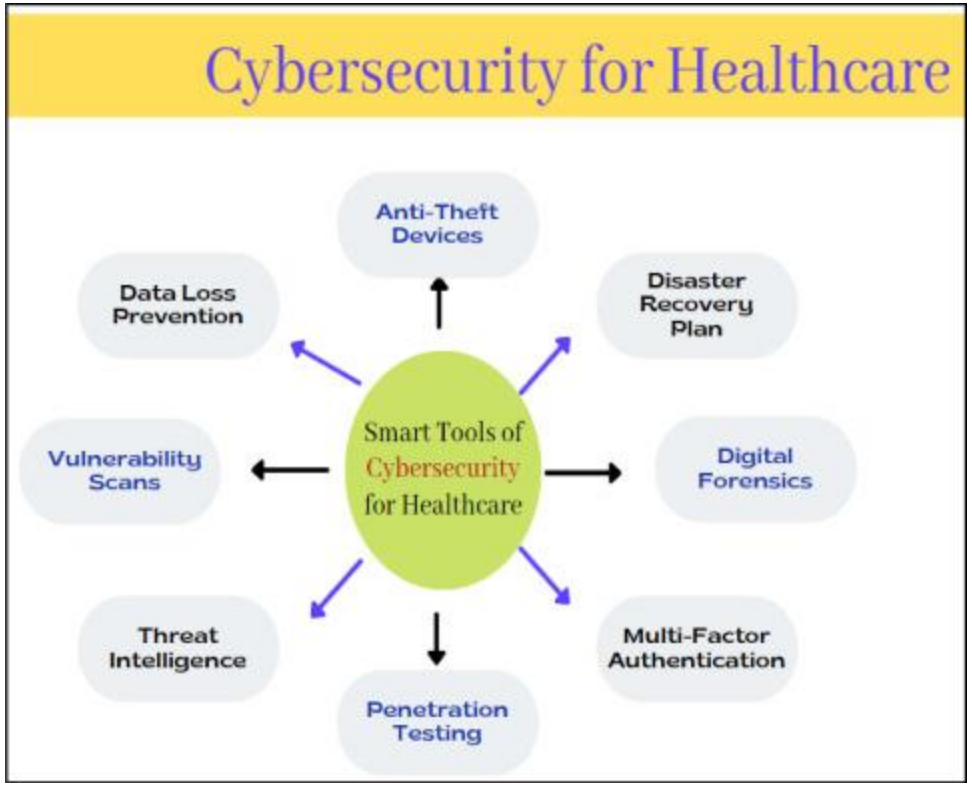
- HIPPA (U.S), GDPR (EU): aim protect patient data.
  - Privacy laws that enforce strict standards on how healthcare organizations collect, store, and share patient data.
- Public policy's role in regulating security behaviors.
  - Governments play a crucial role in setting cybersecurity standards through legislation and oversight.
- Compliance challenges in underfunded environments.
  - Smaller clinics, rural hospitals struggle to meet requirements and lack IT staff.
- Source: Reuters (2024), USF Health

Case Study: DaVita Ransomware Attack

- April 2025: DaVita faced ransomware attack impacting 3,000+ clinics.
- Resulted in disrupted dialysis treatment.
- Highlights how cyber incidents affect public health.
- Source: Reuters (2025)

Solutions and Recommendations

- Technical: encryption, access control, and segmented networks.
- Social: training, ethical design, and community education.
- Policy: funding, standardized reporting, and government oversight.
- Sources: AHA, Synoptek



Maqsood, Humza, et al. "Towards Insighting Cybersecurity for Healthcare Domains." Health Data Science, vol. 2023, 2023, p. 100004, https://doi.org/10.1016/j.hds.2023.100004.

Conclusion

- Cybersecurity in healthcare is a shared responsibility across technology, ethics, and public policy.
- Protecting data is protecting lives- investing in resilient systems and informed people ensures safer, more equitable care.

References

Synoptek. Cybersecurity in Healthcare: How to Protect Patient Data.

Reuters (2024, 2025). DaVita ransomware attack highlights healthcare vulnerabilities.

American Hospital Association (AHA). Cybersecurity resources for health systems.

USF Health. How HIPAA and other policies protect patient information

National Institutes of Health (NIH) (2021). Health Data Privacy and Public Trust in the Digital Era.

Wired (2025). Cyberattacks on the healthcare system: Why hospitals are prime targets