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

APPLY YOUR KNOWLEDGE

- Knowledge Check
DIG DEEPER

Additional Resources
Lesson 1 of 5

Introduction

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.
Data Analysis

What is Data Analysis?

Data analysis refers to the process by which data is 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.
Data collection: Data are identified and collected. It is preferable to obtain as much data as possible, particularly from diverse sources, which can lead to the discovery of stronger correlations, more actionable insights and building better models.

Data cleaning: The expression “garbage in, garbage out” means that even if a program’s logic is valid, if the data being analyzed are invalid, so too will be the findings. In this step, errors and missing data are identified, and nonsense information is removed, so as not to corrupt future analysis.

Data modeling, analysis and insight development: Models are built to correlate data with outcomes and make recommendations on potential changes that could improve those outcomes. Ideally, through this analysis, organizations will discover actionable, data-supported strategies for reaching identified objectives.


Internet of Things

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.

**Sources:**

**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
In 2016, 76% of health care organizations were involved in some type of population health management (PHM) initiative. By focusing on improving health care delivery for defined groups of individuals with similar needs, health care providers have the opportunity to improve outcomes while lowering costs, reduce emergency room visits and hospitalizations, enhance patient experience and engagement, and improve patient self-management.

Successful PHM programs depend on access to and analysis of vast amounts of patient data, allowing health care providers to define populations, monitor outcomes, improve treatment...
plans and improve care coordination. For these efforts to be possible, health care organizations must be capable of integrating the various available data types into existing systems and workflows and aggregate data across the continuum of care.


**Patient Generated Health Data**

A survey conducted by Medscape and presented at the 2017 Healthcare Information and Management Systems Society (HIMSS) annual conference found that less than 40% of patients have provided patient-generated health data (PGHD) to their health care providers. Among those who have, 57% responded that they did so "all the time" or "often" without being asked by their providers to do so. There is agreement among providers and patients that patients are more engaged during office visits in which they have provided PGHD. Ninety-seven percent of surveyed patients said that they would be somewhat or much more likely to collect and share PGHD with their providers if they thought it would be used to develop their treatment plans.

Among health care providers, the barriers to incorporating PGHD into practice included:

- Lack of relevance
- Organization and health record integration
- Lack of time to consider data
- Perceived lack of patient motivation to collect and share PGHD
The survey defined PGHD as “Logs, diaries or lists of health-related information, measured, recorded or gathered by the patient, or by their family members or care givers. The gathering of health data could be done manually (written down) or by an electronic device (for example, a fitness tracker or Smartphone app).”


Health Care Data

A 2017 survey of members of the NEJM Catalyst Insights Council found clinical data, cost data and claims data to be the three most valuable sources of health care data. Among the biggest
opportunities for the use of health care data were care coordination, improved decision support and predictive analytics.

**Lack of interoperability** was cited as the biggest barrier to making use of patient data, followed by difficulty and time required collecting data. However, more than three in four respondents said that there were either currently useful applications for big data, or that within several years useful applications would exist.


**Difficulties in Health Care Data**

The University of Iowa, Carver College of Medicine, projects that by 2020, health data will double every 73 days.

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 accurately assess value.
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.


Yadav S, Kazanji N, Narayan KC, Paudel S, et al. Comparison of accuracy of physical examination findings in initial progress notes between paper charts and a newly implemented
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.
Early collaborators include IBM, Cerner, Intermountain Healthcare, the American Heart Association, the American Medical Informatics Association, and a list of others. The initial AMA focuses include:

- Clinical and issue-based communities that focus on **costly and burdensome areas**
- A clinical validation process to determine and apply appropriate **clinical frameworks**
- A model to encode information in the **IHMI data model**


**Data Lakes**

The term data lake refers to a **repository** in which huge amounts of data are stored in their native format, rather than being customized for individual purposes. These data can then be **queried for analytic purposes**. A number of ongoing efforts in health care are making use of data lakes.

*Instructions:* Click each tab to learn more about ongoing efforts

<table>
<thead>
<tr>
<th><strong>SEMANTIC DATA LAKE</strong></th>
<th><strong>CANCERLINQ INITIATIVE</strong></th>
<th><strong>IDEA PLATFORM</strong></th>
</tr>
</thead>
</table>

Semantic computing attempts to align computational data with the intention of the user so that the user may make use of those data. Montefiore Medical Center has partnered with Franz Inc. to create a semantic data lake (SDL). An initial pilot program pulled real-time data from the SDL and used **predictive analytics to flag patients at risk of death or in need of intubations**
within 48 hours. The program uses a predictive algorithm based on retrospective data from over 68,000 patients from Montefiore and the Mayo Clinic, and creates a risk score reflecting the patient's likelihood of a major event.

As of late 2016, the American Society of Clinical Oncology’s CancerLinQ initiative contained health data from more than one million cancer patients in its data lake. The goal of the system is to provide real-time feedback to oncologists on patterns in outcomes, benchmark performance compared to national guidelines and colleagues in other practices, and offer clinical decision support. CancerLinQ can connect to most major EHR systems, and is potentially available to any practice in the United States.

In 2016, Partners Healthcare introduced the Integrated Data Environment for Analytics (IDEA) platform. The platform aims to provide storage for vast datasets dealing with PGHD, translational research and precision medicine, and function as a testing environment for developing decision support tools and investigating clinical questions. The data lake also has the potential to centralize data from the IoT, due to the unstructured nature of the data contained in it.


Predicted Impacts

AMA_Trends 2018-19 Health IT MM3 Data Analysis.pdf

187.8 KB
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**
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.


As of January 2018, **3,286,498 individuals** had been impacted by breaches in 2017 (final figures do not become available until March 1 of the following year). This represented a **347%** decline from the previous year, and a **continued downward trend** in impacted individuals. However, the number of health care security breaches has continued to grow steadily. In 2015, **270 security breaches** occurred, a number that **increased to 327** in 2016, and **342** in 2017 (likely to increase slightly in the final count).

Hacking and IT incidents affected more individuals than any other type of breach in 2017, and appear to be **growing in prevalence**. This rise can partially be attributed to the growing number of ransomware attacks against health systems, during which access to systems or networks is blocked until a sum of money is paid to the attacker. **Unauthorized access** and **disclosures and loss** or **theft of devices and records** are among the other leading causes of data breaches.
A 2017 survey by KPMG found that 47% of health care organizations experienced a HIPAA-related security violation or breach in the two preceding years, and more than 77% of organizations experienced a device breach in recent years.

Organizations perceive the following as their biggest vulnerabilities:

- Third party data sharing (63%)
- Devices not fully controlled by IT (59%)
The study found that more than half of health care organizations rely on cyber insurance. Additionally, more than four in ten respondents have not increased their cyber-security budgets and/or did not anticipate doing so in the next year; thirty-four percent of organizations did not invest at all in information security in the previous year.

The report also found that organizations are far more likely to invest in security policies (82%) and technology (79%) than in staff (24%), but emphasized that technology is only as effective as the people charged with its operation and monitoring.

The report recommended practices for securing health care data:

- Make cyber security an urgent priority.
- Provide input to manufacturers of medical devices in the design stage.
- Employ proactive rather than reactive defense.
- Learn where the greatest security risks lie.
- Focus heavily on staff training.

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.

A 2017 survey by HyTrust of 51 health care and biotech organizations found that 25% of health care organizations storing data on a public cloud did not encrypt their data. While 63% of health care organizations reported using public cloud storage, and 63% of HIT decision makers intended to use multiple cloud vendors, 38% of those organizations that currently used multiple cloud vendors for their data were not encrypting their data in any way. 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.


HITRUST and the AMA have partnered to offer cybersecurity workshops in 50 cities to educate physicians and small practices on cyber risk and security.

The workshops will cover topics such as cyber and HIPAA risk assessments, cyber hygiene, implementing cost-effective and manageable solutions, and lessons from other practices.

Workshops are offered free of charge, and intend to offer actionable takeaways and guidance for small practices that may lack resources.


Disclaimer

© 2018 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.
Predicted Impacts

AMA_Trends 2018-19 Health IT MM3 Data Security.pdf
188 KB
Lesson 5 of 5

Additional Resources

Transcript

AMA_Trends_2018-19 Health Information Technology_MM3 Data Analysis and Security_Transcript.pdf
136.2 KB

Predicted Impacts

AMA_Trends 2018-19 Health IT MM3 Data Analysis.pdf
187.8 KB

AMA_Trends 2018-19 Health IT MM3 Data Security.pdf
188 KB
Return to the menu to review content, or close the browser tab to claim CME credit.