INL/MIS-24-79859-Revision-0

Healthcare Cybersecurity

July 2024

Amaturrahman Raihanah Medlock

Changing the World's Energy Future

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/MIS-24-79859-Revision-0

Healthcare Cybersecurity

Amaturrahman Raihanah Medlock

July 2024

Idaho National Laboratory
Idaho Falls, Idaho 83415

http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

July 29, 2024

Amaturrahman Raihanah Medlock
Mentors: Jana Richens and Ben Lampe
Michigan Technological University
D-052

Healthcare Cybersecurity

With a focus in patient data security, system interoperability, and medical device vulnerability mitigation

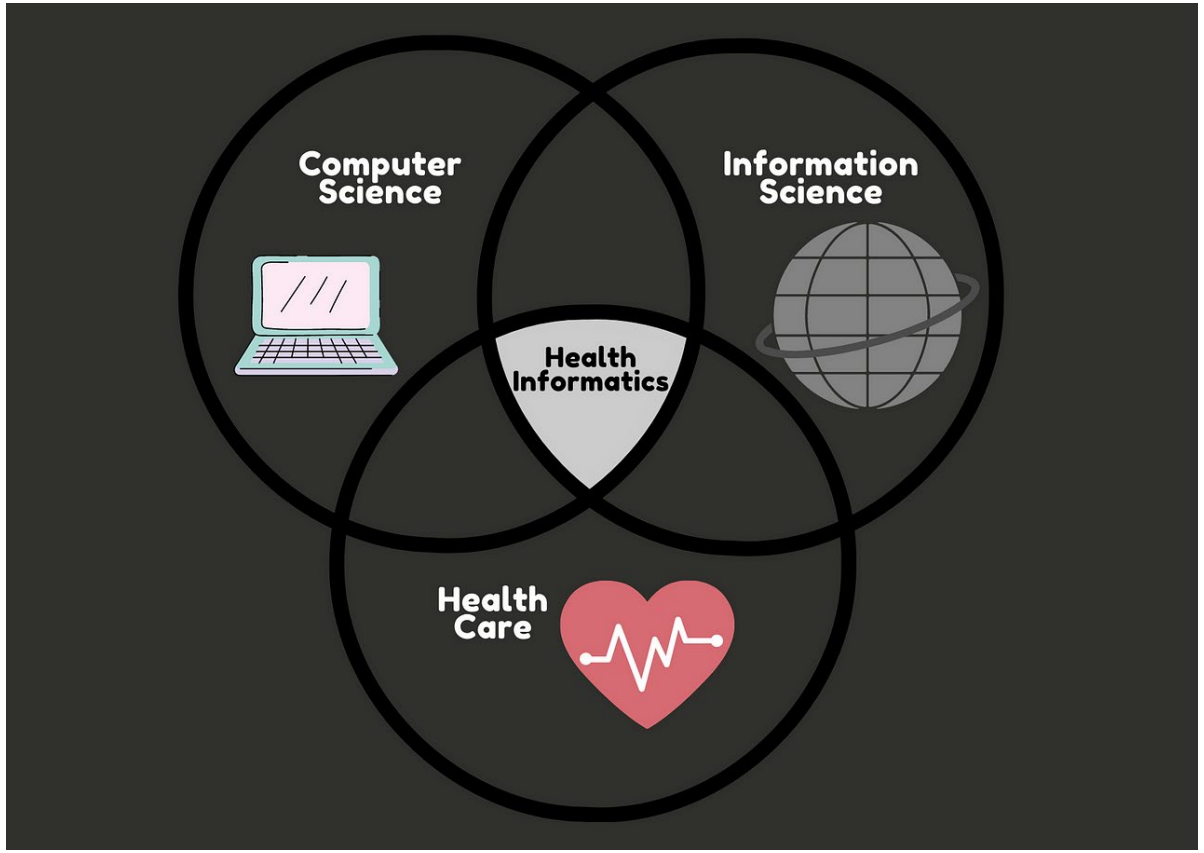
Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

Idaho National Laboratory

Table of Contents

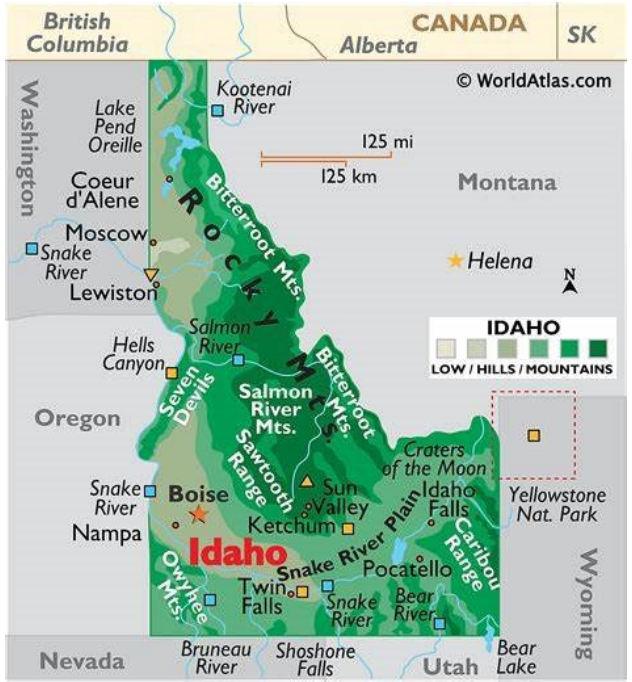
Introduction

- Health Informatics and Healthcare Cybersecurity



Relevance

- In 2023, Idaho Falls Community Hospital, Mountain View Hospital, Madison Memorial Hospital, and Portneuf Medical Center were victims of cyber attacks
  - East Idaho News



Cyber on the Rise

- Emerging Trends
  - MIoT
  - Big Data
  - Mobile Health Apps
  - Cloud Computing
- Cyber Challenges
  - Lack of Policy
  - Human Factor
  - Stakeholder Consensus
  - Inadequate Investments
- Countermeasures
  - Blockchain
  - Encryption
  - Education/Training
  - Policy/Regulation
  - IT infrastructure management
  - Cyber-Informed Engineering

Principles of CIE

- **Consequence-Focused Design***
- Engineered Controls
- **Secure Information Architecture***
- Design Simplification
- **Resilient Layered Defenses***
- Active Defense
- **Interdependency Evaluation***
- Digital Asset Awareness
- **Cyber-Secure Supply Chain Controls***
- Planned Resilience
- Engineering Information Control
- Cybersecurity Culture

Recent Threats to the Sector

- Ransomware Attacks
  - Compromised data security
  - Significant service disruption
- Phishing attacks
  - Employees unable to access patient info, X-rays, and unable to backup services
- DDoS (Distributed Denial of Service) attacks
  - Disrupt hospital operations
- Social engineering
- Malware
  - Postpone high-risk surgeries
  - Permanently destroyed backup files

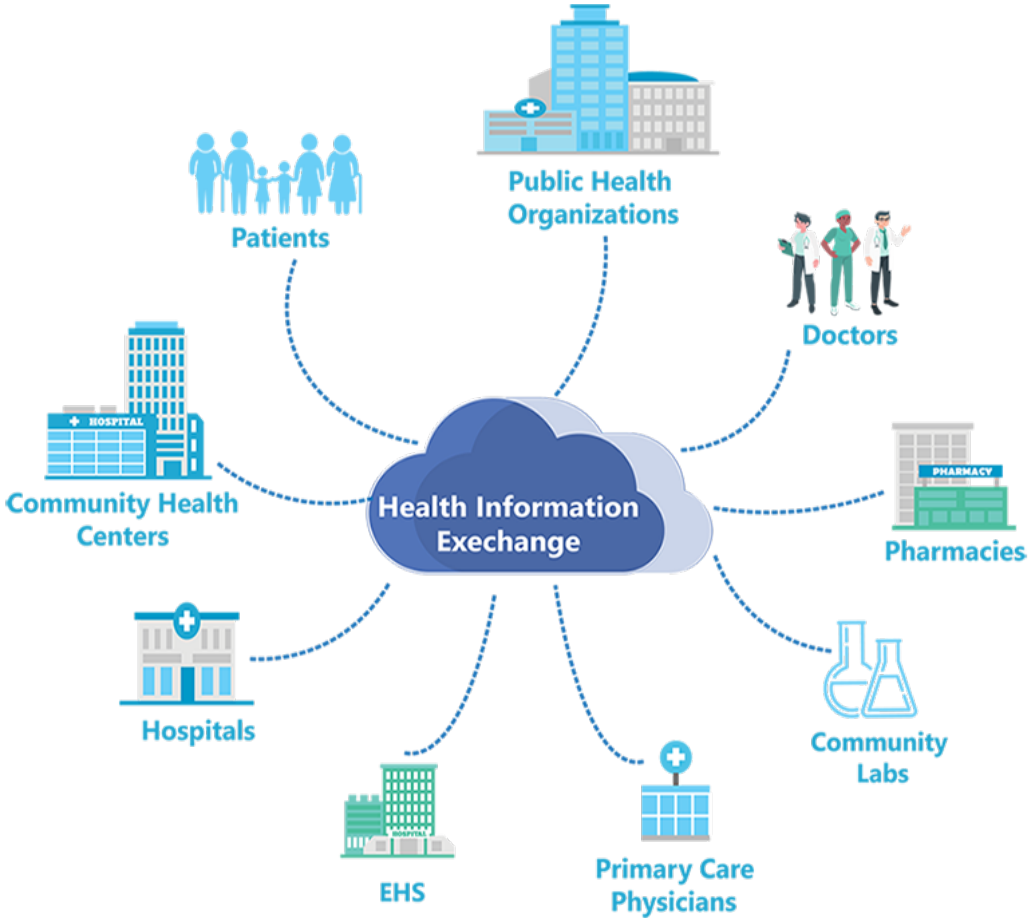
According to IBM- as of 2023, the average cost of a healthcare data breach is $10.9 million.

2- Patient Data Security

Current Technical Regulations

1. Health Information Technology for Economic and Clinical Health Act (HITECH)
    I. Sets meaningful use of interoperable electronic health record (HER) adoption in healthcare system as a critical national girl and incentivized EHR adoption
2. Health Insurance Portability and Accountability Act (HIPAA)
    I. Stipulated the guidelines by which personally identifiable information (PII) maintained by healthcare providers and insurance entities should be protected form theft and fraud, and addressed some limitations on healthcare insurance coverage
3. Pre-Market Approval
    I. FDA scientific and regulatory evaluation of Class iii medical devices

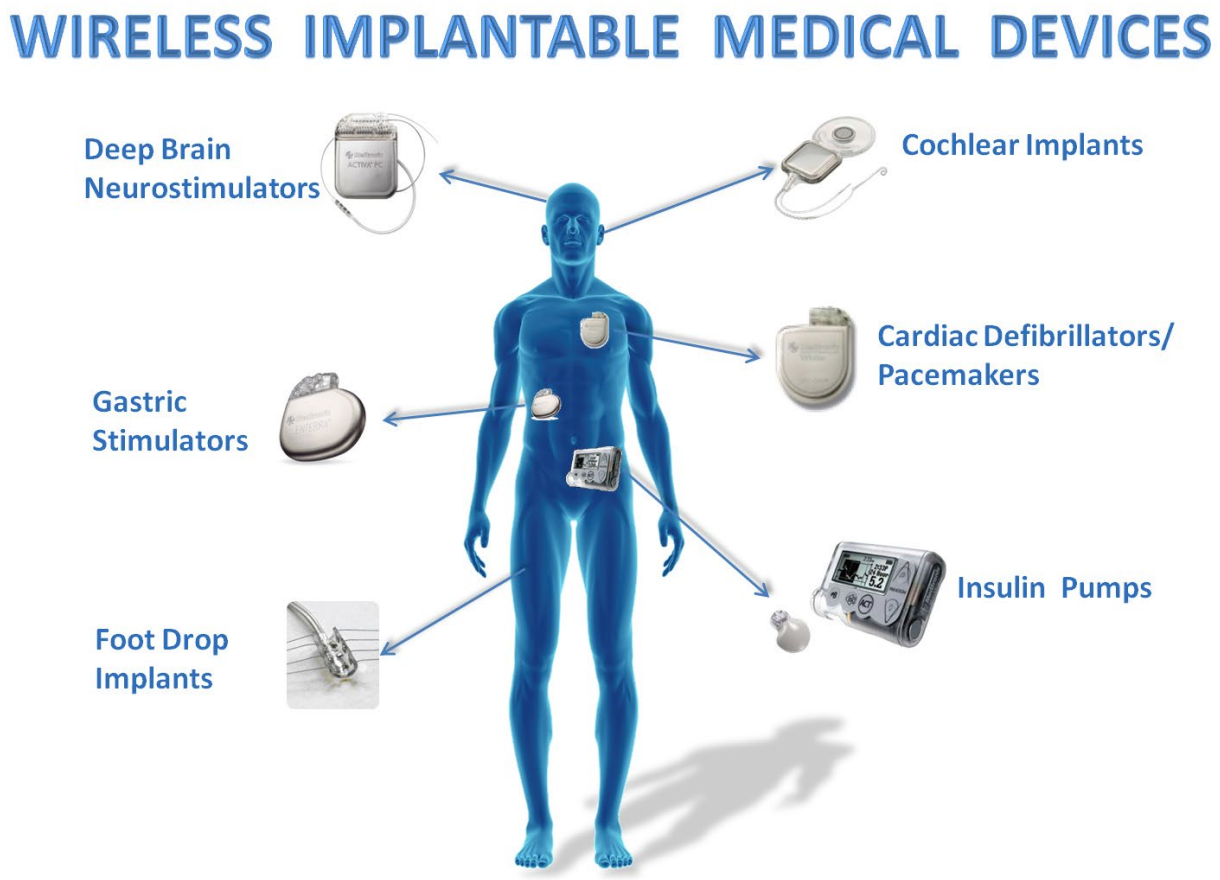
3- System Interoperability



Interoperability Opportunities

- FHIR
  - Fast healthcare interoperability resources is a standard developed by HL7 which facilitates HIE
- Data virtualization
  - Integrating and presenting data from multiple sources in a unified manner without physical changes
- Big data analytics
  - Use of advanced analytical techniques to process and analyze large volumes of diverse data generated within the healthcare environment

4- Medical Device Vulnerability Mitigation



Medical Internet of Things

- MIoT
  - IoT
    - Network of interconnected devices embedded with software and connectivity capabilities to exchange data
  - Medical
    - Enables operation of smart health devices

Mitigation

- HL7 FHIR
- Cryptography
- Data anonymization
- Subnetting
- Blockchain found in cloud
- Engineered controls

FDA Approvals for AI Medical Devices

510(k) clearance

Granted when an algorithm is proven to be at least as safe and effective as a similar, legally marketed algorithm

Premarket Approval

Issued for Class iii devices for proven safety and effectiveness with satisfactory scientific evidence

de novo pathway

Used to classify novel medical devices for which there are no legally marketed counterparts but offer adequate safety and effectiveness with general controls. FDA performs risk-based assessment before marketing

Conclusions

- This project provides INL with:
  - A tangible educational framework for those interested in healthcare cybersecurity
  - An educational experience highlighting some of the core problem areas and potential mitigation opportunities in healthcare cybersecurity
  - An introduction to the critical nature and dire need for investment in healthcare cybersecurity

References

- Journal of Medical Internet Research - Cybersecurity in Hospitals: A Systematic, Organizational Perspective (jmir.org)
- A Socio-technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks (thieme-connect.de)
- Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies (semanticscholar.org)
- Step-by-Step Risk Management for Medical IT Networks | Biomedical Instrumentation & Technology (aami.org)
- Transforming Healthcare Cybersecurity from Reactive to Proactive: Current Status and Future Recommendations | Journal of Medical Systems (springer.com)
- Big healthcare data: preserving security and privacy | Journal of Big Data (springer.com)
- Trustworthy Intrusion Detection in E-Healthcare Systems - PMC (nih.gov)
- A comparative study of cyber security intrusion detection in healthcare systems - ScienceDirect
- Interoperability framework for integrated e-health services | Amin | Bulletin of Electrical Engineering and Informatics (beei.org)
- JMIR Medical Informatics - Fast Healthcare Interoperability Resources (FHIR) for Interoperability in Health Research: Systematic Review
- Blockchain for healthcare data management: opportunities, challenges, and future recommendations | Neural Computing and Applications (springer.com)
- Approval of artificial intelligence and machine learning-based medical devices in the USA and Europe (2015–20): a comparative analysis - The Lancet Digital Health
- The state of artificial intelligence-based FDA-approved medical devices and algorithms: an online database | npj Digital Medicine (nature.com)

Idaho National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.