As part of the Health Care Trends series, in this course you will learn about trends on data analysis and security. The course also posits projected impacts of these trends.

Questions or comments? Contact us [here](#).

**Instructions:** Click **Start** above or navigate to a section below to begin.

**LEARN**

- Introduction
- Data Analysis
- Data Security
- Predicted Impacts

**APPLY YOUR KNOWLEDGE**

- Knowledge Check
Learning Objectives

After completing this course, you will be able to:

1. Describe the types and qualities of medical data, capabilities of data analysis and impediments to data quality and analytics, and efforts underway to make use of the vast amount of data being produced.

2. Recognize the importance of cybersecurity and what it encompasses, methods for improving cybersecurity practices, and the prevalence of cyberattacks and data breaches.

3. Explain predicted impacts of data analysis and security trends for patients, physicians and payers.
What is Data Analysis?

Data analysis refers to the process by which data are systematically examined in order to spotlight useful information.

The process of data analysis includes the following steps:

1. **Identify objectives:** Before data are collected, objectives are determined and key metrics or performance indicators are identified, so that it will be possible to measure progress toward those objectives.
Health Informatics and Categories of Health Care Data

Health Informatics (HI) refers to an interdisciplinary field that uses information technology to organize and analyze health records to improve healthcare outcomes.

The following types of data are among the most significant to health informatics:

Instructions: Click each tab below to learn more.
As organizations provide clinical care, they can collect data about which of their services are being used and how these services are being paid for. These data are often collected at an individual patient level based on claims, patient encounters or enrollment in wellness programs, and might include information such as types of service and length of stay. These data can help health organizations better understand the specific needs of the populations they serve and properly distribute resources.

Electronic health records (EHRs) contain an individual’s clinical history. These records are created and kept current through the input of physicians and other members of the care team. Physicians can use EHRs to more acutely treat individual patients, and specialists and other providers may also use them to share information, ensuring a comprehensive picture of a patient’s health history and needs.

Some health organizations are required to report standardized clinical data, which may be used by Medicare or other regulatory agencies to assess needs and make adjustments to resource allocation. These data can also enable facility-specific performance assessments.
Organizations can look at information and trends in insurance claims data, providing insights into the kinds of services patients are seeking. These data can also be used to identify overused or expensive treatments that could be replaced with something more efficient.

Health care organizations can survey their patients, asking them to assess their care experiences. While this information is often more qualitative than quantitative, it can still provide clinicians and administrators with insight that can be used to improve processes.

Sources: https://www.northeastern.edu/graduate/blog/what-is-health-informatics/

https://healthinformatics.uic.edu/blog/types-of-data/

Patient Generated Health Data

The Office of the National Coordinator for Health Information Technology defines patient-generated health data (PGHD) as “health-related data—including health history, symptoms, biometric data, treatment history, lifestyle choices, and other information—created, recorded,
gathered, or inferred by or from patients or their designees (i.e., care partners or those who assist them) to help address a health concern.”

PGHD can **improve efficiency of physician visits** by offsetting administrative tasks that would otherwise have to be completed by providers and support staff. However, the quality and reliability of the PGHD data sources vary, and engagement among patients also can vary based on patient health, technological literacy and concerns about privacy and security.


**Difficulties in Health Care Data**

The volume of health care data is projected to grow faster than other industries through 2025. Over that period, researchers expect health care data to experience a **compound annual**
growth rate (CAGR) of 36%, significantly higher than the manufacturing industry (30% CAGR), financial services data (26%) and the media and entertainment industry (25%).

Aside from the pure volume of data being created, a number of difficulties contribute to making health data unique and difficult to manage. A report by Health Catalyst outlines some of these difficulties:

Instructions: Click each plus sign below to learn more about these difficulties.

---

**Data are in multiple places.**

Be they different EHRs or software systems, or different departments within an organization, data often reside in different locations and different formats.

---

**Data are structured and unstructured.**

Structured data are generally highly organized, easy to include in databases and searchable (e.g. names, addresses, isolated lab values). Unstructured data, which by some estimations make up about 80% of all data in health care, are the opposite: highly unorganized and typically requiring human interpretation (e.g. text requiring contextual analysis, X-rays, sonograms). EHRs attempt to standardize data capture in order to make data more structured, but for physicians, one-size-fits-all approaches tend to be inadequate and frustrating.

---

**Definitions are inconsistent.**

Variable definitions of health care data and constant discoveries and newly agreed-upon knowledge make the consistent definition and collection of health care data an evolving challenge.
Data are complex.

Data of different types (e.g. claims data, EHR data) and from different systems offer **varying levels of detail and completeness**. Data from individual systems are unique, complex and often do not interact with one another. Managing these various data and making them actionable across populations requires tools that are more sophisticated than in other industries.

Regulations change and evolve.

The shift to value-based models adds to **administrative burden**, and payers need quality data to accurately assess value.


The Internet of Things (IoT) refers to the network of devices connected to the internet and able to collect and exchange data.

This concept extends beyond standard devices, like computers and smartphones, and into everyday items (cars, kitchen appliances and headphones) and components of machines (jet engines, oil rig drills).

In health care, the IoT includes RPM devices, smart sensors, activity trackers, wearable biometric sensors, smart beds and other types of medical devices.


Possible Applications of IoT in Health Care

Data produced by the IoT has the potential to transform health care in a variety of ways, among individuals and populations.

**Instructions:** Flip each card to learn more about potential transformation of health care

- Improving patient health through real-time monitoring
- Lowering health care costs by promoting preventive care
Enhancing patient satisfaction and engagement through automation of processes and allowing alternative types of access to physicians.

Improving care coordination and workflows through continuous data collection and exchange between patients and care teams.

Health leaders are underwhelmed by population health management technology

According to a survey of 224 health care leaders conducted in April 2020, **56% said** their current population health management solution doesn’t meet their needs. On a 1-10 scale, 38% of respondents rated their population health solution as eight, nine or ten, 24% rated it a seven, and 37 percent judged their solution to be a six or less. Only 41% of those surveyed reported using a population health management (PHM) solution or participating in value-based care.

**Lack of clinician engagement** was cited as the **top reason** organizations are looking to replace their PHM solutions (62%). Other reasons cited as top reasons for wanting to replace PHM solutions were an inability to convert data to action (48%) and the inability to perform sufficient analytics (43%).


Discordant Reporting and Inaccurate Documentation

A study published in JAMA Ophthalmology in 2017 found **large discrepancies** between patient self-report and EHR documentation, with symptoms more frequently reported by patients. The study of 162 patients found **discordant reporting** of the following conditions:
Exact agreement between patient self-reporting and the EHR occurred in only 23.5% of patients.

The study noted that EHRs were not originally intended for the complete documentation of clinical encounters, and suggested that EHR data may not provide a comprehensive resource for clinical practice or big data research.

Another study published in the Journal of the American Medical Informatics Association (JAMIA) found that the rate of inaccurate documentation of initial progress notes from patients in EHRs was significantly higher than in paper charts by a rate of more than five to one. Expected physical examination findings, however, were more than twice as likely to be omitted from paper records as EHRs. Resident physicians were less likely to report inaccuracies and omit information than attending physicians, and the authors suggested that this could be due to residents being under more scrutiny, and/or residents being younger and hence more computer savvy. The study noted that level of training influences the accuracy of documentation.


Integrated Health Model Initiative

The Integrated Health Model Initiative platform will bring together the health and technology sectors around a common data model that will evolve with real world use and participant feedback.

In 2017, the AMA announced a new collaborative initiative aimed at a data evolution to improve, and better organize and share health care information. The Integrated Health Model Initiative (IHMI) platform will bring together the health and technology sectors around a common data model that will evolve with real world use and participant feedback. A common data model for health systems to collect, organize, exchange and analyze data could allow
clinicians to access all the information necessary to **improve care and long-term wellness**. Participation is open to all health care and technology stakeholders.

IHMI aims to solve issues of health care inoperability by addressing two major challenges, data liquidity and data portability.

*Instructions*: Flip each card to learn more about these challenges and IHMI’s efforts to address them.

---

**Data Liquidity**

In collaboration with HL7® FHIR®, IHMI attempts to resolve the issues related to data liquidity including consistent meaning; the ability to aggregate, compare and drive analytics needed to better.

**Data Portability**

IHMI is aiming to bring consistency, clinical prioritization and validation to FHIR® standard development. Data portability becomes the primary problem of interoperability once data
What is data security and why does it matter?

Data security encompasses network, physical and file security, and refers to protecting data from unauthorized access, use, change and destruction.

The Health Insurance Portability and Accountability Act (HIPAA) Security Rule covers any health care provider who electronically transmits health information in connection with a transaction for which the Secretary of Health and Human Services (HHS) has adopted standards under HIPAA, and their business associates. While the HIPAA Privacy Rule protects individually identifiable health information, or protected health information (PHI), the Security Rule protects all individually identifiable health information created, received,
maintained or transmitted by a covered entity in electronic form, or electronic protected health information (e-PHI).

Under the Security Rule, covered entities must maintain appropriate and reasonable administrative, technical and physical safeguards to protect e-PHI. This includes:

- **Ensuring confidentiality** (not available or disclosed to unauthorized persons), **integrity** (not altered or destroyed in an unauthorized manner) and **availability** (accessible and usable on demand by an authorized person) of all e-PHI created, received, maintained or transmitted by covered entities.

- **Identifying and protecting** against reasonably anticipated threats to the security or integrity of information.

- **Protecting** against reasonably anticipated, impermissible uses or disclosures.

- **Ensuring** workforce compliance.


---

**Improving Cybersecurity Practices**

**The HIPAA Security Rule and the EHR Meaningful Use/Advancing Care Information program require**
physicians to conduct security risk analyses, but government compliance is not the only step practices can take to safeguard their data effectively.

The AMA developed the following checklist to help improve cybersecurity and implement improved safeguards.

- **Encrypt** and password-protect mobile devices, tablets and laptops.
- **Ensure** that software and computer server operating systems are regularly patched and updated to protect against malicious software, or “malware.”
- **Install** and regularly update anti-virus software.
- **Use** separate Wi-Fi networks with different passwords for your practice and your patients.
- **Require** strong passwords, containing a mixture of letters, numbers and symbols.

Additionally, these tips are designed to protect office computers from viruses, malware and hackers:
Do not share log-in information with anyone inside or outside the organization; each staff member should have a unique username and password.

Make sure computers are set to automatically download and install new versions of operating systems and software; make sure computers are turned on when new updates are scheduled to install.

Enable automatic web browser updates, and confirm that you are using the most current version of the software.

Purchase and install anti-virus software, and make sure the software is updated at least once per week; in order for updates to occur, the computer must be turned on and have Internet access.

Whenever possible, disable macros in Microsoft Office. Microsoft Office applications use macros to automate routine tasks, but macros can contain malicious code.

Make sure all additional software is running the most current version.

Enable firewalls.

More than four in five physician practices have already experienced a cyberattack

A national survey conducted in 2017 by the AMA and Accenture found that 83% of physician practices have experienced a cyberattack.

The findings of the survey went on to identify three key themes:

1. Cybersecurity is a patient safety issue, not simply a technical issue: Physicians’ top three concerns about cyberattacks were interruptions in practice operations (74%), compromised EHR security (74%) and threats to patient safety (53%).

2. Physicians are not security experts, and practices rely on HIT vendors for network and system security: only 20% of small practices have security officers on staff.

3. HIPAA compliance in itself is not enough to protect patient records: while 85% of surveyed physicians believed it was “very” or “extremely” important to share e- PHI outside of their own system to provide quality care, they knew it was necessary to share it safely.


More than 29 million health care records were breached in 2020. Hacking/IT incidents accounted for 67% of data breaches and 92% of breached records.

More large health care data breaches were reported in 2020 than in any other year since the U.S. Department of Health and Human Services' Office for Civil Rights began publishing health care data breach figures on its website.

In 2020, more than 1.76 data breaches of 500 or more records were reported per day. 642 large data breaches were reported by health care providers, health plans, health care clearing houses and business associates of those entities. These figures represented a 25% year-over-year increase in data breaches compared to 2019, which itself was a record-breaking year.

More than twice the number of data breaches are now being reported than six years ago and three times the number of data breaches that occurred in 2010.
Hacking and other IT incidents dominated data breach reports in 2020, accounting for 66.82% of all reported breaches and 91.99% of all breached records. These incidents include exploitation of vulnerabilities and phishing, malware, and ransomware attacks.


Ransomware Attacks

A report by Comparitech found that in 2020, 92 individual ransomware attacks affected over 600 separate clinics, hospitals, and organizations and more than 18 million patient records. The estimated combined cost of these attacks was $20.8 billion.
Ransomware attacks involve types of malicious software (malware) that threaten to publish or block access to data or systems, usually by encryption, until the victim pays a ransom fee. Often, the ransom demand comes with a deadline, and if the victim doesn’t pay in time, the data cannot be retrieved.

The number of ransomware attempts against the health care industry rose by 123% from 2019 to 2020, according to the 2021 SonicWall Cyber Threat Report. Health care organizations are particularly vulnerable to ransomware attacks because they cannot afford to lose access to patient records, and avoiding downtime is critical and can put patients at risk. Additionally, both reports found that hospitals often have antiquated IT infrastructure and cybersecurity systems compared with other industries, which are difficult to maintain and protect.

The following advice was offered to combat Ransomware attacks:

- **Train staff** to spot and avoid phishing and brush up on basic digital hygiene.
- **Harden and back up systems regularly** so they can be quickly restored in the event of a ransomware attack.
- **Deploy machine learning** and advanced threat protection–enabled endpoint protection.
- **Adhere to zero trust principles**, which involves granting the least access necessary to perform a job, and follows the motto, “never trust, always verify.”
- **Limit access to a single resource** or machine as necessary rather than the entire network when granting a remote employee VPN access.
- **Utilize multifactor authentication**, which requires users to verify their identities in multiple ways such as an authenticator app or receiving a code via text message or email.


Encryption

Encryption refers to converting data from its original form into encoded text, making it unreadable without a decryption code. Data can be encrypted when “in motion,” meaning being shared between individuals and devices, or “at rest,” meaning while in storage. As of 2017, all certified EHRs were capable of encrypting data.

Data encryption becomes especially valuable when data are compromised, as in the case of a ransomware attack, or in the case of a stolen laptop containing patient health information. While encrypting data is not specifically required by the HIPAA, it does fall under the addressable implementation specification; if an organization does not implement encryption, it must document that decision and implement an equally-effective alternative measure, or provide a rationale for otherwise meeting the requirement.

Predicted Impacts

Instructions: Click each plus sign to reveal potential outcomes for patients, physicians and policymakers.
Devices, Internet of Things, and Patient-Generated Health Data

Patients will increasingly use devices connected to the Internet of Things (IoT), and will expect to share patient-generated health data (PGHD) with their providers, and for those data to be used to inform treatment plans.
Unstructured Data

Semantic computing and natural language processing will increasingly be applied to unstructured data, allowing for greater clinical discoveries at faster speeds than were previously possible.
Familiarity with Technology

As increasing numbers of medical school graduates and residents who grew up using computers enter practice, errors related to record keeping in EHRs will decline.
Clinical Support Tools

More clinical support tools will become available that provide insights driven by data analytics to physicians at the point of care.
Ransomware and Other Hacking Attacks

Ransomware and other hacking attacks will increasingly aim to exploit small medical practices, as hackers recognize the challenges to maintaining system security inherent to these practices.
Cloud Storage

The increasing use of cloud storage among health care organizations will lead to a new set of security challenges, particularly related to the training of staff to use safe practices when storing and sharing files in the cloud.
Electronic Health Information

The value of electronic health information on black markets will drive increasing attempts to illegally obtain such information from health organizations.
Prevalence of Ransomware Attacks

Ransomware attacks will become increasingly prevalent and the biggest threat to health care organizations and patient safety.

Disclaimer

© 2021 American Medical Association. All rights reserved.

In producing this publication, the AMA Council on Long Range Planning and Development has consulted and cited sources believed to be knowledgeable. However, the AMA does not warrant that the information is in every respect accurate and/or complete. The AMA assumes no responsibility for use of the information contained in this publication. The AMA shall not be responsible for, and expressly disclaims liability for, damages of any kind arising out of the use of, reference to, or reliance on, the content of this publication.

This publication is for informational purposes only. The AMA does not provide medical, legal, financial, or other professional advice, and readers are encouraged to consult a professional adviser for such advice.
Now that you’ve learned about trends in health data analysis and security trends, identify which of the following are the potential benefits of big data analytics in health care, as well as current barriers that prevent health systems from making use of data.

Instructions: Drag each description to the appropriate category. If incorrectly sorted, the tile will shake and return to the stack. Please try again by sorting it in the correct category.
Potential Benefits

- Real-time monitoring
- Lowering health care costs
- Enhancing patient satisfaction and engagement
- Improving care coordination and workflows
- Population health management
Lesson 6 of 7

CME Credit

Want to earn CME credit for this activity?

Return to the AMA Ed Hub activity and click the Take Quiz tab to proceed.
Lesson 7 of 7

Additional Resources

Transcript

AMA_Trends_2018-19 Health Information Technology_MM3
Data Analysis and Security_Transcript.pdf
19.5 MB

Return to the menu to review content, or close the browser tab to claim CME credit.

© 2021 American Medical Association. All rights reserved.