Cybersecurity in Healthcare

Protecting Patient Data and Public Health in the Digital Age

Old Dominion University – School of Cybersecurity

Jacob Asare: Cybersecurity Undergraduate

CYSE 201S

Professor: Diwakar Yalpi

December 1st, 2025

Introduction

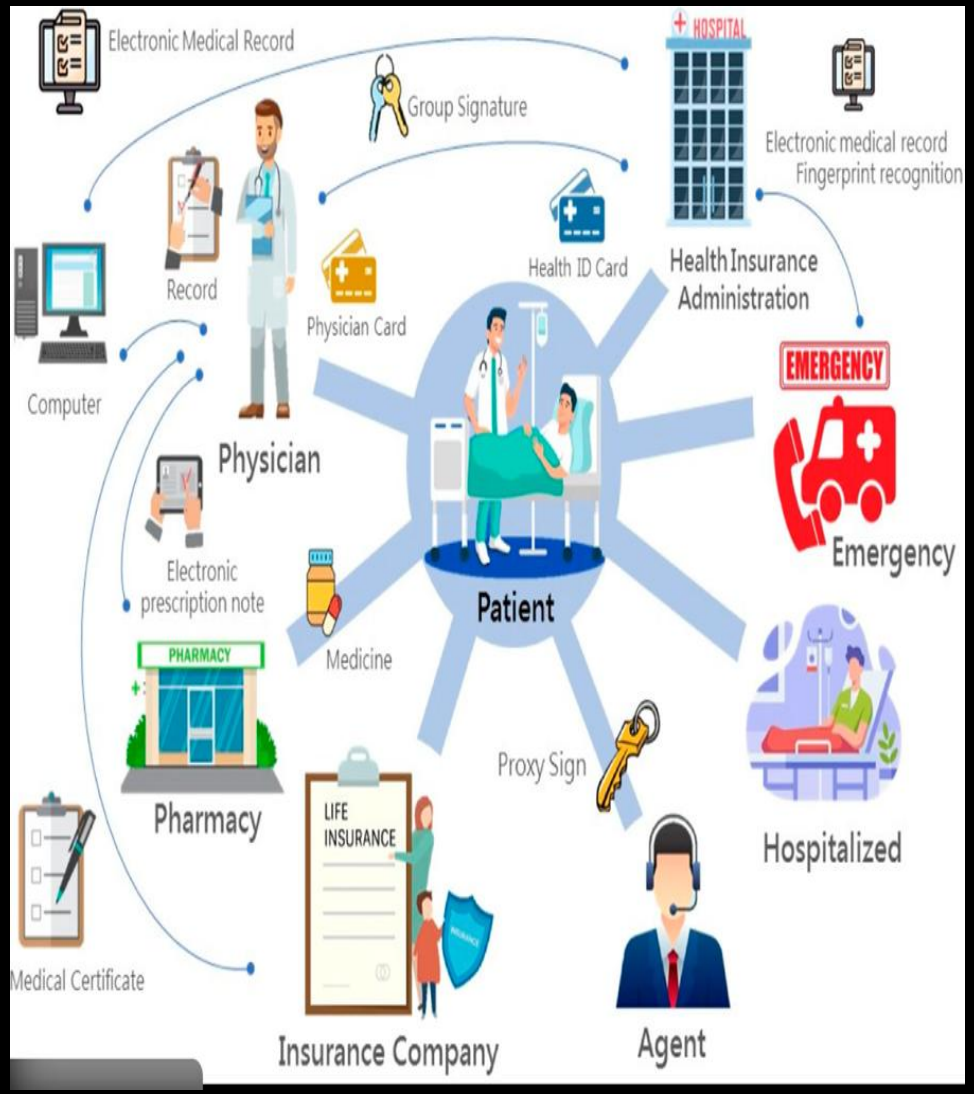
The Digital Healthcare Landscape

- Electronic healthcare technology has transformed care delivery worldwide,
  - creating unprecedented opportunities to improve clinical outcomes.
  - However, this digital transformation has introduced significant cybersecurity vulnerabilities that threaten patient safety and privacy.

Healthcare is an attractive target for cybercrime due to;

- Rich source of valuable data
- Weak cybersecurity defenses
  - (Coventry & Branley, 2018)

Cybersecurity in Healthcare Industry Concept



https://www.mdpi.com/1424-8220/21/3/713

The Growing Threat Landscape

- Cyberattacks on healthcare organizations have increased dramatically in recent years,
  - exposing critical vulnerabilities in systems designed to protect sensitive patient information.

Traditional Attacks

- Targeting IT infrastructure vulnerabilities

Social Engineering

- Exploiting human vulnerabilities

Ransomware

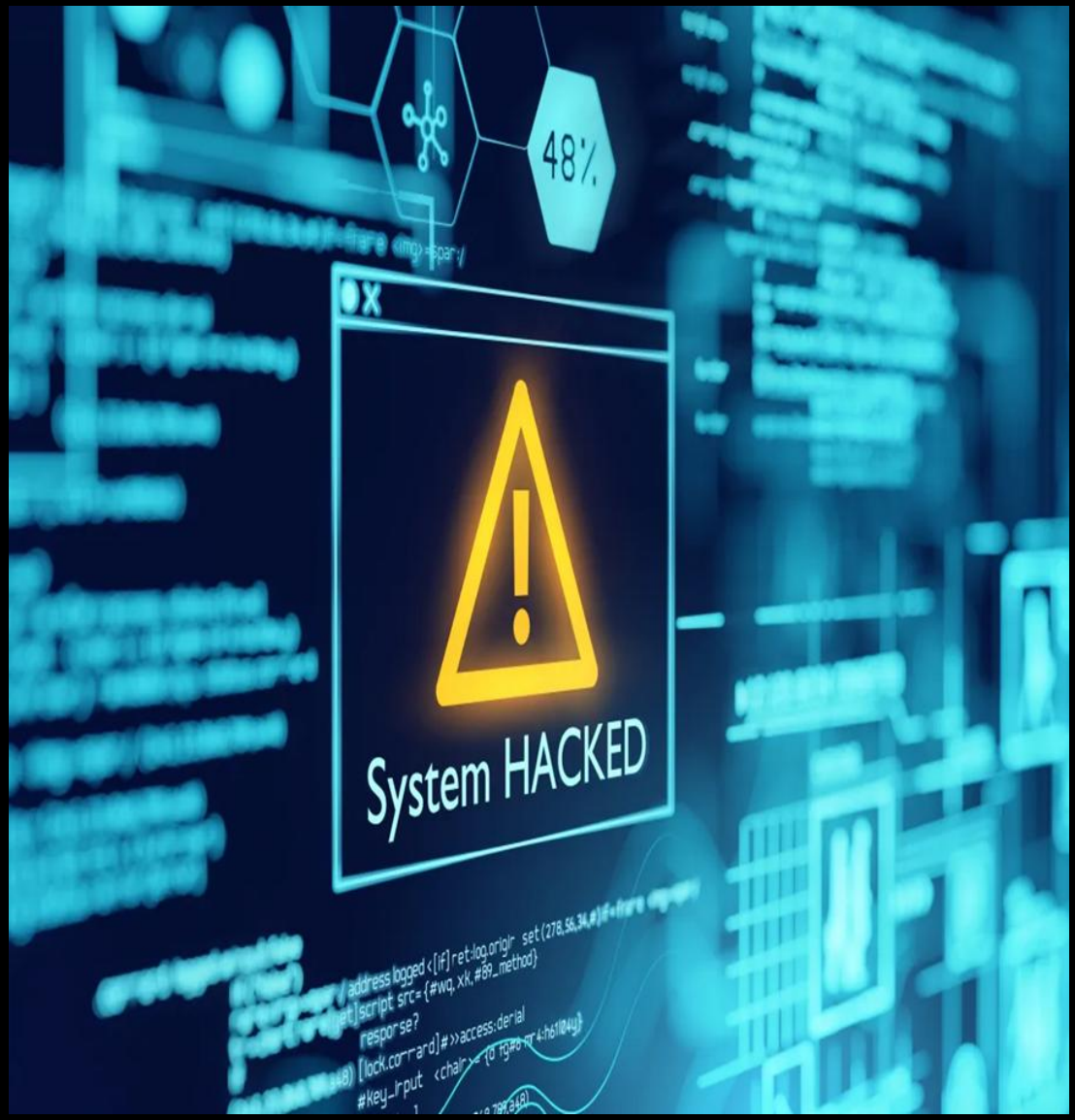
- Encrypting systems and demanding payment

Data Breaches

- Stealing protected health information

(Al-Qarni, 2023; Nifakos et al., 2021)

Ransomware Attacks, Deadly for Patients

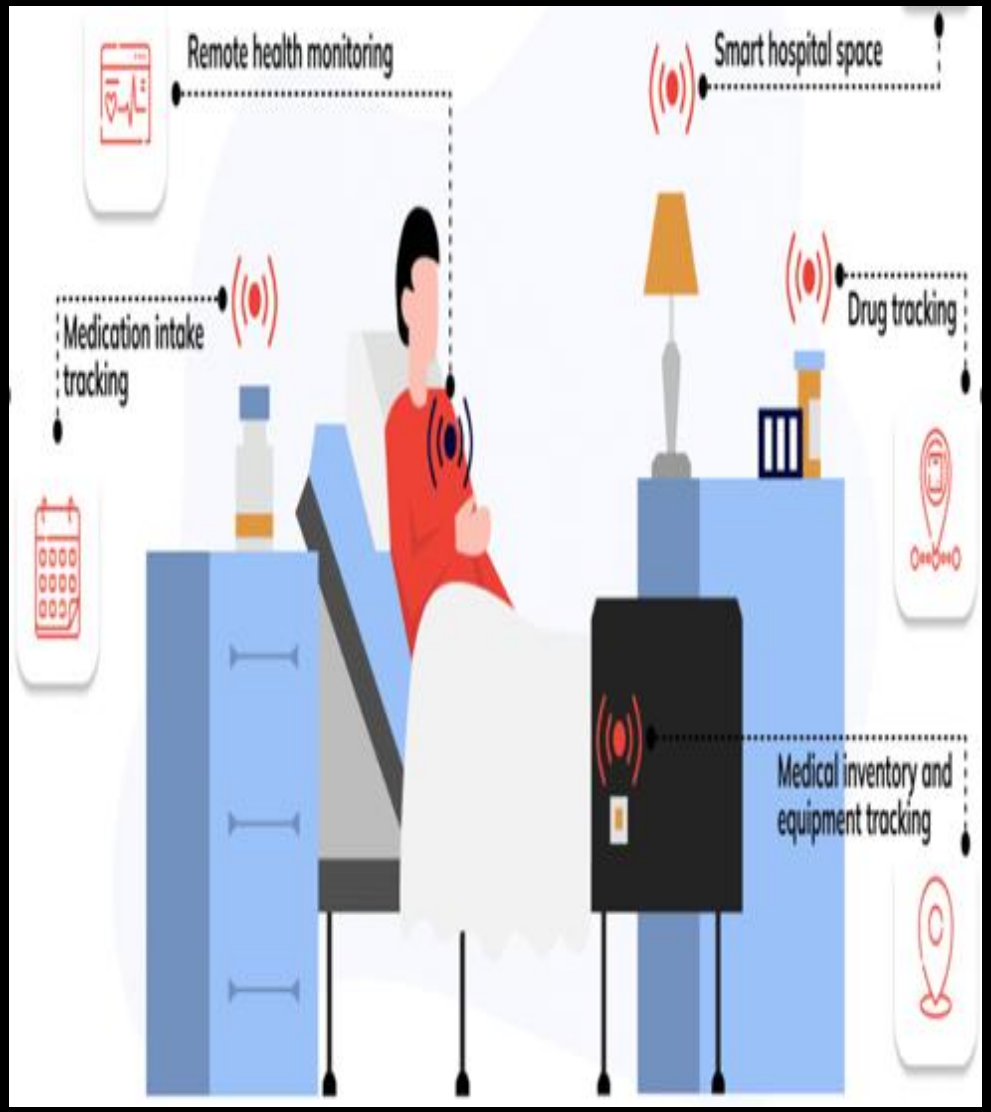


https://tradeoffs.org/2023/10/05/ransomware-attacks-patient-deaths/

Why Healthcare is Particularly Vulnerable?

1) Inadequate Security Measures
   - Chronic underfunding of cybersecurity initiatives in healthcare organizations
2) Outdated Systems and Practices
   - Legacy systems not designed with modern security threats in mind
3) High-Value Data
   - Medical records contain comprehensive personal information valuable for identity theft
4) Internet of Medical Things (IoMT)
   - **Connected medical devices create multiple entry points for attackers**
     - (Cartwright, 2023; Coventry & Branley, 2018)

IoMT risks, networked hospital equipment



https://intellisoft.io/iot-in-healthcare-key-trends-usages/

The Human Factor in Healthcare Cybersecurity

- While technology vulnerabilities exist,
  - **human behavior** remains one of the most significant cybersecurity risks in healthcare organizations.
  - Social engineering attacks specifically target healthcare professionals' lack of awareness and training.

Key Human Vulnerabilities includes;

- Phishing Attacks
  - Increasing threat of deceptive emails targeting healthcare staff
- Poor Cyber Hygiene
  - Unsafe practices when accessing social media platforms
- Insufficient Training
  - Lack of awareness programs to identify cyber threats
- Password Vulnerabilities
  - Weak or shared credentials among staff members

(Nifakos et al., 2021)

https://www.istockphoto.com/photos/social-engineering

Effective ways to Implement Cybersecurity Training for Employees - Staff Awareness

https://www.appliedtech.us/resource-hub/how-to-cybersecurity-train-employees/

Human Factor in Healthcare Cybersecurity - Continue

- Human error remains healthcare's major vulnerability
- Staff often fall for deceptive phishing attempts
- Limited cybersecurity training decreases organizational readiness
- High workload stress encourages risky digital actions
- Social engineering tactics exploit psychological weaknesses
- Human behavior significantly influences cybersecurity outcomes

Impact on Patient Safety and Public Health

- Cybersecurity breaches in healthcare extend beyond data theft,
  - they directly threaten patient safety and
  - can cripple entire health systems, with
  - potentially life-threatening consequences.

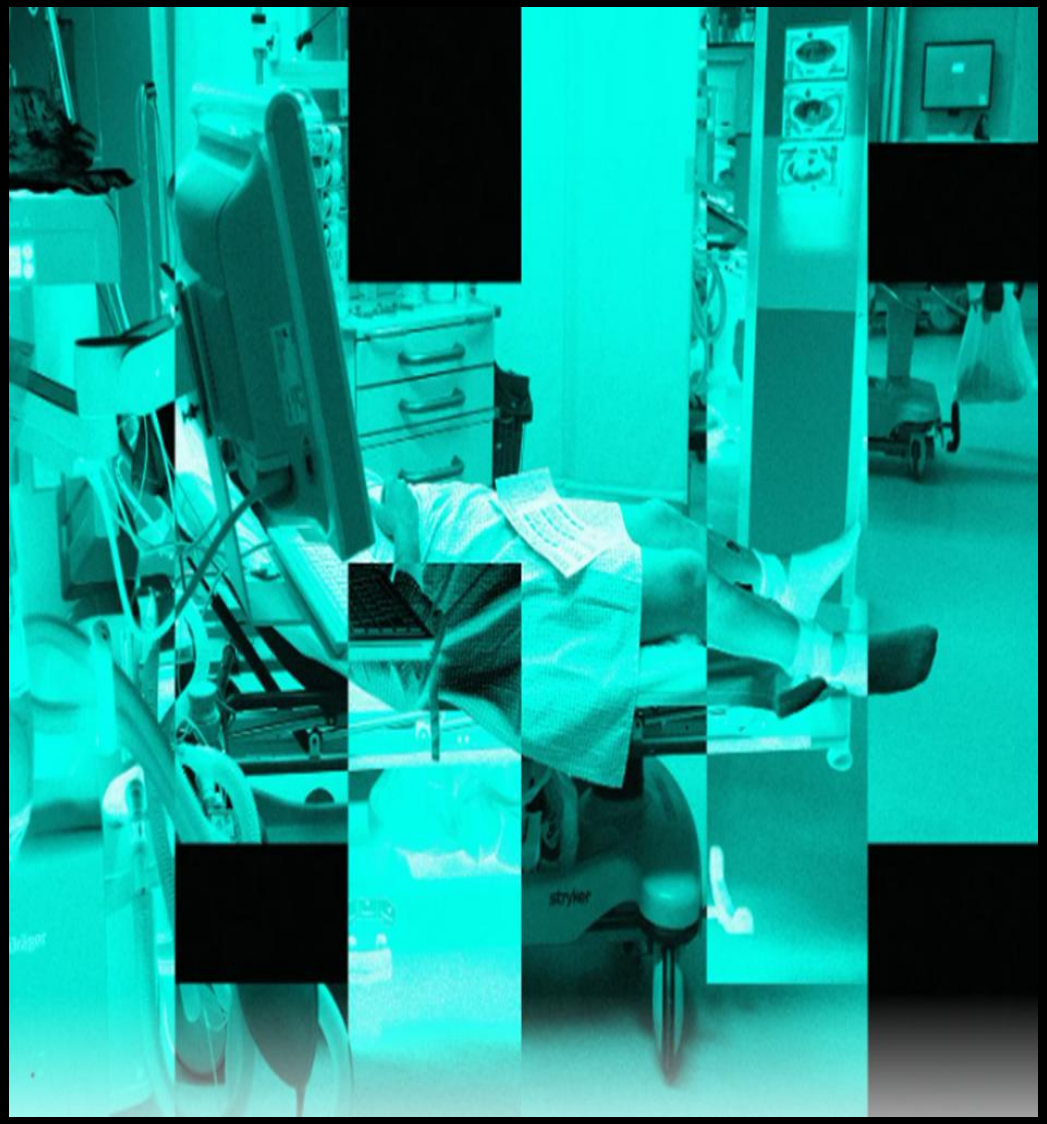
- **Direct Patient Harm**
  - Attacks on medical devices and monitoring systems
  - can lead to incorrect readings or altered treatment settings

- Service Disruption
  - Ransomware attacks can shut down hospital operations,
  - forcing emergency departments to divert patients

- Loss of Patient Trust
  - Data breaches erode confidence in healthcare systems and
  - may discourage patients from seeking care

(Coventry & Branley, 2018; Cartwright, 2023)

A woman dying in a hospital due to ransomware attack – Germany.



https://www.wired.com/story/ransomware-hospital-death-germany/

Case Study on WannaCry Ransomware Attack

- The WannaCry ransomware attack demonstrated the destructive nature of cyberattacks on healthcare systems.
- This global attack specifically highlighted the vulnerability of healthcare organizations to widespread service disruption.

Impact on Healthcare

- Hospitals and clinical environments experienced severe service disruptions,
  - with some facilities forced to cancel procedures and divert emergency patients to other hospitals.

Key Lesson

- The attack brought to life the need for robust cybersecurity measures and the real consequences of inadequate protection in healthcare settings.
  - (Nifakos et al., 2021)

- **How do we overcome this?**

COVID-19 Pandemic: Amplifying Vulnerabilities

- The COVID-19 pandemic significantly increased the threat surface for;
  - cyberattacks in healthcare,
  - creating circumstances that exposed the sector to heightened risk.

Rapid Digital Adoption

- Accelerated implementation of telehealth and
  - remote monitoring without adequate security planning.

Changed Work Patterns

- Remote work arrangements increased exposure to
  - unsecured home networks

System Strain

- Overwhelmed healthcare systems had fewer resources to dedicate to cybersecurity

Opportunistic Attacks

- Cybercriminals exploited the crisis, targeting vulnerable healthcare organizations (Cartwright, 2023)

Patient Data and Privacy

- Protected health information requires strong safeguards
- Data breaches seriously undermine patient confidence
- Privacy protection remains fundamental healthcare responsibility
- Regulations guide appropriate patient data handling
- Security must balance clinical information accessibility
- Data protection directly supports patient safety

https://www.istockphoto.com/photos/patient-privacy

Privacy and Ethical Considerations

- **Healthcare cybersecurity** intersects critically with privacy rights and ethical obligations.
- The protection of Protected Health Information (PHI) is both a legal requirement and an ethical imperative.

Ethical Dimensions

- Patient Autonomy
  - Individuals have the right to control their personal health information

Confidentiality

- Healthcare providers have a duty to protect patient privacy

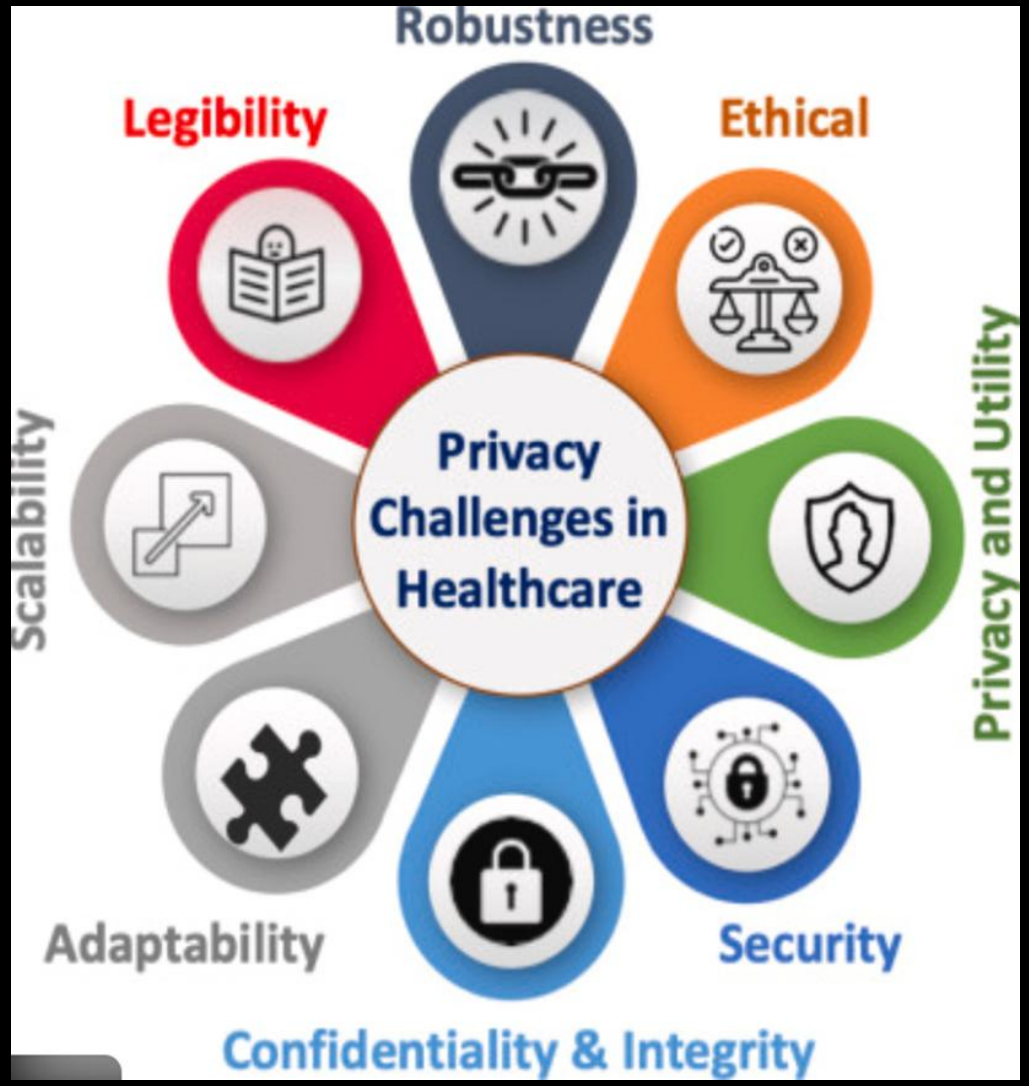
Trust

- **The patient-provider relationship depends on confidence in data security**

Justice

- Vulnerable populations may be disproportionately affected by breaches

(Coventry & Branley, 2018; Cartwright, 2023)



https://www.sciencedirect.com/science/article/pii/S001048252300313X

Mitigation Strategies: Technology Solutions

- Addressing cybersecurity in healthcare requires a holistic approach;
  - that combines technological solutions with human and
  - organizational changes.

System Updates and Patches

- Constantly upgrade systems to address known vulnerabilities

Network Segmentation

- Isolate critical systems and medical devices from general networks

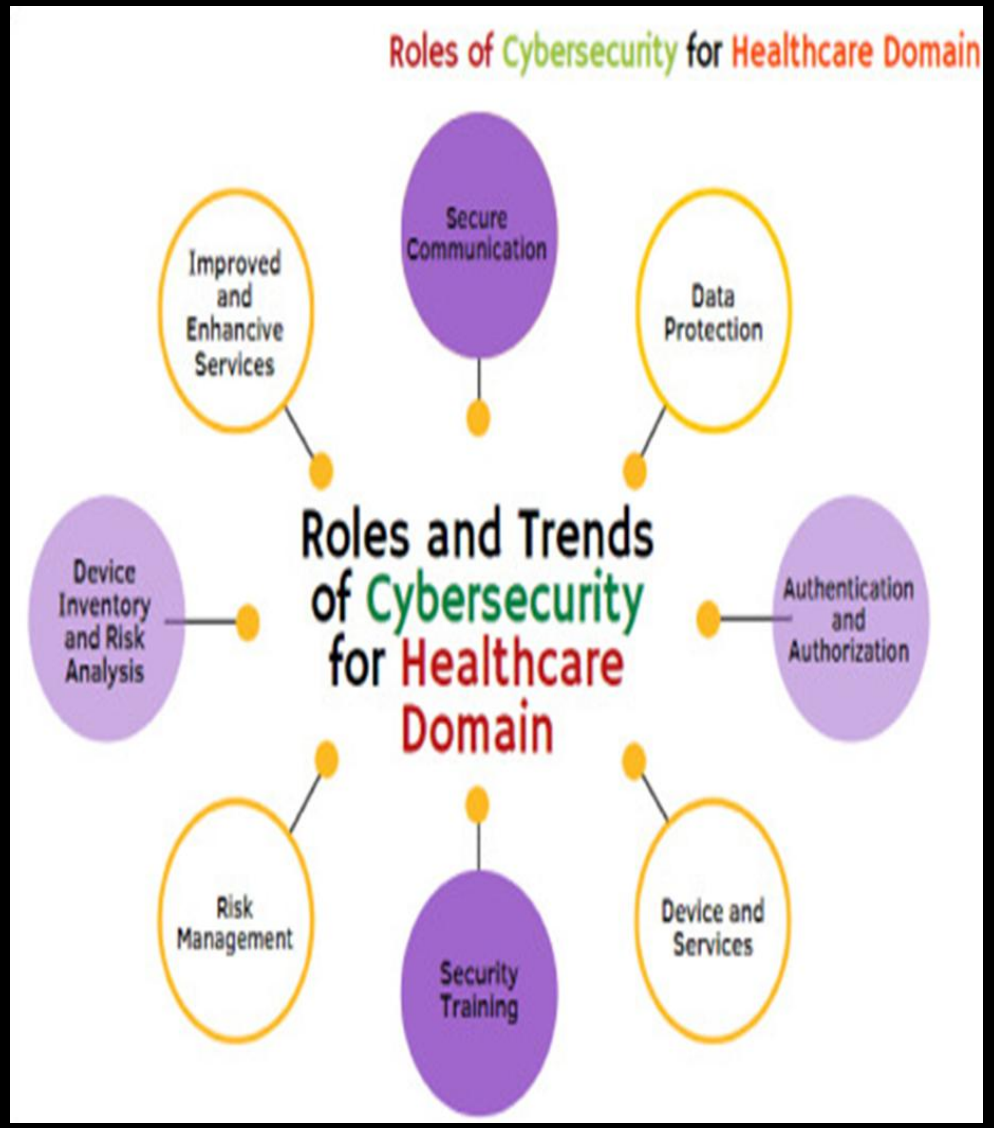
Encryption Standards

- Implement strong encryption for data at rest and in transit

Access Controls

- Multi-factor authentication and role-based access management

(Al-Qarni, 2023; Kruse et al., 2017)



https://www.sciencedirect.com/science/article/pii/S2772918423000048

Mitigation Strategies: Human Factors

Technology alone cannot solve cybersecurity challenges.

- Addressing human factors through comprehensive training and
  - awareness programs is essential for creating a security-conscious culture.

Regular Training

- Ongoing cybersecurity awareness programs for all staff members

Phishing Simulations

- Practice identifying and responding to social engineering attempts

Cyber Hygiene

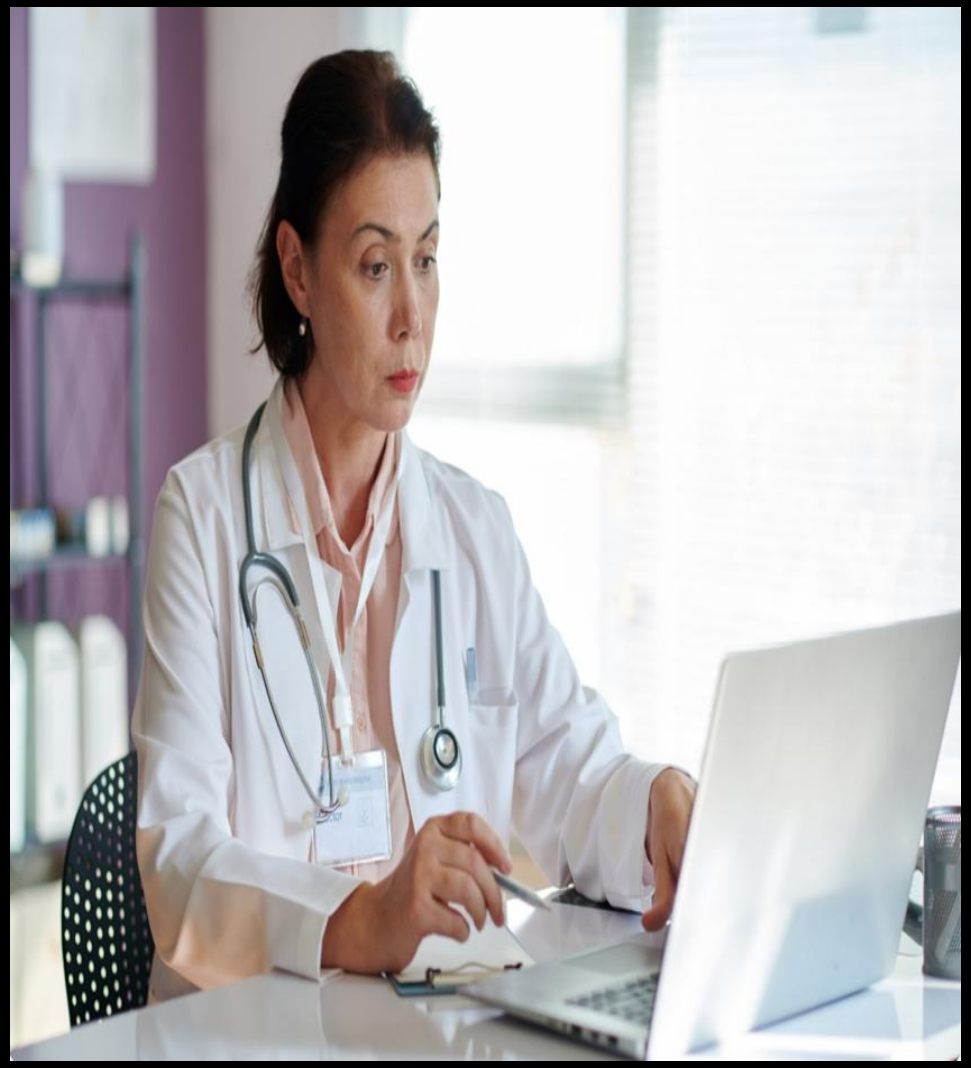
- Establish safe practices for social media and personal device usage

Reporting Culture

- Encourage staff to report suspicious activities without fear

(Nifakos et al., 2021; Al-Qarni, 2023)

Clinical Staff – Training on Phishing Detection



https://focushcs.com/phishing-detection-in-healthcare/

Policy and Organizational Requirements

- **New legislation and regulations mandate that;**
  - **cybersecurity become an integral part of patient safety.**
  - **Healthcare organizations must adopt comprehensive policies and governance structures.**
  - **Example: HIPAA has established standards to protect patient privacy**

Clear Security Policies

- Establish and enforce comprehensive cybersecurity policies across all departments

Incident Response Plans

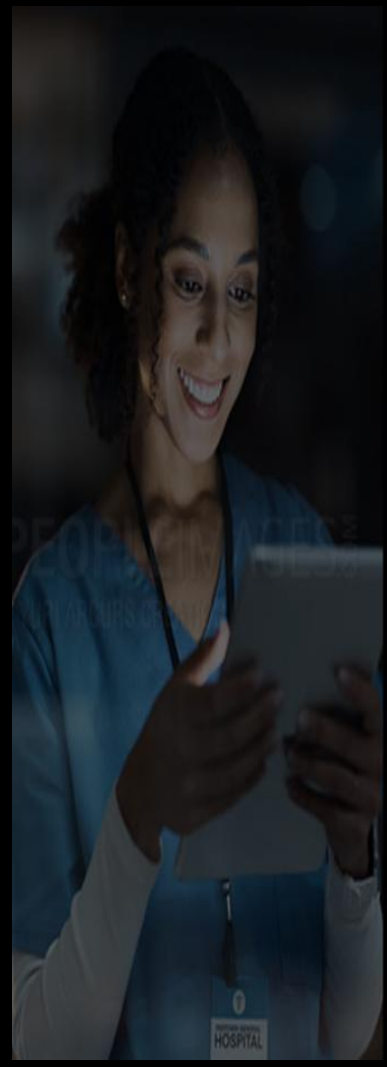
- Develop and regularly test backup plans for managing and recovering from cyberattacks

Risk Assessment Methodologies

- Implement systematic approaches to identify and evaluate cybersecurity risks

Adequate Investment

- Allocate sufficient resources to cybersecurity infrastructure and personnel



(Coventry & Branley, 2018; Al-Qarni, 2023)

https://www.vectorstock.com/royalty-free-vector/shield-line-icon-privacy-data-protection-vector-19322557

Conclusion: A Holistic Approach

- **Cybersecurity in healthcare is fundamentally a patient safety issue;**
  - **that requires integration of technological solutions,**
  - **human behavior changes, and**
  - **organizational processes.**
- The intersection of cybersecurity with social sciences reveals that technical measures alone are insufficient.

Key Takeaways:

- **Healthcare cybersecurity is critical to patient safety and public trust**
- **Human factors are as important as technological defenses**
- **A holistic approach addressing technology, people, and processes is essential**
- **Continuous adaptation is necessary as threats evolve**
- **Protecting healthcare systems protects human lives.**

References

Al-Qarni, E. A. (2023). Cybersecurity in healthcare: A review of recent attacks and mitigation strategies. Retrieved from https://pdfs.semanticscholar.org/6602/dc04b31e9e124c72c1854faa657767766798.pdf

Cartwright, A. J. (2023). The elephant in the room: Cybersecurity in healthcare. Journal of Clinical Monitoring and Computing. https://doi.org/10.1007/s10877-023-01013-5

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52.

https://doi.org/10.1016/j.maturitas.2018.04.008

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care, 25(1), 1-10.

https://doi.org/10.3233/THC-161263

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. Sensors, 21(15), 5119.

https://doi.org/10.3390/s21155119