Emerging Technology and the Security Implications for the Health Sector

September 8, 2022

TLP: WHITE, ID# 202209081300

Agenda

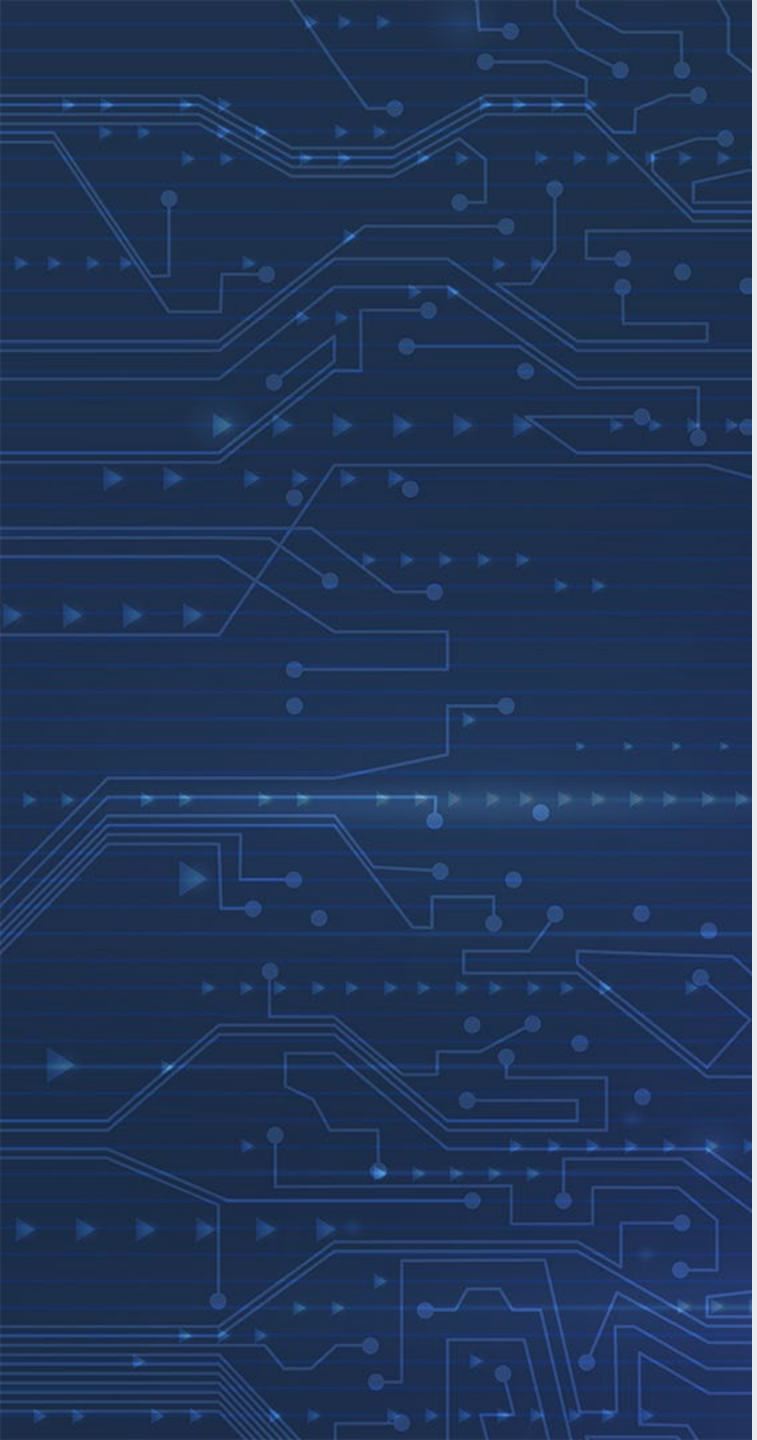
Modern information technologies are having a profound effect on the health sector, but they also bring with them security considerations

- Introduction
- Artificial Intelligence
- 5G Cellular Technologies (and Beyond)
- Nanomedicine
- Smart Hospitals
- Quantum Computing

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)



Artificial Intelligence

The science of intelligent machines

Artificial Intelligence

Artificial intelligence is technology that mimics human activity, decision-making, and learning

- What is Artificial Intelligence (AI)?
  - Per John McCarthy, Stanford University:
    - "…the science and engineering of making intelligent machines, especially intelligent computer programs"
    - "… related to the similar task of using computers to understand human intelligence…"
    - "…AI does not have to confine itself to methods that are biologically observable"
  - Per IBM:
    - "…leverages computers and machines to mimic the problem-solving and decision-making capabilities of the human mind"

Blade Runner movie poster
Image source: IMP Awards

Artificial Intelligence in Healthcare

Artificial intelligence in healthcare has the potential to revolutionize clinical research and the monitoring and delivery of care

Recommended reading:
Cloud Security Alliance: Artificial Intelligence in Healthcare

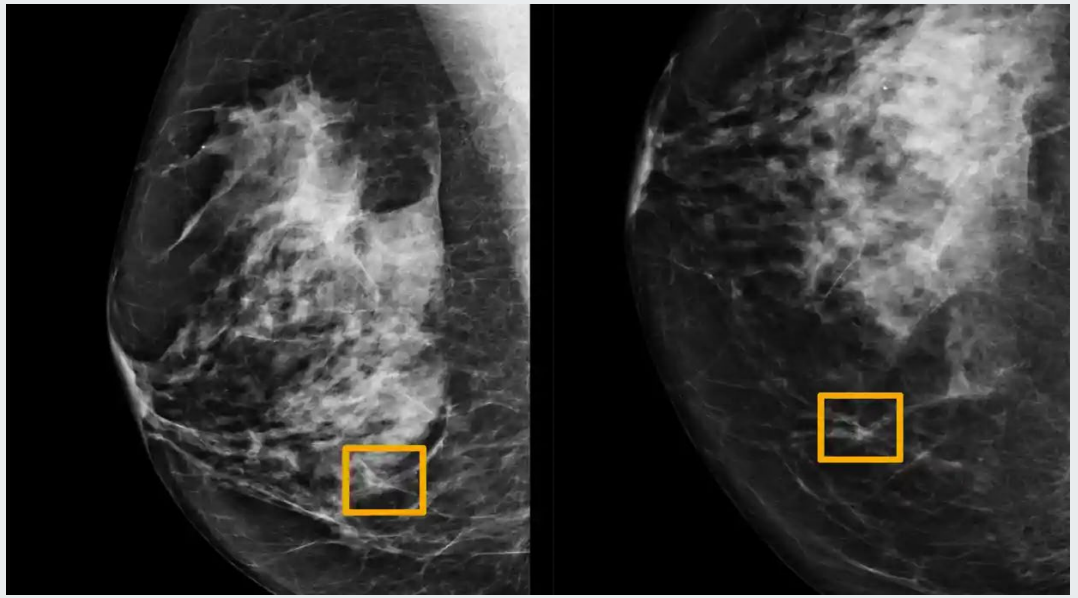
- Benefits of AI to the health sector:
  - Analysis of big data sets
    - Accelerated clinical decisions
      - Example: Interpretation of medical imaging
    - Improved (deeper) patient insights → predictive analysis
      - Connecting disparate health data (integrated electronic health records)
    - New drug discovery and preventive medicine
  - Medical devices (Software-as-a-Medical-Device/SaMD)
    - "...software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device"
  - Improved efficiency of enterprise operations/streamlined workflows

Artificial Intelligence: Benefits to Healthcare

AI system outperforms experts in spotting breast cancer

An AI program developed by Google in 2020 has demonstrated the ability to spot breast cancer in mammograms better than expert radiologists

The yellow box in the images on the right indicate where an AI system identified cancer in breast tissue. Six radiologists had previously failed to identify it.



Medical imagery indicating cancer
Image source: The Guardian

Read more:
https://www.theguardian.com/society/2020/jan/01/ai-system-outperforms-experts-in-spotting-breast-cancer

Artificial Intelligence: Benefits to Healthcare, Part 2

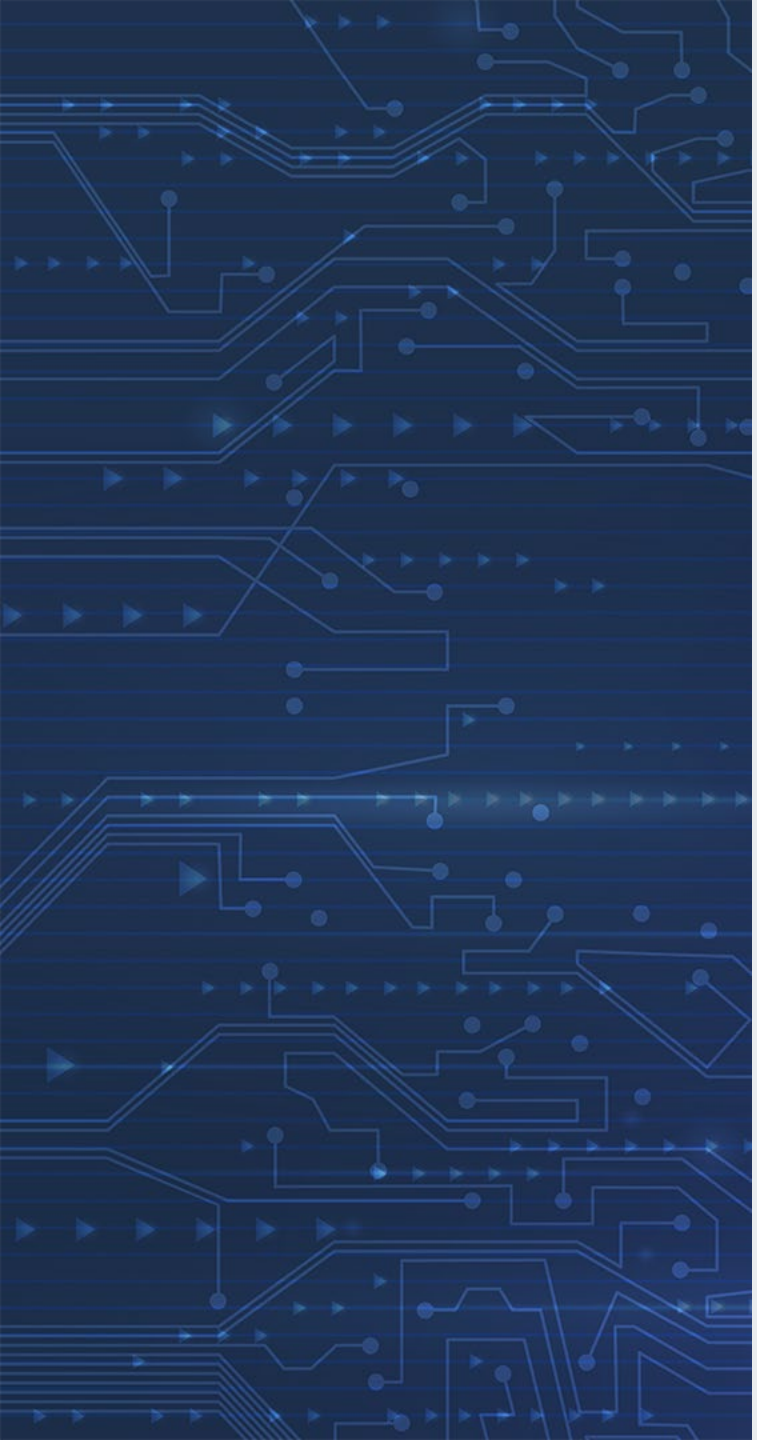
Scientists demonstrate that AI systems can identify bacteria systems quickly and accurately:

- Kenneth P. Smith, Anthony D. Kang, and James E. Kirby, microbiologists at the Beth Israel Deaconess Medical Center, published a paper in the *Journal of Clinical Microbiology* in 2018 titled, “Automated Interpretation of Blood Culture Gram Stains by Use of a Deep Convolutional Neural Network.”
- “With further development, we believe this technology could form the basis of a future diagnostic platform that augments the capabilities of clinical laboratories, ultimately speeding the delivery of patient care.”
- “Like a child, the system needed training. Learning to recognize bacteria required a lot of practice, making mistakes and learning from those errors.”

Source: https://journals.asm.org/doi/10.1128/JCM.01521-17

Artificial Intelligence in Healthcare: Security Concerns

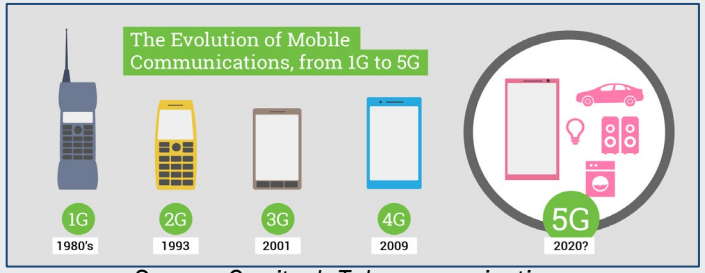
- Artificial Intelligence is not inherently insecure, but…
- Artificial Intelligence requires the gathering of very large collections of data in order to learn
  - Privacy and security concerns regarding personal health information (PHI)
  - U. California at Berkeley 2019 study: Artificial intelligence advances threaten privacy of health data
  - Therefore, data needs to be protected at rest and in motion:
    - Data repository security
    - End-to-end encryption and multi-factor authentication
- Artificial Intelligence allows for the re-identification of de-identified data
- Repurposing of research data must be done with consideration for de-identification
- Confidentiality is very important in protecting the health sector from AI technologies



5G Cellular and Beyond

5G Cellular and Beyond

- Fifth generation cellular network technology (officially called ‘5G New Radio’)
- Adopted by 3rd Generation Partnership Project (3GPP), an international organization responsible for 3G UMTS (Universal Mobile Telecommunications System) and 4G LTE (Long-Term Evolution)
- Several improvements:
  - Approximately 10 to 100 times faster than typical current cellular connections; faster than residential physical fiber optic cable; can handle significantly greater number of devices simultaneously (IoT)
  - Significantly reduced latency: 20 milliseconds to 1 millisecond
  - Customized networks
- Potential issues:
  - High speed/capacity means shorter range of each cell tower, more must be deployed
  - Concerns over health issues
  - Eyesores in residential neighborhoods



Source: Carritech Telecommunications

Cellular Technology Generations

	1G	2G	3G	4G	5G
Period	1980 – 1990	1990 – 2000	2000 – 2010	2010 – (2020)	(2020 - 2030)
Bandwidth	150/900MHz	900MHz	100MHz	100MHz	1000x BW pr unit area
Frequency	Analog signal (30 KHz)	1.8GHz (digital)	1.6 – 2.0 GHz	2 – 8 GHz	3 – 300 GHz
Data rate	2kbps	64kbps	144kbps – 2Mbps	100Mbps – 1Gbps	1Gbps <
Characteristic	First wireless communicatio n	Digital	Digital broadband, increased speed	High speed, all IP	
Technology	Analog cellular	Digital cellular (GSM)	CDMA, UMTS, EDGE	LTE, WiFi	WWWW

Source: LinkedIn

5G and Healthcare

- “Healthcare will benefit from 5G technology from countless aspects; it is basically the field that might experience the most changes.” – *The Medical Futurist*
- 5G technology is expected to enable telemedicine due to the low latency it offers
- Robotics autonomously or semi-autonomously performing medical procedures
- 5G is expected to make telesurgery possible, due to the low latency that it offers as well as its enhancements to robotics, which would then aid surgery
- In the future, language translators will be able to video conference with the patient and doctor using models at the network edge with low latency
- Better leveraging of Artificial Intelligence tools
- Better access to more specialists for collaboration
- 5G data traffic explosion to drive 5G small cell deployments to 13 million by 2027

5G Enables Internet of Medical Things (IoMT)

- Wearables/Internet of Medical Things (IoMT):
  - Transmit often real-time data to doctors about the user's health (remote patient monitoring)
  - Facilitate improved care remotely and to more people
  - According to Anthem, 86% of doctors say IoMT devices increase patient engagement with their own health
  - Predicted to decrease hospital costs by 16 percent in the next five years
  - 5G technology enables IoMT networks to operate in a stable, fast and highly reliable manner

Source: Researchgate (Din and Almogren)

5G in Healthcare: Security Concerns

- In many ways, security threats for 5G-enabled healthcare technologies overlap with IoT threats:
  - Need to secure medical devices as they connect to the network (authentication)
  - Need to secure data as it is transmitted to/from medical devices (end-to-end encryption)
  - Need to secure data on device (whole disk encryption or similar procedure)
- IoMT software/firmware development should include both trustworthiness and resilience
  - Trustworthiness may require the use of authentication and encryption technology
  - Resilience may require fallback to a safe mode in the case of a cyberattack
  - Software design and update practices should be transparent
- The design and implementation of the software in medical devices should include a specification of cybersecurity features and validation of those features, as well as a Cybersecurity Bill of Materials ("CBOM")
- Regularly employ static and/or dynamic vulnerability testing of the software on 5G devices
- Regularly update software on 5G devices in a secure manner
- It will be absolutely critical to segment and monitor 5G networks

Nanomedicine

The application of nanomaterials to address healthcare problems

Nanomedicine

- What is nanomedicine?
  - One definition: “The comprehensive monitoring, control, construction, repair, defense, and improvement of human biological systems at the molecular level, using engineered nanodevices and nanostructures, operating massively in parallel at the single-cell level, performing ‘single-cell medicine,’ ultimately to achieve medical benefit.” (Schachat, 2018)
  - In simpler terms, it is the medical application of nanotechnology (very small technology)
    - Smaller than 100 nanometers (1 billion nanometers = 1 meter)
- What benefits can nanomedicine bring?
  - The possibility of delivering drugs to specific cells using nanoparticles = improved absorbability
  - Improved diagnostics due to the distinct properties of nanomaterials, making them suitable for diagnostic imaging (especially the detection of cancerous tumors)
  - Improved theranostics (the combination of diagnostics with therapy)
    - Potential for personalized medicine
  - Testing that can be done remotely, such as in pharmacies

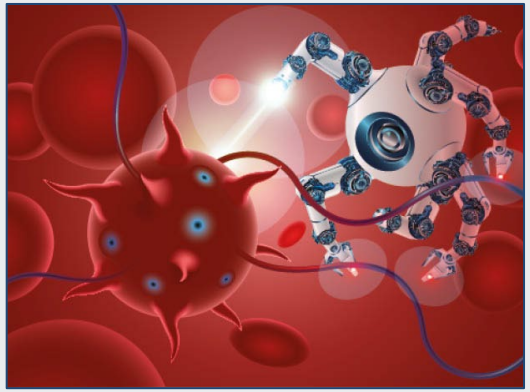


Image source: Pharmatimes

Nanomedicine and Cybersecurity

- Potential threats to nanomedicine – "hacking humans"
  - Remote connectivity
    - Ransomware and the disruption of nanotechnology devices with theoretically fatal consequences
    - Compromise of many nanodevices for traffic flooding/DDoS
  - Weaponized inhalable particles as a delivery system for bioterrorism
- Penetration and security testing is likely going to play a big role in securing nanomedicine technologies
- It is also believed that many of the same principles that are used to secure medical devices will also be used to secure nanomedicine technology
  - Securing data at rest and in motion
  - Software and hardware bills of materials
  - Resilience

Smart Hospitals

Improved efficiency via the latest information technologies

What Is a Smart Hospital?

- Features:
  - Greater interconnectivity
  - Real-time access to data
  - Real-time processing
- Impacts:
  - Environmental
  - Patient administration
  - Patient care
    - Shared health records
    - Efficient disease prevention
    - Efficient primary care
    - Targeted/effective quality acute care
    - Improved long-term disease management

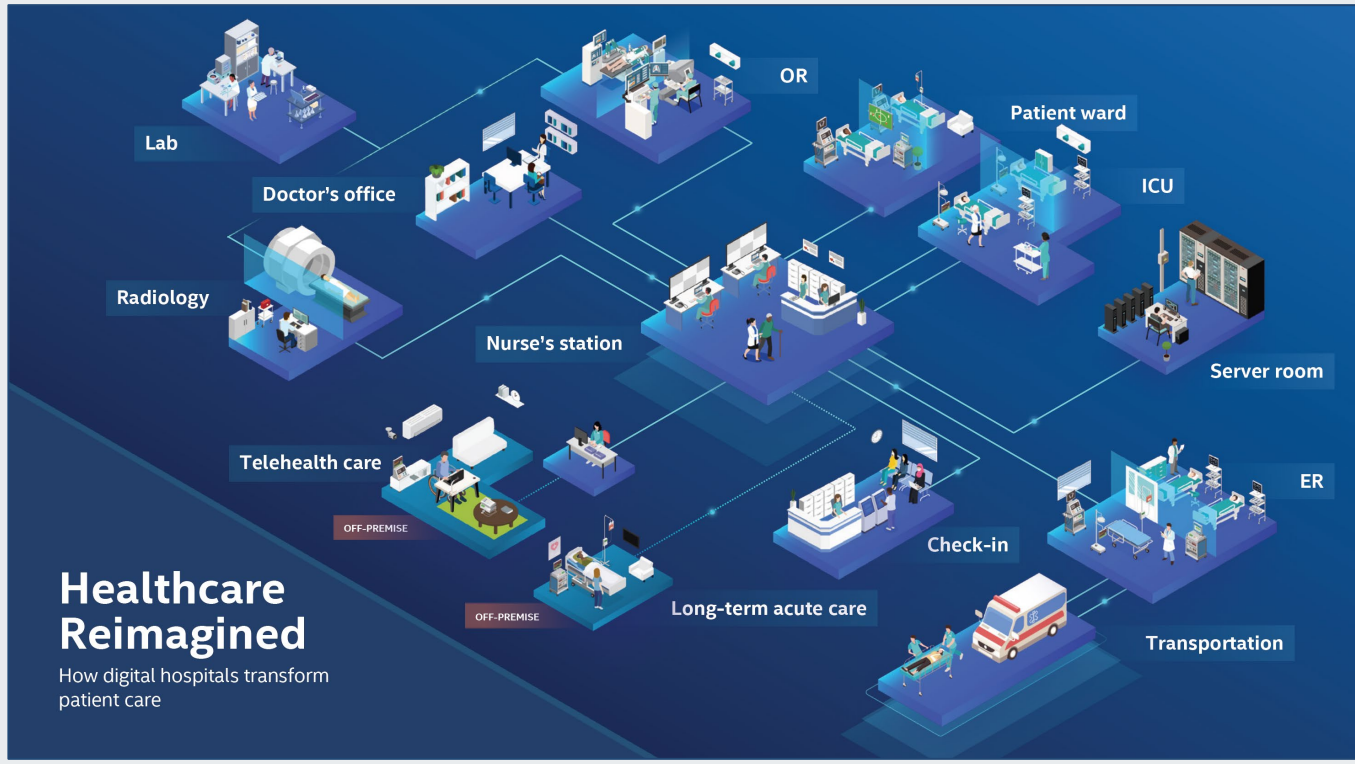


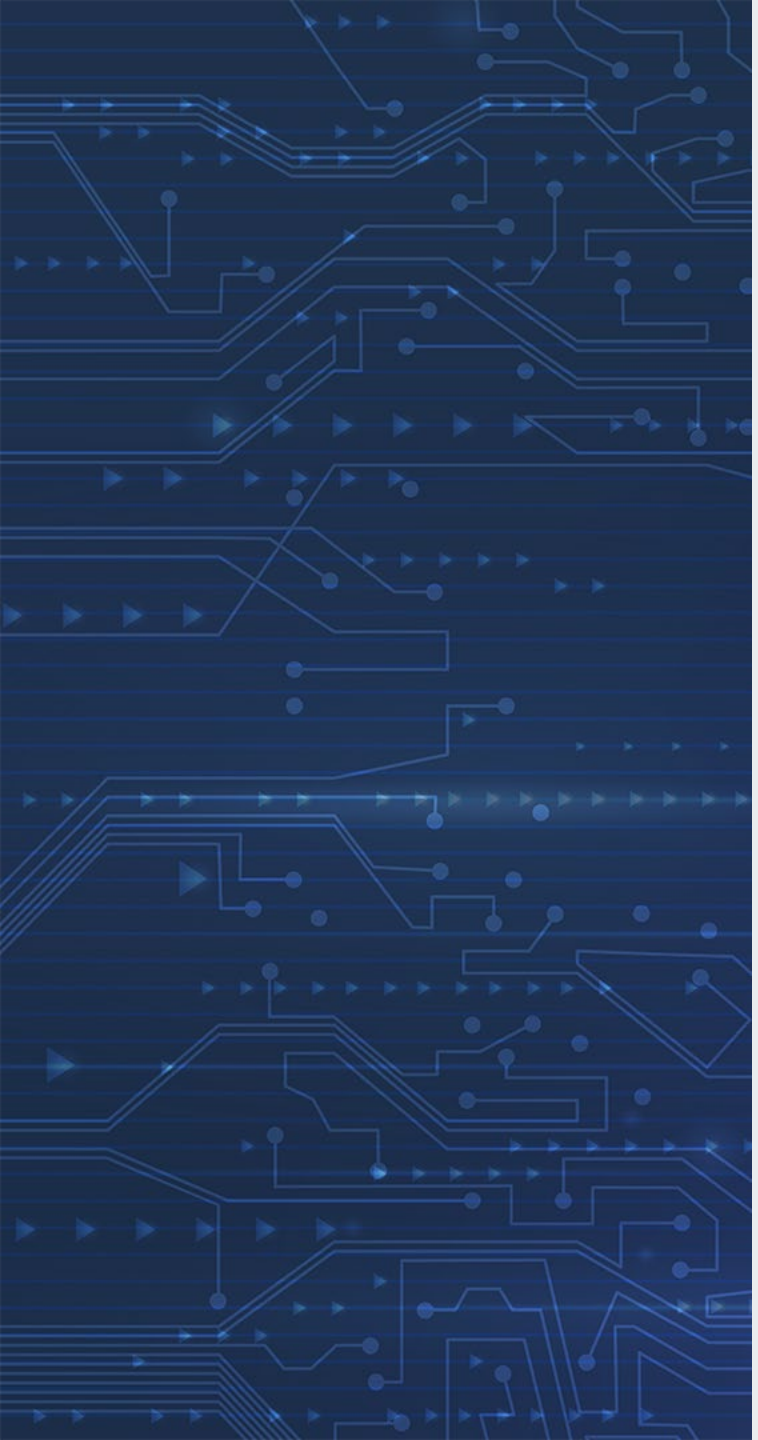
Image source: Intel

Example: [iPhones deployed for clinical communication and nursing care]

Security in Smart Hospitals

- As 5G (and future cellular generations) and Artificial Intelligence are components of smart hospitals, many of the security considerations that applied to those areas also apply to smart hospitals:
  - Confidentiality must be protected (large data repositories at rest and in motion)
  - Data pipes must be protected and resilient
- Inventory management will drive device security
  - Software/firmware updates
  - Security recalls
- Continuous monitoring will be critical
- Resilience will also be key
- Expanded attack surface

Image source: ENISA



Quantum Computing and Cryptography

The next evolution of processing for information systems will revolutionize cryptographic algorithms

Quantum Computing and Cryptography

- Quantum computing is expected to impact cryptography across industries in the next decade
- Protecting personal health information:
  - One report from Stanford University estimates a 48% growth in medical data each year
  - According to Politico, 50 million Americans had their sensitive health data breached in 2021
  - Stolen health records can be sold for as much as $1,000 each on the black market
- Health Insurance Portability and Accountability Act (HIPAA) cryptography requirements:
  - The HIPAA Security Rule requires healthcare entities to implement safeguards, such as encryption, that renders electronic Protected Health Information (ePHI) “unreadable, undecipherable or unusable” so that any “acquired healthcare or payment information is of no use to an unauthorized third party.”
- National Institute of Standards and Technology (NIST)
  - FIPS 140-2: Security Requirements for Cryptographic Modules
- AES 128, 192 and 256-bit encryption are commonly recommended standards

Quantum Computing, Cryptography and Security

- Quantum computing will result in a need to review and possibly update all cryptographic algorithms that are part of an information infrastructure
  - Quantum risk assessment:
    - How much data do you have?
    - What are the varying sensitivity levels of your data?
    - Where is it stored? How is that storage protected?
    - How long do you need to store/protect it? Legally? Operationally?
    - Who should have access to it?
      - Internal (employees, contractors, vendors, etc.)
      - External (patients, customers, etc.)
  - Which aspects of your operations are dependent on cryptography?
- HC3 presentation: https://www.hhs.gov/sites/default/files/quantum-cryptography-and-health-sector.pdf

Reference Materials

References

Artificial Intelligence

IBM: Artificial Intelligence
https://www.ibm.com/cloud/learn/what-is-artificial-intelligence

What is Artificial Intelligence? (John McCarthy, Stanford)
http://jmc.stanford.edu/articles/whatisai/whatisai.pdf

FDA: Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning - Based Software as a Medical Device - Discussion Paper and Request for Feedback
https://www.fda.gov/media/122535/download

Artificial Intelligence and Machine Learning in Software as a Medical Device
https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device

References

Smart Hospitals

“Smart Hospital Rooms” Powered by Alexa are Being Introduced in Many Healthcare Facilities
https://nurse.org/articles/Alexa-smart-hospital-rooms/

Siemens: Accelerating the digital transformation of hospitals
https://new.siemens.com/global/en/markets/healthcare/smart-hospitals.html

White paper: Smart, connected hospital framework
https://www.vocera.com/smart-connected-hospital

Pan American Health Organization: Smart Hospitals Toolkit
https://www.paho.org/en/health-emergencies/smart-hospitals/smart-hospitals-toolkit

Smart hospitals need to leverage data analytics
https://medcitynews.com/2022/03/smart-hospitals-need-to-leverage-data-analytics-for-better/

References

Smart Hospitals

Intel Digital Hospitals: Empowering the Transformation of the Healthcare Industry
https://www.intel.com/content/www/us/en/healthcare-it/resources/digital-hospital-whitepaper.html

How to create a smart hospital
https://blog.matchmore.io/how-to-create-a-smart-hospital/

As Hospitals Get Smart, Cybersecurity Challenges Will Increase
https://www.isaca.org/resources/isaca-journal/issues/2018/volume-3/as-hospitals-get-smart-cybersecurity-challenges-will-increase

ENISA: Smart Hospitals Security and Resilience for Smart Health Service and Infrastructures
https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals/at_download/fullReport

References

5G Cellular

5G-Enabled Health Technologies
https://mdic.org/program/5g-enabled-health-technologies/

5G Use in Healthcare: The Future is Present
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8764898/

5G IoT: Literally a Matter of Life or Death
https://threatpost.com/5g-iot-literally-a-matter-of-life-or-death/145161/

3GPP Approves Plans to Fast Track 5G NR
https://www.lightreading.com/mobile/5g/3gpp-approves-plans-to-fast-track-5g-nr/d/d-id/731018

5G Networks Spark Concerns For Enterprise Risks
https://threatpost.com/5g-networks-spark-concerns-for-enterprise-risks/145224/

References

Nanomedicine

ScienceDirect: Nanomedicine
https://www.sciencedirect.com/topics/pharmacology-toxicology-and-pharmaceutical-science/nanomedicine

Nanomedicine: the next breakthrough in oncology?
https://www.pharmatimes.com/magazine/2018/may_2018/nanomedicine_the_next_breakthrough_in_oncology

Nanomedicine refers to the use of nanomaterials and nanoscale devices for the treatment, diagnosis, monitoring, and control of diseases.
https://www.ais.science.vt.edu/academics/nanomedicine.html

Immunomodulating Nanomedicine for Cancer Therapy
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6238186/

References

Quantum Cryptography

Cryptographic Standards and Guidelines
https://csrc.nist.gov/Projects/cryptographic-standards-and-guidelines

NIST: Post-Quantum Cryptography Standardization
https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

How close are we to breaking encryption with quantum computing?
https://www.idginsiderpro.com/article/3532897/how-close-are-we-to-breaking-encryption-with-quantum-computing.html

Why Encryption is Essential in Healthcare Cybersecurity Strategies
https://www.healthitanswers.net/why-encryption-is-essential-in-healthcare-cybersecurity-strategies/

Cryptography safe for now, but urgent need to build quantum skills
https://www.zdnet.com/article/cryptography-safe-for-now-but-urgent-need-to-build-quantum-skills

Questions

FAQ

Upcoming Briefing

- September 22 – APT41 and Recent Activity

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are **highly encouraged** to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer

These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.

About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

Sector and Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

Alerts and Analyst Notes

Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings

Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Office of
Information Security
Securing One HHS

Health Sector Cybersecurity Coordination Center

Contacts

HHS.GOV/HC3

HC3@HHS.GOV