Data Security in Healthcare: Whatever Happened to Blockchain & the Emerging Impact of Artificial Intelligence

Matt Hustad, PharmD

PGY-2 Pharmacy Informatics Resident, HCA Healthcare

Preceptor: Amanda Foster, PharmD

Manager, Meditech/PK Systems Pharmacy

HCA Healthcare, ITG Product Development, Nashville, TN

HCA Healthcare®

Disclosure

- Neither the speaker nor his preceptor have relevant financial relationships with ineligible companies to disclose.
- This program may contain the mention of suppliers, brands, products, services, or drugs presented in a case study or comparative format using evidence-based research. Such examples are intended for educational and informational purposes and should not be perceived as an endorsement of any supplier, brand, product, service, or drug.
- The content presented is for informational purposes only & is based upon the presenter(s) knowledge & opinion. It should not be relied upon without independent consultation with & verification by appropriate professional advisors. Individuals & organizations shall have sole responsibility for any actions taken in connection with the content herein. HealthTrust, the program presenter(s) & their employers expressly disclaim any & all warranties as to the content as well as any liability resulting from actions or omissions of any individual or organization in reliance upon the content.

Learning Objectives for Pharmacists, Nurses, Supply Chain & Healthcare Executives

1. Recall fundamental concepts of data security related to healthcare
2. Recognize Blockchain concepts and data security considerations in healthcare
3. Identify Artificial Intelligence (AI) concepts and data security considerations for healthcare

Learning Objectives for Pharmacy Techs

1. Recall fundamental concepts of data security related to healthcare
2. Recognize Blockchain concepts and data security considerations in healthcare
3. Identify Artificial Intelligence (AI) concepts and data security considerations for healthcare

Data Fundamentals

- Stemming from the Latin word “datum” (‘something given”), **data** is an assortment of numbers, words, facts, or other useful information

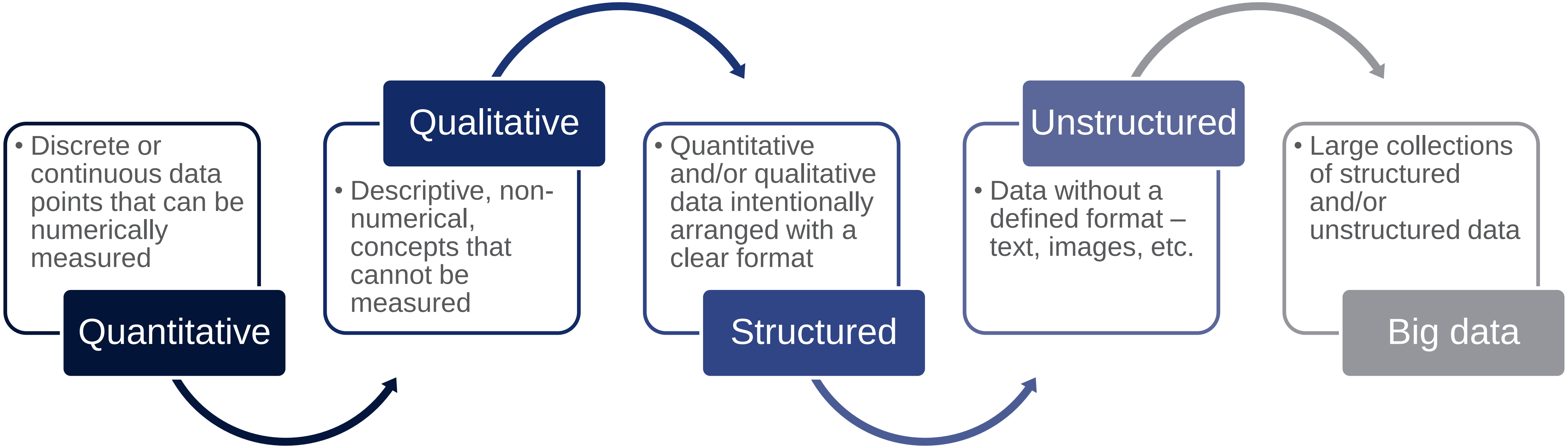
- Data is collected in various types, depending on the data characteristics, source, and format (qualitative vs quantitative, etc.)

- Increasing adaption of technology has led to massive increases of data generation, complexity, and importance

- Constant stream of data can be leveraged into useful insights, optimization, and predictions through data analytics

Source: Badman A, Kosinski M. What is data? IBM. https://www.ibm.com. Published October 1, 2024. Accessed January 7, 2025.

Data Types



Quantitative
- Discrete or continuous data points that can be numerically measured

Qualitative
- Descriptive, non-numerical, concepts that cannot be measured

Structured
- Quantitative and/or qualitative data intentionally arranged with a clear format

Unstructured
- Data without a defined format – text, images, etc.

Big data
- Large collections of structured and/or unstructured data

Source: Badman A, Kosinski M. What is data? IBM. https://www.ibm.com. Published October 1, 2024. Accessed January 7, 2025.

Data Fundamentals

Data Collection

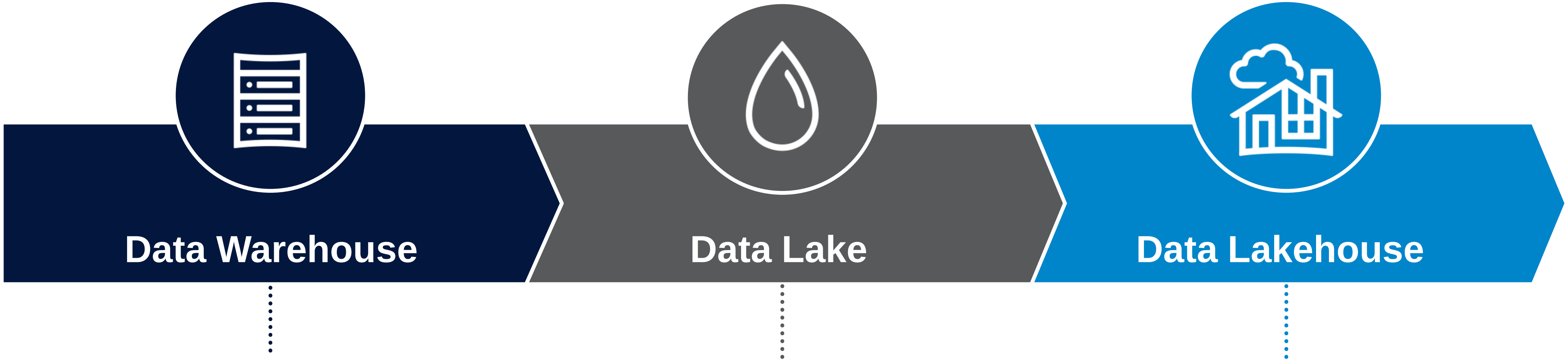
- Systematically gathering raw data from differing sources while ensuring data quality and integrity
- Raw data is cleaned and stored with ongoing quality analysis, assuring data is accurate and reliable

Data Management

- Collecting, processing, and leveraging data in a secure and optimal manner to drive outcomes
- Management systems, like data warehouses, aid in providing users access to stored data sets

Source: Badman A, Kosinski M. What is data? IBM. https://www.ibm.com. Published October 1, 2024. Accessed January 7, 2025.

Data Management Systems



Data Warehouse

Stores data from multiple sources that has been optimally structured, typically for analytics or data mining

Data Lake

Stores raw and unstructured data that could potentially be processed and analyzed

Data Lakehouse

Management solution which is able to handle both structured and unstructured

Source: Badman A, Kosinski M. What is data? IBM. https://www.ibm.com. Published October 1, 2024. Accessed January 7, 2025.

HITECH Act

- The Health Information Technology for Economic and Clinical Health Act of 2009 sought to increase the use of Electronic Health Records (EHRs) through financial incentives

- EHR adoption: 10-20% → 75% over 6 years
  - Internet: 10% → 75% over 18 years

- In 2018, Centers for Medicare & Medicaid Services (CMS) changed “Meaningful Use” to “Promoting Operability” in an effort to optimize data collection and submission

Source: Alder S. What is the Hitech Act? The HIPAA Journal. https://www.hipaajournal.com. Published December 5, 2024. Accessed January 7, 2025.

HITECH Act

- Additionally, the HITECH Act sought to increase compliance with HIPAA privacy and safety rules aimed at keeping health information confidential

- An amendment to HITECH in 2018 was aimed at improving healthcare collaboration through **improved data sharing** and easing HIPAA compliance burden

- HIPAA Safe Harbor law allows discretionary reduction or elimination of penalties if negligent party had **implemented appropriate security frameworks** prior to HIPAA violations associated with security (data breach, etc.)

Source: Alder S. What is the Hitech Act? The HIPAA Journal. https://www.hipaajournal.com. Published December 5, 2024. Accessed January 7, 2025.

Big Data in Healthcare

- Digitization and adoption of computers due to the HITECH Act has turned the healthcare system into a major driver of "**big data**", which is often defined by four Vs
  - **V**olume
  - **V**elocity – how quickly data is received and collected
  - **V**ariety – organized/unorganized, numbers, text, audio, video, transactions, logs
  - **V**eracity – consistency, accuracy, quality, and trust in data collected
- The vast amounts of data collected as "big data" surpass traditional storage, processing, and analytical technology, often requiring use of machine learning and artificial intelligence algorithms in management

Source: Dash S, Shakyawar SK, Sharma M, Kaushik S. Big Data in Healthcare: Management, analysis and future prospects. *J Big Data*. 2019;6(1).

Big Data in Healthcare

- **Clinical & medical data**
  - Electronic health records (EHRs)
    - Receive and collect data from connected technology (smart IV pumps, barcode scanning)
  - Electronic medical records (EMRs)
  - Personal health records (PHRs)
  - Medical practice management software (MPM)
  - Continuous monitoring devices

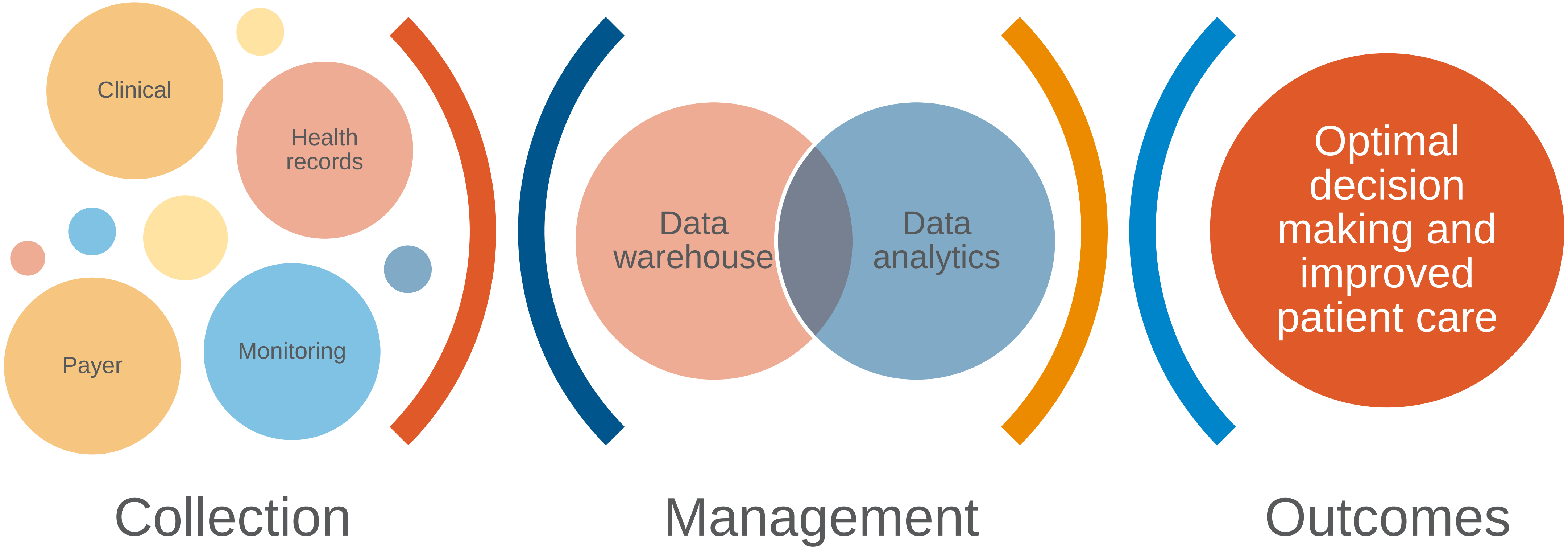
Source: Dash S, Shakyawar SK, Sharma M, Kaushik S. Big Data in Healthcare: Management, analysis and future prospects. *J Big Data*. 2019;6(1).

Big Data in Healthcare

- **Payer-provider data** is collected from the EMR, pharmacy prescriptions (e-prescribing and retail pharmacy software), and insurance records
- Wearable technology and mobile health (mHealth) generate large amounts of real-time **biomedical and patient health data**
- **Research data** (biomedical, genomics, pharmaceutical)

Source: Dash S, Shakyawar SK, Sharma M, Kaushik S. Big Data in Healthcare: Management, analysis and future prospects. *J Big Data*. 2019;6(1).

Using Healthcare Data



Data Protection

- **Privacy**
  - Policies and procedures that allow **personal control** over data, including how it is collected, stored, and used

- **Security**
  - Measures aimed at **protecting data** from unauthorized access
  - Information security, physical security, organizational policy

Source: Badman A, Kosinski M. What is data? IBM. https://www.ibm.com. Published October 1, 2024. Accessed January 7, 2025.

Knowledge Check #1

- What term refers to large, complex sets of data that are typically characterized by volume, velocity, and variety, and require advanced tools for processing and analysis?

  A. Data Warehouse

  B. Big Data

  C. Machine Learning

  D. Quantitative Data

Knowledge Check #1: Correct Response

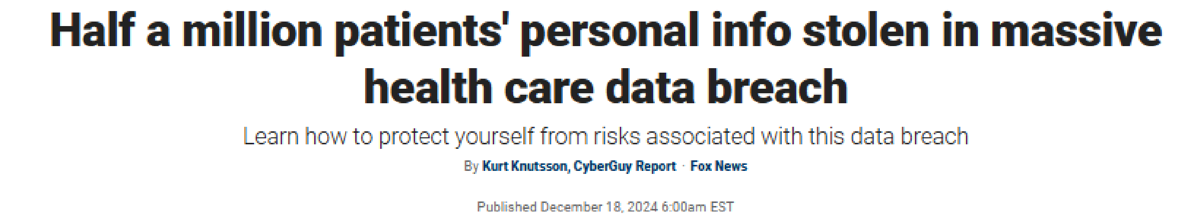
- What term refers to large, complex sets of data that are typically characterized by volume, velocity, and variety, and require advanced tools for processing and analysis?

A. Data Warehouse

B. Big Data ← Correct Response

C. Machine Learning

D. Quantitative Data

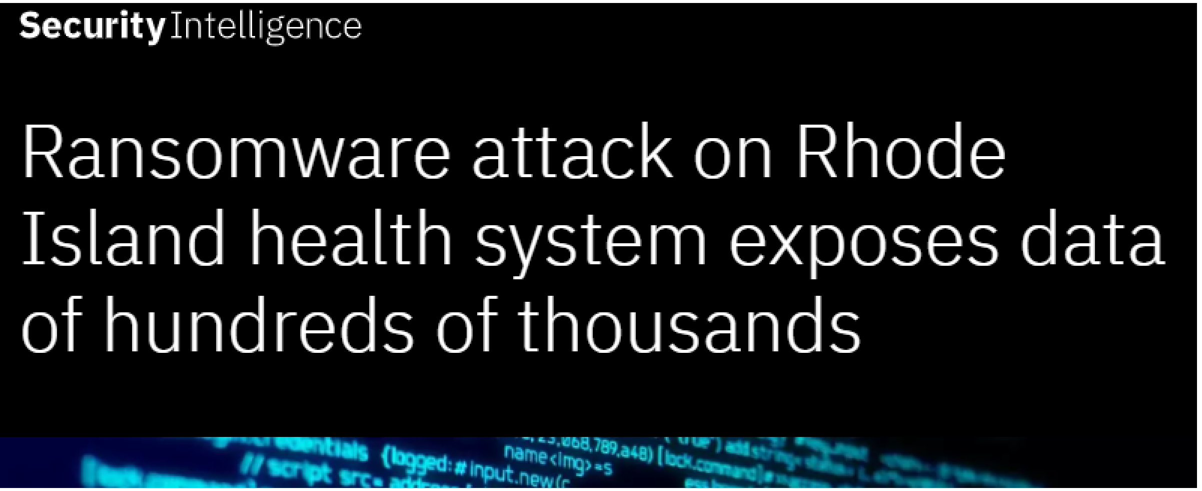


Half a million patients' personal info stolen in massive health care data breach

Learn how to protect yourself from risks associated with this data breach

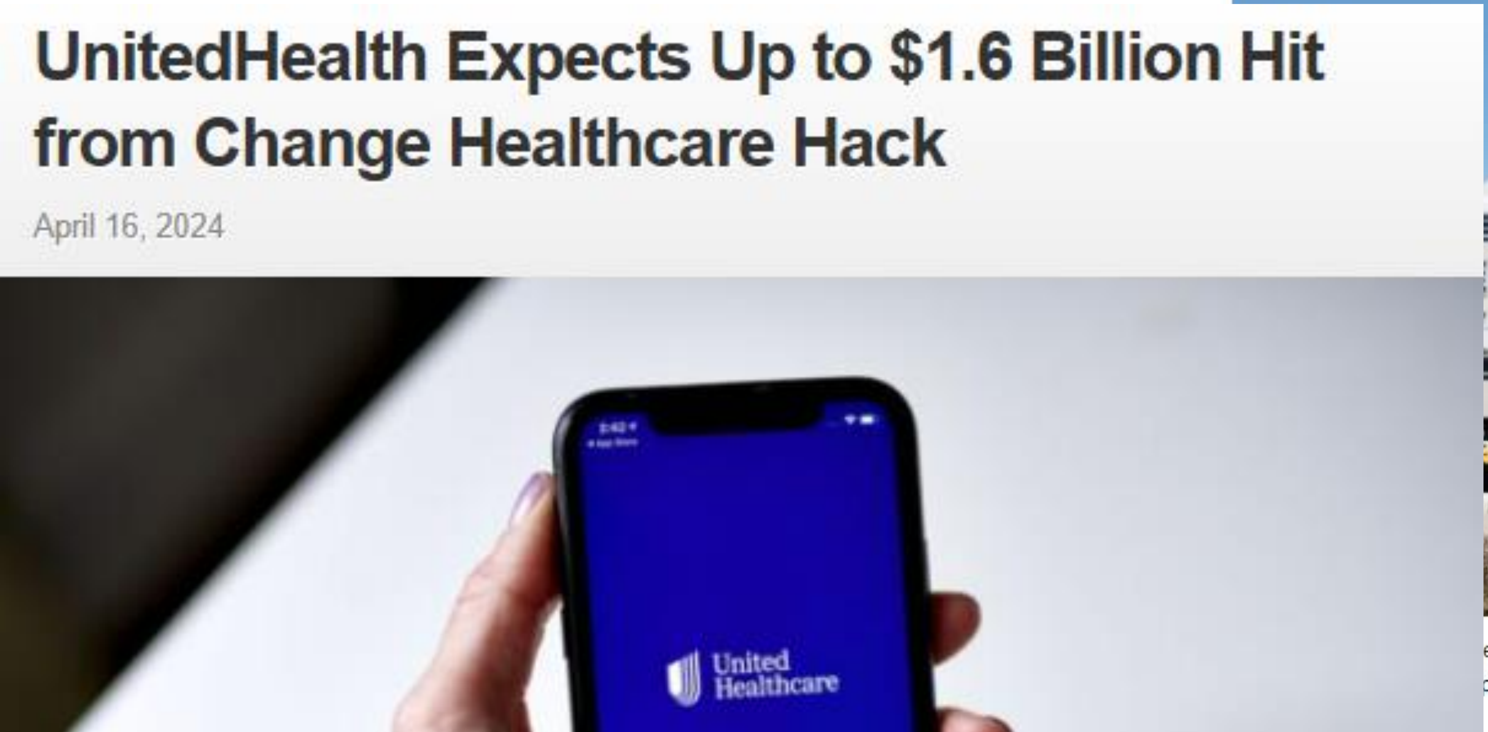
By Kurt Knutsson, CyberGuy Report · Fox News

Published December 18, 2024 6:00am EST



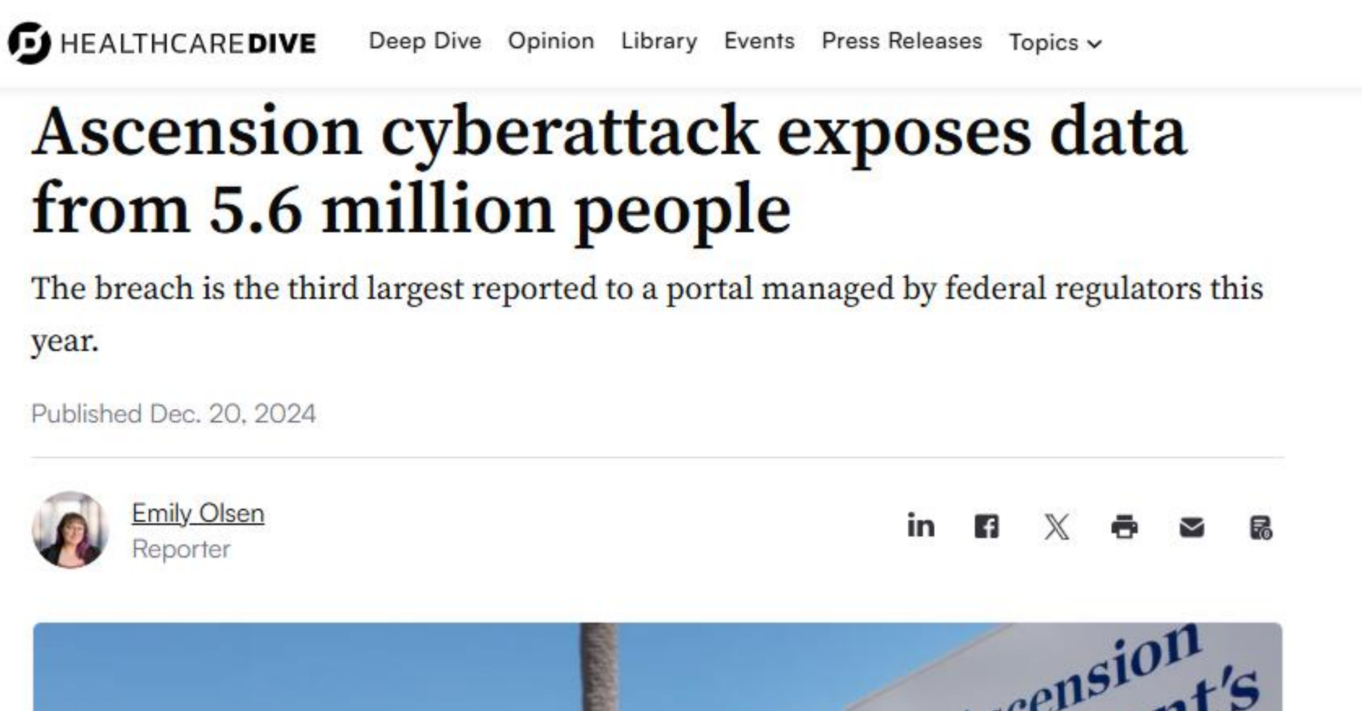
SecurityIntelligence

Ransomware attack on Rhode Island health system exposes data of hundreds of thousands



UnitedHealth Expects Up to $1.6 Billion Hit from Change Healthcare Hack

April 16, 2024



Ascension cyberattack exposes data from 5.6 million people

The breach is the third largest reported to a portal managed by federal regulators this year.

Published Dec. 20, 2024

Emily Olsen
Reporter

ension St. Vincent's Riverside Hospital on March 14, 2020 in Jacksonville, Florida. Data from nearly
posed after a ransomware attack on Ascension this spring. *Cliff Hawkins via Getty Images*

Healthcare Data Breaches

- Illegitimate access or disclosure of protected health information (PHI) that compromises the privacy and security of the data
- Despite advantages of increased use of technology and digitization in healthcare, patient digital health data is increasingly at risk
- From 2005 to 2019, there was **3912 confirmed healthcare data breaches**
  - ~43% of all health data was compromised during this time
- Average costs of a healthcare data breach were **up to $6 million** in 2020
- Effective prevention and data security are becoming increasingly important as healthcare data generation continues to grow

Source: Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: Insights and implications. *Healthcare (Basel)*. 2020;8(2):133.

Healthcare Data Threats

Hacking Incidents

Most common healthcare data breach

- Cyber-attacks used to gain unauthorized confidential health data access
- Ransomware, malware – malicious software

Unauthorized Access / Internal Disclosure

- Attacks aided by an internal organization source that leads to exposure of confidential health data
- Unauthenticated access, privilege abuse, social engineering

Improper Data Disposal

- Exposure of unnecessary but still confidential health data

Physical Theft or Loss

Source: Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: Insights and implications. *Healthcare (Basel)*. 2020;8(2):133. doi:10.3390/healthcare8020133

Data Security Types

Encryption

- Algorithms encode sensitive information into random meaningless and unreadable formats
- Encryption keys allow authorized users to access and read the previously scrambled data
- **Key management** secures cryptographic keys by controlling their generation, exchange, storage, deletion and any updates
  - Ensures users have the correct keys when needed, while also allowing organizations to track who has access to what

Source: What is data security? IBM. https://www.ibm.com. Accessed January 7, 2025.
Vaideeswaran N. What is data security? Crowdstrike. https://www.crowdstrike.com. Published September 18, 2023. Accessed January 7, 2025

Data Security Types

Data erasure

- Permanent removal of data sets no longer required on a storage device
- **Overwriting** ensures data is unrecoverable
- Better than standard data wiping

Data masking

- **Obscuring and/or replacing** specific data points to renders data useless to any unauthorized users
- Data is still accessible by authorized users

Data resiliency

- Creation of **data backup copies** that allow organizations to recover damaged, deleted, or stolen data
- **Reduce downtime** during and after cyberattacks

Source: What is data security? IBM. https://www.ibm.com. Accessed January 7, 2025.
Vaideeswaran N. What is data security? Crowdstrike. https://www.crowdstrike.com. Published September 18, 2023. Accessed January 7, 2025

Key Data Security Components

Access Control and the Principle of Least Privilege (POLP)

Cloud Data Security

Data Loss Prevention (DLP)

Email Security

Source: What is data security? IBM. https://www.ibm.com. Accessed January 7, 2025.
Vaideeswaran N. What is data security? Crowdstrike. https://www.crowdstrike.com. Published September 18, 2023. Accessed January 7, 2025

Key Data Security Components

Governance, Risk, and Compliance (GRC)

Password Hygiene

Authentication & Authorization

Zero Trust

Source: What is data security? IBM. https://www.ibm.com. Accessed January 7, 2025.
Vaideeswaran N. What is data security? Crowdstrike. https://www.crowdstrike.com. Published September 18, 2023. Accessed January 7, 2025

Data Security Best Practices

- Authenticate identities using multi-factor authentication (MFA) or other methods to verify and access management
- Regularly back up data to minimize disruptions and prevent data loss
- Implement endpoint security to protect devices with detection and response tools to mitigate risks and prevent cyberattacks
- Educate employees on cybersecurity policies, threats, and best practices to avoid data breaches

Source: What is data security? IBM. https://www.ibm.com. Accessed January 7, 2025.
Vaideeswaran N. What is data security? Crowdstrike. https://www.crowdstrike.com. Published September 18, 2023. Accessed January 7, 2025

Data Security Best Practices

- Create data security clear policies outlining roles, access levels, and incident response procedures
- Secure connected devices like laptops, phones, and Internet of Things (IoT) devices like printers and Bluetooth devices from attacks
- Secure cloud environments with robust measures and reinforce physical on-premises data from intruders and hazards

Source: What is data security? IBM. https://www.ibm.com. Accessed January 7, 2025.
Vaideeswaran N. What is data security? Crowdstrike. https://www.crowdstrike.com. Published September 18, 2023. Accessed January 7, 2025

Healthcare Data Security Considerations

- **Authentication** is important for verifying users are who they are pretending to be at the entry of every access
- **Encryption** is effective at preventing unauthorized access of protected health data, schemes should be efficient, easy to use by end users (healthcare professionals and patients), and adaptable to new EHRs
- **Data masking** is cost-effective and useful tool in de-identifying sensitive data sets or masking PHI, especially for live data anonymization
- Appropriate **access control** in conjunction with authentication and POLP
- Continual security **monitoring** to catch intrusions

Source: Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. *J Big Data*. 2018;5(1):1.

Healthcare Data Security Considerations

- **mHealth** application security should be enhanced through the use of appropriate encryption along with secure storage and robust data backups

- With the increasing push for **interoperability**, it is necessary to standardize secure data sharing protocols and formats

- Secure **data storage** preserves patient data integrity, accuracy, and privacy, supporting critical medical decisions while fostering compliance, reducing costs, and building trust in healthcare organizations

Source: Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and privacy of technologies in health information systems: a systematic literature review. *Computers*. 2024;13(2):41.

Knowledge Check #2

- What term refers to the process of algorithms converting information or data into an unreadable format that prevents access to unauthorized users without the correct key?

A. Data erasure

B. Data masking

C. Authentication

D. Encryption

Knowledge Check #2

- What term refers to the process of algorithms converting information or data into an unreadable format that prevents access to unauthorized users without the correct key?

A. Data erasure

B. Data masking

C. Authentication

D. Encryption

Correct Response

Pharmacy Data

- Pharmacy departments generate **large volumes of diverse and distinctive data sets**, as operations include multiple integral and complex processes – like the medication-use process – which include both business and clinical decision making

- Analytics requires utilizing financial information, medication utilization, and activity-based cost analysis that can provide insights which impact health outcomes, medication adherence, and effective disease management

Source: Wolfe A, Hess L, La MK, et al. Strategy for Pharmacy Data Management. *AJHP*. 2017;74(2):79-85.

ASHP Policy 2413: Role of AI in Pharmacy Practice

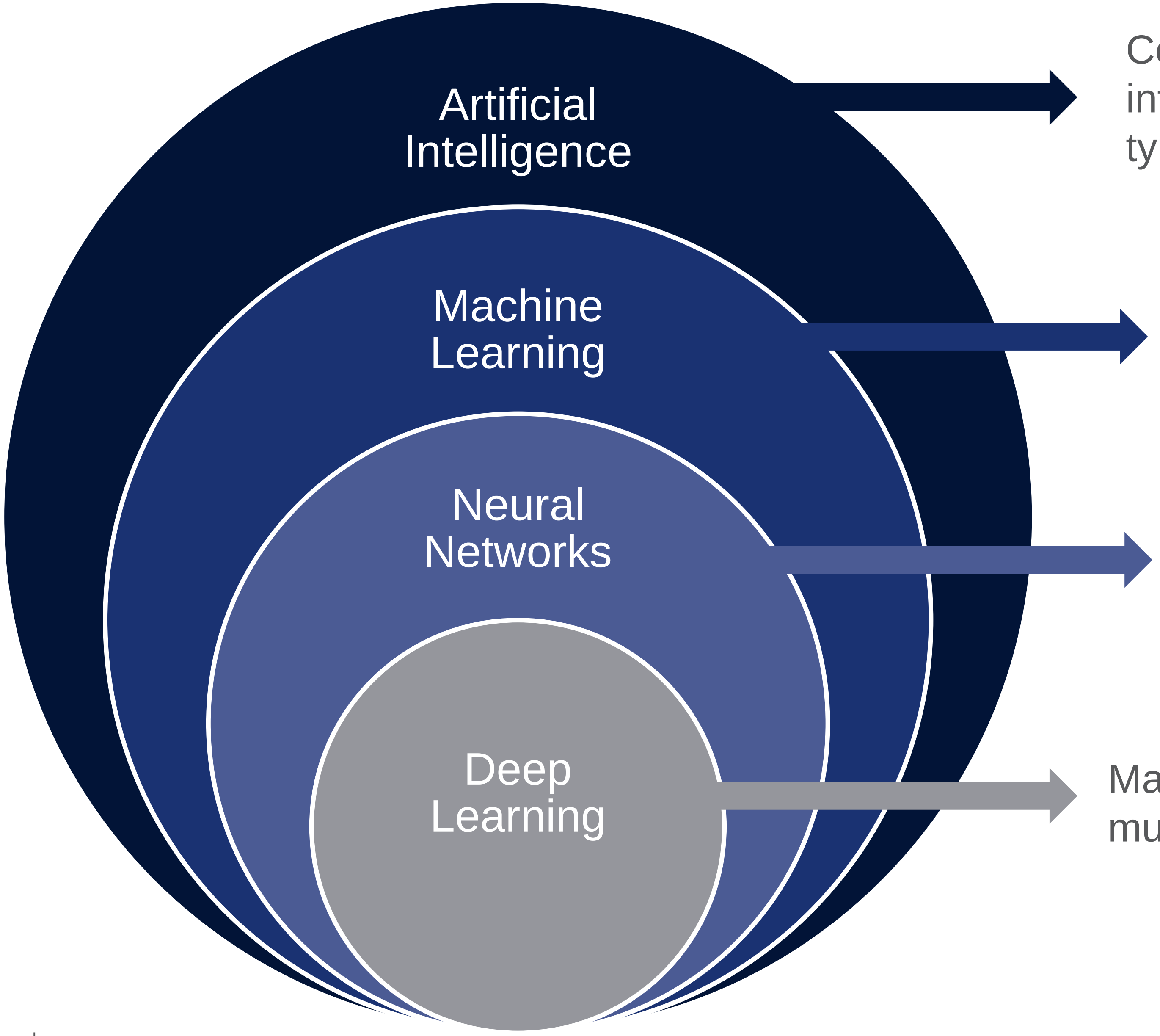
1. To embrace artificial intelligence (AI) as a tool with tremendous potential to improve patient care and the medication-use process through the enhancement of pharmacy practice
2. To recognize that AI technologies offer innovative ways to gather clinical knowledge, assist learners, enhance educational experiences, and streamline administrative processes
3. To advocate for standards, policies, and procedures that permit the use of AI in circumstances in which it has proven safe and effective as an augmentation of pharmacy services and to ensure safeguards along with its implementation

Source: Professional policies approved by the 2024 ASHP house of delegates. American Journal of Health-System Pharmacy. 2024;81(22):1205-1207.

ASHP Policy 2413: Role of AI in Pharmacy Practice

4. To encourage the adoption of policies regarding the use of AI and ongoing surveillance of these tools to maintain professional integrity
5. To advocate for pharmacy workforce involvement and transparency in the decision-making, design, validation, implementation, and ongoing evaluation of AI-related applications and technologies
6. To recognize that ethical considerations must guide the development and use of AI in pharmacy practice, and to oppose any use of AI that compromises human interaction or replaces ethical decision-making, professional judgment, critical thinking, or the safety and effectiveness of pharmacy services

Source: Professional policies approved by the 2024 ASHP house of delegates. American Journal of Health-System Pharmacy. 2024;81(22):1205-1207.



Computer systems mimicking human intelligence and performing tasks typically done by humans

Improvement of AI algorithm programming without additional human data input

Mimic biological neuron signaling by processing information through layers of connected nodes

Machine learning net generation allows for multiple learning layers from different datasets

Source: Kumar M, Nguyen TPN, Kaur J, et al. Opportunities and challenges in application of artificial intelligence in pharmacology. *Pharmacol Rep*. 2023;75(1):3-18

Artificial Intelligence Overview

Generative AI

- Subset of AI that focuses on creating new content, data, or outputs, that resembles human-generated outputs
- Sophisticated machine learning models and deep learning models generate original and realistic content from existing data

Large Language Models

- Deep learning models pre-trained with large amounts of data
- Underlying neural networks extract meaning from sequences of text, understanding relationships between words and phrases
- OpenAI’s GPT series, Google Gemini

Source: Craig L. Compare large language models vs. generative AI. TechTarget. https://www.techtarget.com. Published February 29, 2024. Accessed January 7, 2025

Artificial Intelligence in Healthcare

1 Patient Facing

- Wearables
- Genomics
- AI-powered Chatbots
- Mental health

2 Telehealth

- Disease management
- Lifestyle management
- Tele-medicine

3 Provider Facing

- Medical imaging
- Data analytics
- Multi-modal medical data

4 Research

- Drug discovery
- Clinical trial optimization
- Genetic research

Source: Khalid N, Qayyum A, Bilal M, Al-Fuqaha A, Qadir J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Comput Biol Med*. 2023;158:106848.

AI Data Privacy Risks

- AI has been shown to successfully increase potential **re-identification** of patients in previously de-identified data sets
  - AI and ML algorithms can be leveraged by hackers during data breaches
  - Successful even when data is anonymized and identifiers purged
- Machine learning algorithms and AI reasoning are obscured to human users (“**black box**”)
- Training AI algorithms requires vast quantities of potentially sensitive patient data
- Data integrity and bias
- Inadvertent disclosure

Source: Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Med Ethics*. 2021;22(1):122.

AI Data Privacy Challenges

Adaptability

- Privacy-preserving ML techniques are specific to particular ML algorithms – new algorithms require new techniques

Scalability

- As ML advances, excessive computational power and costs to ensure algorithm privacy become a bigger limitation for use

Legibility

- Informing data owners of data collection and data privacy protection measures

Authentication and access control

Source: Khalid N, Qayyum A, Bilal M, Al-Fuqaha A, Qadir J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Comput Biol Med*. 2023;158:106848.

AI Data Privacy Challenges

Data integrity

- Data poisoning attacks can result in inaccurate AI output

Robustness

- Mechanisms to protect healthcare data from tampering

Privacy vs. Utility

- Disclosing de-identified data that is accurate also avoiding prejudice

Ethics

- Ensuring AI algorithms are fair, unbiased, and transparent
- Respecting patient data confidentiality can negatively affect ML model performance

Source: Khalid N, Qayyum A, Bilal M, Al-Fuqaha A, Qadir J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Comput Biol Med*. 2023;158:106848.

AI Bias

- AI systems can perpetuate and amplify human biases present in their training data, leading to unfair outcomes
- Biases can originate from various stages, including data collection, algorithm design, and deployment
- Addressing potential AI bias
  - Diversify training data to ensure datasets are representative and minimize inherent biases
  - Developing interpretable models to highlight background decision-making processes and provide algorithmic transparency
  - Regular audits for detection and correction of biases in AI systems

Source: Manyika J, Silberg J, Presten B. What Do We Do About the Biases in AI? Harvard Business Review. HBR.org. Published October 25, 2019. Accessed January 7, 2025.

AI Ethics Considerations

- Increasing use of AI in healthcare requires that models are morally accountable
- Essential to ensure AI models are created ethically and with un-biased data
- Responsible AI includes transparent, explainable, and accountable systems
- No standardized guidelines for moral use of AI in healthcare
- Absent legal repercussions on the machine means the responsibility borne by users

Source: Naik N, Hameed BMZ, Shetty DK, et al. Legal and ethical consideration in artificial intelligence in healthcare: who takes responsibility? *Front Surg*. 2022;9:862322.
Khan B, Fatima H, Qureshi A, et al. Drawbacks of artificial intelligence and their potential solutions in the healthcare sector. *Biomedical Materials & Devices*. 2023;1(2):731-738.

Knowledge Check #3

- Which of the following is a data security concern that is associated with the use of Artificial Intelligence (AI) and patient health information (PHI)?

A. Algorithmic bias

B. Black box

C. Re-identification

D. Data resiliency

Knowledge Check #3

- Which of the following is a data security concern that is associated with the use of Artificial Intelligence (AI) and patient health information (PHI)?

A. Algorithmic bias

B. Black box

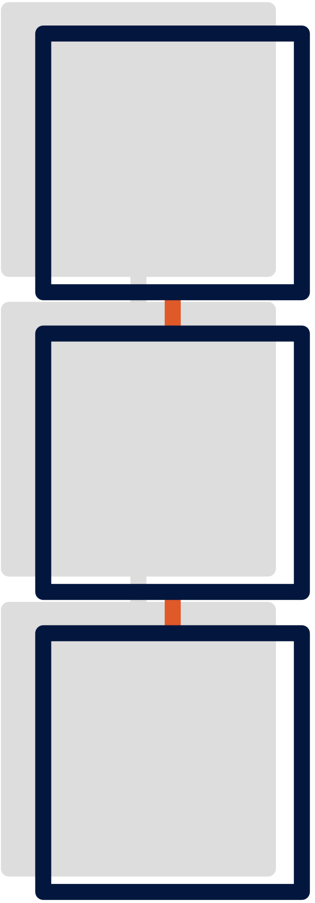
C. Re-identification

Correct Response

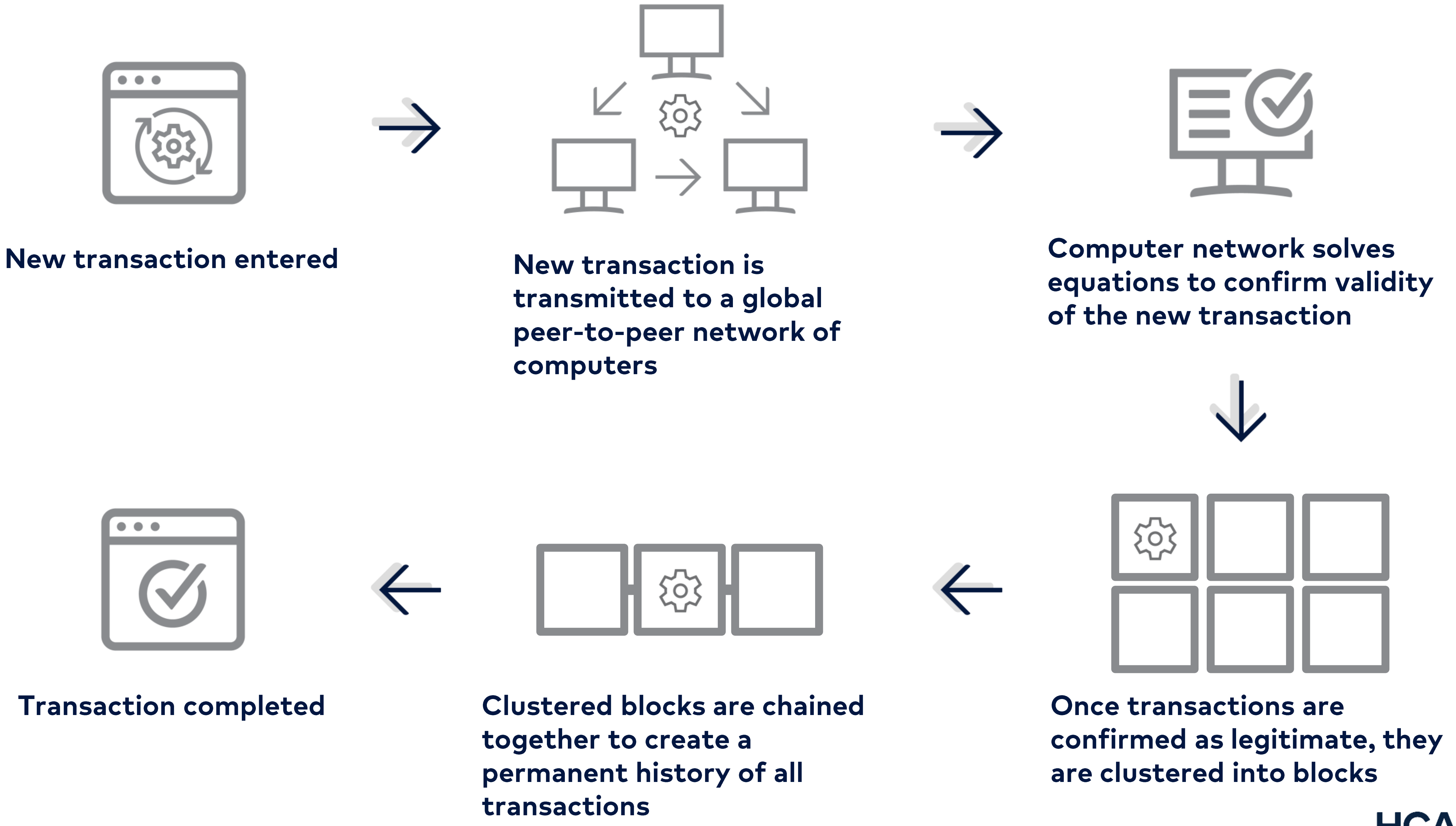
D. Data resiliency

Blockchain

- Decentralized transparent ledger, containing transaction records within a set of data blocks
- Blocks contains data on multiple transactions and as each block is added, the ledger comprises a complete and transaction history. Once a block is stored in the ledger, the information is permanent
- **Public permissionless blockchains** are decentralized and open, allowing any user to join or leave the network
  - No authority monitors and there is no network owner
- **Private permissionless blockchains** limit authorized readers and writers
  - Centralized authority assigns user access



Source: El-Gazzar R, Stendal K. Blockchain in health care: hope or hype? *J Med Internet Res*. 2020;22(7):e17199.



New transaction entered

New transaction is transmitted to a global peer-to-peer network of computers

Computer network solves equations to confirm validity of the new transaction

Once transactions are confirmed as legitimate, they are clustered into blocks

Clustered blocks are chained together to create a permanent history of all transactions

Transaction completed

Source: Hayes A. Blockchain facts: what is it, how it works, and how it can be used. Investopedia. Investopedia.com. Updated September 16, 2024. Access January 7, 2025

Early Blockchain Healthcare Potential

- Belief in blockchain immunity to data security threats
- Immutability of transaction history
- Empowering patients with self-sovereignty and management of their personal patient-generated health data
- Decentralized storage of complete patient health information that is shared and accessible to all parties involved in the patient care process
- Accelerating research through sharing of anonymized patient data
- Advanced health data ledgers that can maintain clinical transaction logs and support pharmacy supply chains

Source: El-Gazzar R, Stendal K. Blockchain in health care: hope or hype? *J Med Internet Res*. 2020;22(7):e17199.

Early Blockchain Healthcare Challenges

- While blockchain can guarantee data integrity, the background calculations for a single block in the chain are time and energy consuming
- Complex or computation-intense systems are not ideal cases for blockchain, but performance, real-time data exchange and communication, and medical service availability are critical to patient care
- Limited interoperability and scalability
- Distributed Denial-of-Service (DDoS) attacks are likely to occur for a blockchain designed to handle large amounts of data
- Adequate compliance with General Data Protection Regulation (GDPR) requirements

Source: El-Gazzar R, Stendal K. Blockchain in health care: hope or hype? *J Med Internet Res*. 2020;22(7):e17199.

Blockchain in Current Research

- Blockchain-based frameworks have been shown improve interoperability and access to quality data used for **Medication Reconciliation**
- Ensures immutable and secure log management for more efficient **auditing** and **error detection**
- Can provide **secure patient monitoring** with IoT devices such as wearables and sensors
- Enhancement of **pharmaceutical supply chain management** by preventing counterfeit drugs, ensuring data integrity, and enabling transparent tracking across stakeholders from manufacturing to patient delivery

Source: Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. *Systems*. 2023;11(1):38.

Ongoing Challenges with Blockchain

Scalability

- Increasing users and devices run into processing limits, high computing demands, costly infrastructures, and transaction volumes that validation times are unable to match

Privacy

- Secure frameworks that prevent unauthorized access but allowing efficient data sharing
- Each new patient added to blockchain networks involves complex verification

Interoperability

- Lack of mechanisms used for data sharing, analysis, and EHR integration
- An overhaul of current EHRs and databases to support decentralized blockchain structures

Source: Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. *Systems*. 2023;11(1):38.

Blockchain Security Considerations

- 51% Attacks – high risk to blockchain systems, allowing attackers the possibility of modifying an entire blockchain
  - One entity owns 51% or more of the blockchain network computing, allowing transaction reversal and blocking of new transaction
- Sybil Attacks – hackers flood networks with fake nodes to disrupt transactions
- Phishing Attacks – target users' credentials through fake links

Source: Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. *Systems*. 2023;11(1):38.

Blockchain Security Considerations

- Routing Attacks – hackers intercept data sent to internet-service providers (ISPs), risking exposure of confidential assets
- Private Key Security Attacks – poor cryptographic implementations risk exposing private keys
- Endpoint Vulnerabilities – hackers exploit user devices to steal keys

Source: Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. *Systems*. 2023;11(1):38.

Future Blockchain Research

- Addressing workarounds, system security, **interoperability**, and access management issues in blockchain implementation
- Development of legally and ethically acceptable electronic healthcare **ecosystems** with robust data authentication processes
- Blockchain system **architecture optimization** to improve efficiency and performance with ever increasing transaction volume demand
- Managing patient **privacy** through compliance with standards like HIPAA
- Blockchain implementation with prescription drug administration and prescription fraud prevention

Source: Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. *Systems*. 2023;11(1):38.

Knowledge Check #4

- What cyberattack targeting blockchain allows for hackers to potentially modify data in an entire blockchain?

A. 51% Attack
B. Phishing
C. Distributed Denial of Service (DDoS)
D. Malware

Knowledge Check #4

- What cyberattack targeting blockchain allows for hackers to potentially modify data in an entire blockchain?

Correct Response

A. **51% Attack**

B. Phishing

C. Distributed Denial of Service (DDoS)

D. Malware

Healthcare is a large contributor of the ever increasing generation and collection of data

Effective data security is necessary to prevent data breaches and protect patient health information

Use of AI in healthcare requires ethical and secure frameworks to prevent compromising patient data

Adoption of blockchain in healthcare slowed by scalability, security, and interoperability challenges

References

1. Badman A, Kosinski M. What is data? IBM. https://www.ibm.com. Published October 1, 2024. Accessed January 7, 2025.
2. Alder S. What is the Hitech Act? The HIPAA Journal. https://www.hipaajournal.com. Published December 5, 2024. Accessed January 7, 2025.
3. Dash S, Shakyawar SK, Sharma M, Kaushik S. Big Data in Healthcare: Management, analysis and future prospects. *J Big Data*. 2019;6(1).
4. Wolfe A, Hess L, La MK, et al. Strategy for Pharmacy Data Management. *AJHP*. 2017;74(2):79-85.
5. Seh AH, Zarour M, Alenezi M, et al. Healthcare data breaches: Insights and implications. *Healthcare (Basel)*. 2020;8(2):133.
6. What is data security? IBM. https://www.ibm.com. Accessed January 7, 2025.
7. Vaideeswaran N. What is data security? Crowdstrike. https://www.crowdstrike.com. Published September 18, 2023. Accessed January 7, 2025
8. Abouelmehdi K, Beni-Hessane A, Khaloufi H. Big healthcare data: preserving security and privacy. *J Big Data*. 2018;5(1):1.
9. Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and privacy of technologies in health information systems: a systematic literature review. *Computers*. 2024;13(2):41.
10. Professional policies approved by the 2024 ASHP house of delegates. American Journal of Health-System Pharmacy. 2024;81(22):1205-1207.
11. Kumar M, Nguyen TPN, Kaur J, et al. Opportunities and challenges in application of artificial intelligence in pharmacology. *Pharmacol Rep*. 2023;75(1):3-18
12. Craig L. Compare large language models vs. generative AI. TechTarget. https://www.techtarget.com. Published February 29, 2024. Accessed January 7, 2025
13. Khalid N, Qayyum A, Bilal M, Al-Fuqaha A, Qadir J. Privacy-preserving artificial intelligence in healthcare: Techniques and applications. *Comput Biol Med*. 2023;158:106848.
14. Murdoch B. Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Med Ethics*. 2021;22(1):122.
15. Manyika J, Silberg J, Presten B. What Do We Do About the Biases in AI? Harvard Business Review. HBR.org. Published October 25, 2019. Accessed January 7, 2025.
16. Naik N, Hameed BMZ, Shetty DK, et al. Legal and ethical consideration in artificial intelligence in healthcare: who takes responsibility? *Front Surg*. 2022;9:862322.
17. Khan B, Fatima H, Qureshi A, et al. Drawbacks of artificial intelligence and their potential solutions in the healthcare sector. *Biomedical Materials & Devices*. 2023;1(2):731-738.
18. El-Gazzar R, Stendal K. Blockchain in health care: hope or hype? *J Med Internet Res*. 2020;22(7):e17199.
19. Hayes A. Blockchain facts: what is it, how it works, and how it can be used. Investopedia. Investopedia.com. Updated September 16, 2024. Access January 7, 2025
20. Ghosh PK, Chakraborty A, Hasan M, Rashid K, Siddique AH. Blockchain application in healthcare systems: a review. *Systems*. 2023;11(1):38.

Thank you!!

Matt Hustad, PharmD

PGY-2 Pharmacy Informatics Resident, HCA Healthcare

Matthew.Hustad@hcahealthcare.com