Understanding Audit Logs and Trails

Risk Strategies for Monitoring Metadata

MedPro Group
a Berkshire Hathaway company

Disclosure

MedPro Group receives no commercial support from any ineligible company/ commercial interest.

It is the policy of MedPro Group to require that all parties in a position to influence the content of this activity disclose the existence of any relevant financial relationship with any ineligible company/commercial interest.

When there are relevant financial relationships mitigation steps are taken. Additionally, the individual(s) will be listed by name, along with the name of the commercial interest with which the person has a relationship and the nature of the relationship.

Today’s faculty, as well as CE planners, content developers, reviewers, editors, and Risk Solutions staff at MedPro Group, have reported that they have no relevant financial relationships with any commercial interests.

Objectives

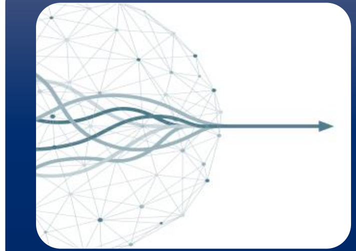
At the conclusion of this program, participants should be able to:

- Describe the different types of metadata and where it can be found within the practice setting
- Understand transaction log requirements and how system interplay impacts organizational processes
- Recognize the value in using audit log information to monitor and improve the quality of care and services
- Implement effective strategies to monitor metadata and respond to legal metadata requests

Overview of metadata and audit trails

Foundational concepts and terms

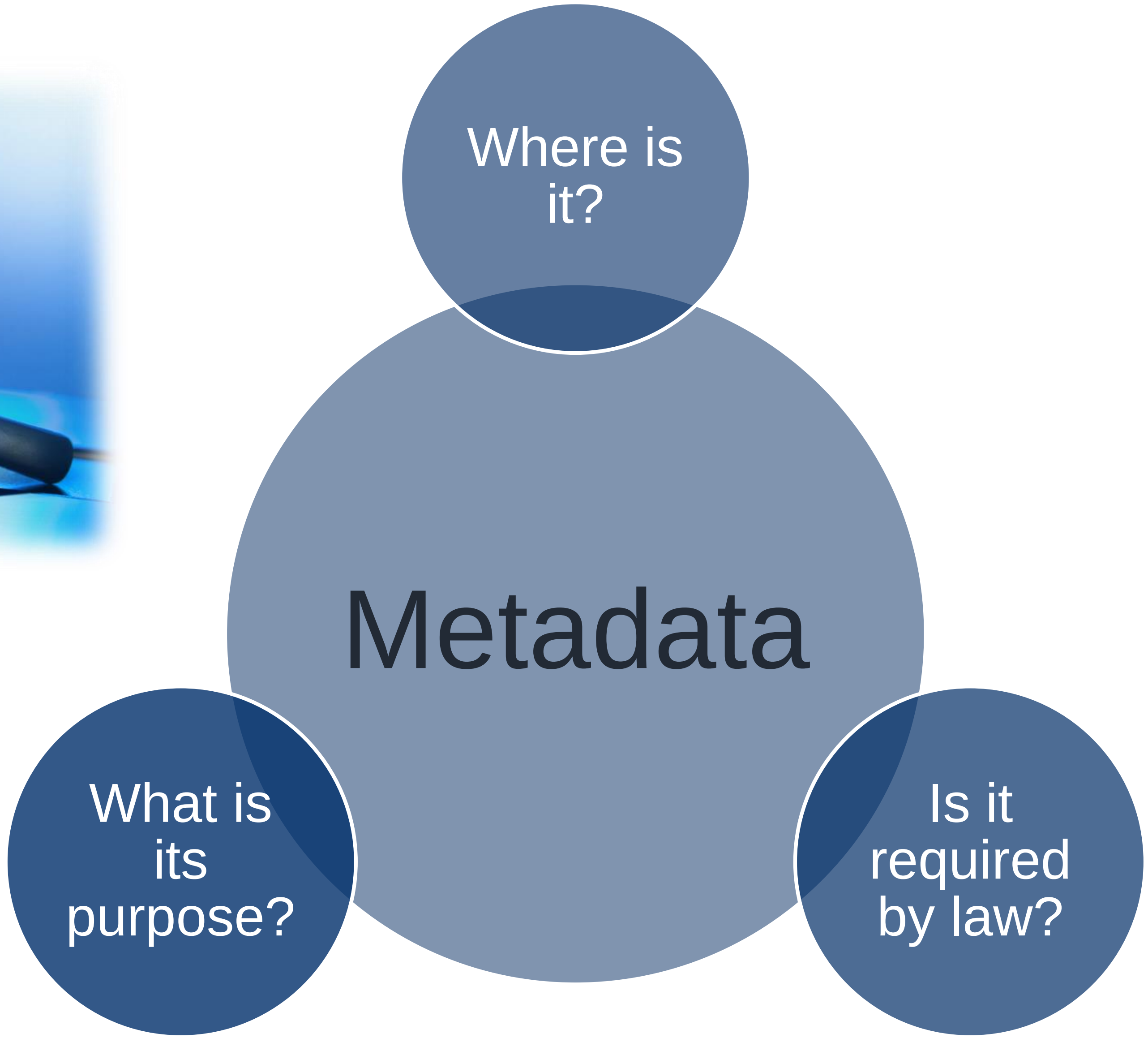
Metadata



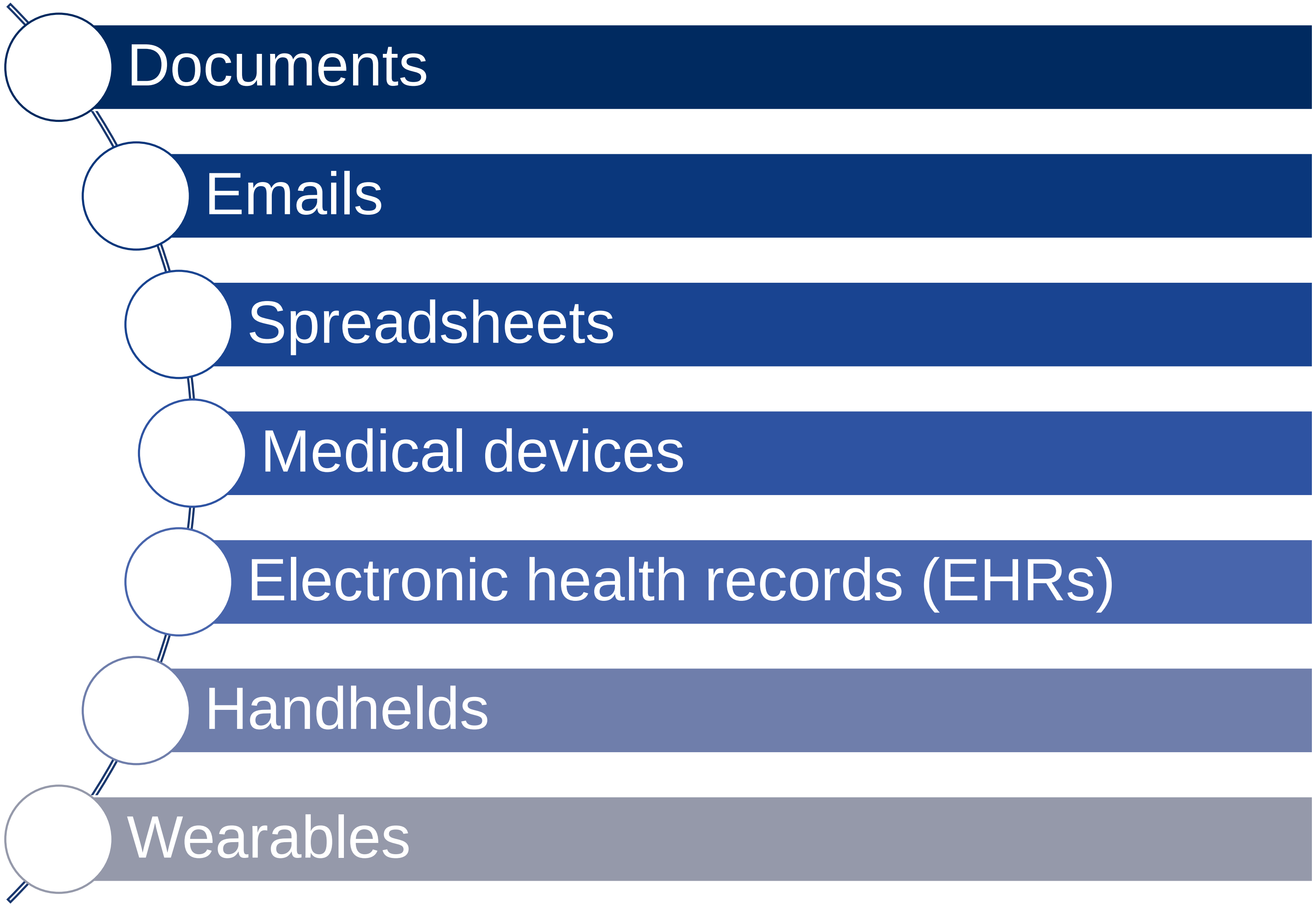
Audit trail

HIPAA Privacy and Security Rules

Metadata basics



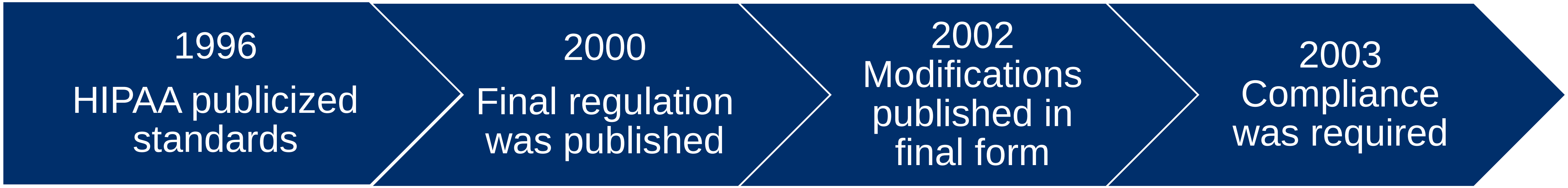
Metadata progression over the years



- Documents
- Emails
- Spreadsheets
- Medical devices
- Electronic health records (EHRs)
- Handhelds
- Wearables

HIPAA Privacy Rule

- Creates standards for compliance on disclosure of patient data to protect all “individually identifiable health information”
- Balances the need for data protection while allowing regulated flow of information when appropriate
- Dictates in which scenarios transmission of patient data is appropriate for care coordination
  - Release to patient
  - Other providers
  - Insurance billing
  - Contracted business associates



1996
HIPAA publicized standards

2000
Final regulation was published

2002
Modifications published in final form

2003
Compliance was required

U.S. Department of Health and Human Services. (n.d.). The Privacy Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

HIPAA Security Rule

Why

What

Implications

1996 Health Insurance Portability and Accountability Act (HIPAA) creates rules, safeguards, and definitions

1998 Security and electronic signature standards were proposed

2003 Final Rule was determined with security standards

2005 Compliance was required

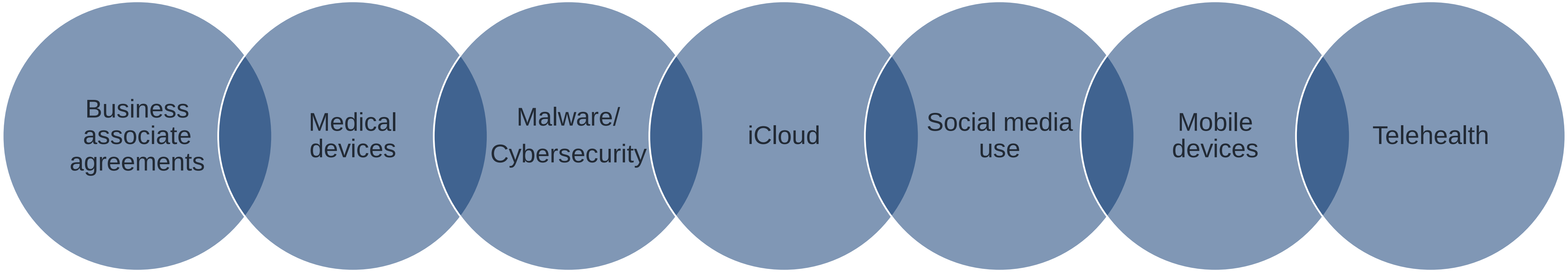
2009 Federal Register Notice of Delegation of Authority to Office for Civil Rights (OCR)

2010 Modification under Health Information Technology for Economic and Clinical Health Act (HITECH Act) proposed included both incentives and penalties to encourage adoption of electronic records versus paper records meaningful use

2013 Modifications made final under the Omnibus HIPAA Final Rule

U.S. Department of Health and Human Services. (n.d.) HIPAA for professionals. Retrieved from https://www.hhs.gov/hipaa/for-professionals/index.html; U.S. Department of Health and Human Services. (n.d.). The Security Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/security/index.html

HIPAA Security Rule enforcement



Business associate agreements

Medical devices

Malware/ Cybersecurity

iCloud

Social media use

Mobile devices

Telehealth

Electronic health record systems

Recognize that not all systems are the same

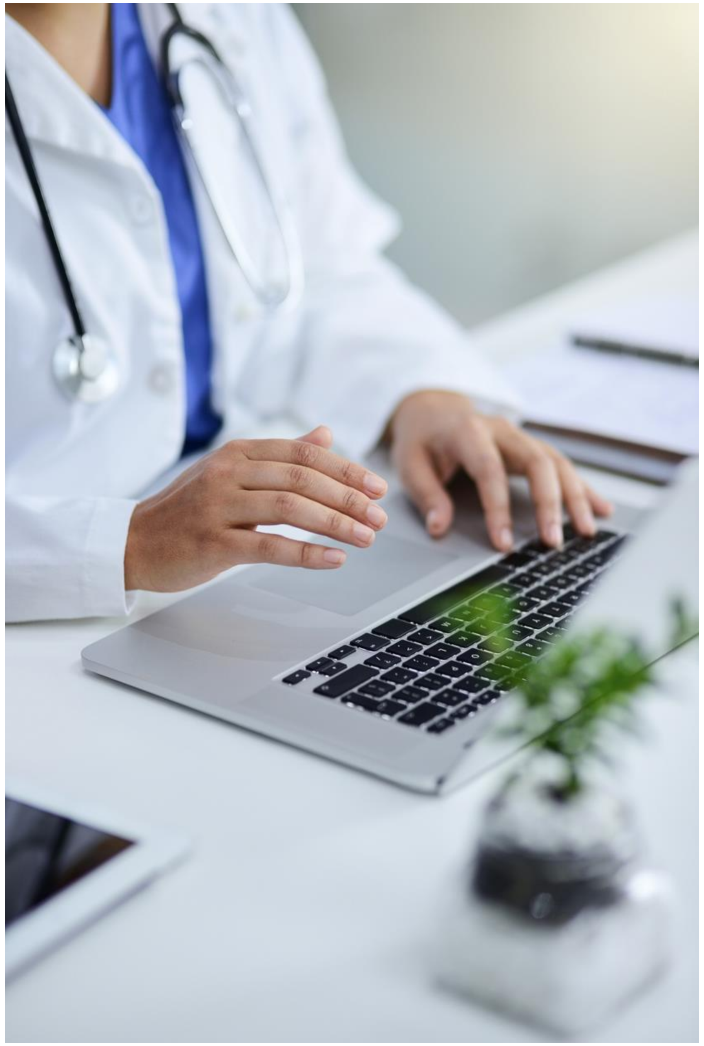
- Epic, eClinicalWorks, NextGen, TouchChart, Meditech, etc.

Know your system

Develop policies

- Standardize
- Specify how to address addendums
- Establish timeframe to close encounter (don’t create something that makes you fail)

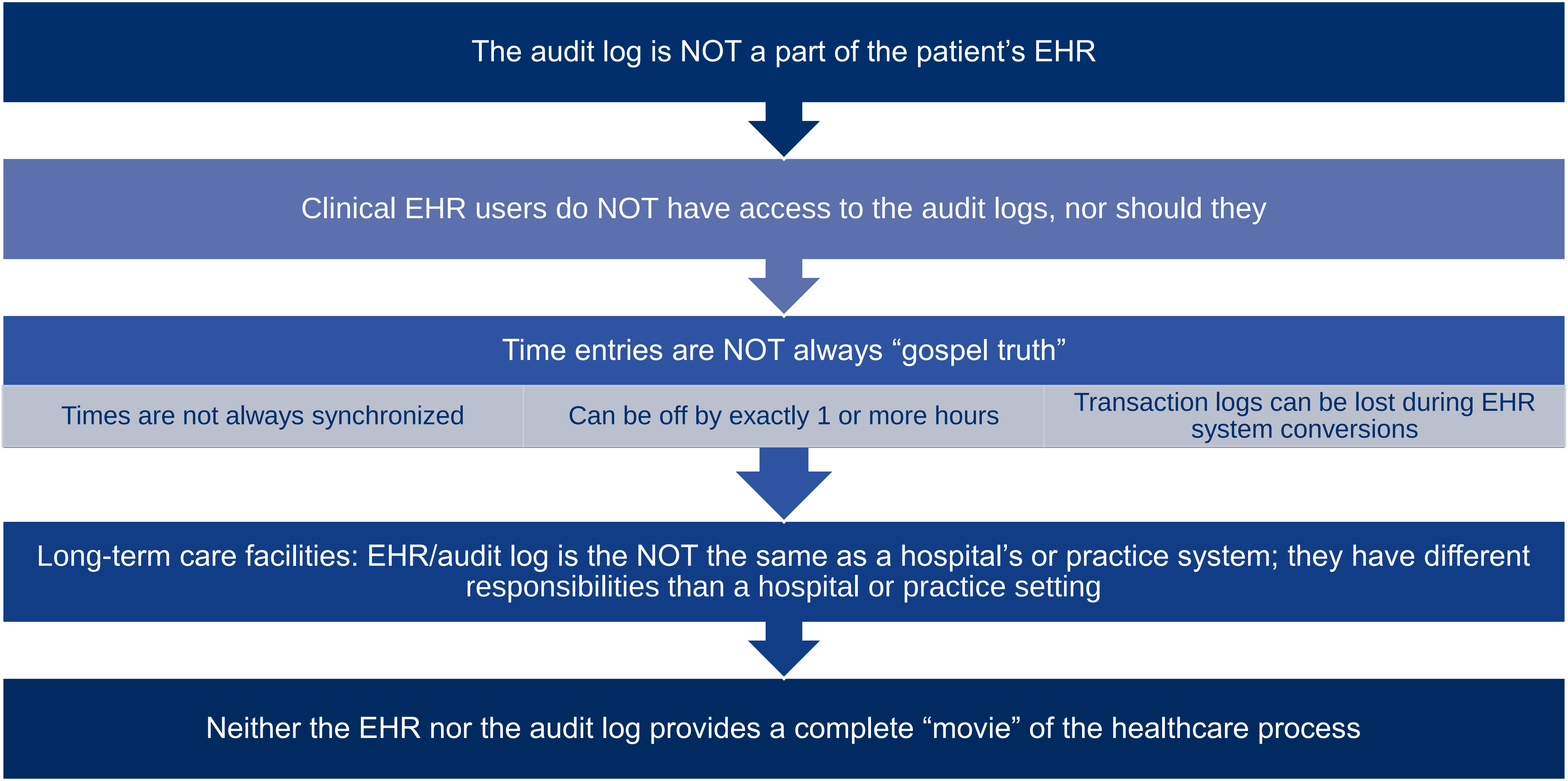
Continuously evolve - Use your IT contacts



Interplay between systems and logs

**System integration streamlines user experience on the front end,
but it expands the perceived electronic footprint behind the scenes.**

Audit log misconceptions



The audit log is NOT a part of the patient’s EHR

Clinical EHR users do NOT have access to the audit logs, nor should they

Time entries are NOT always “gospel truth”

Times are not always synchronized	Can be off by exactly 1 or more hours	Transaction logs can be lost during EHR system conversions

Long-term care facilities: EHR/audit log is the NOT the same as a hospital’s or practice system; they have different responsibilities than a hospital or practice setting

Neither the EHR nor the audit log provides a complete “movie” of the healthcare process

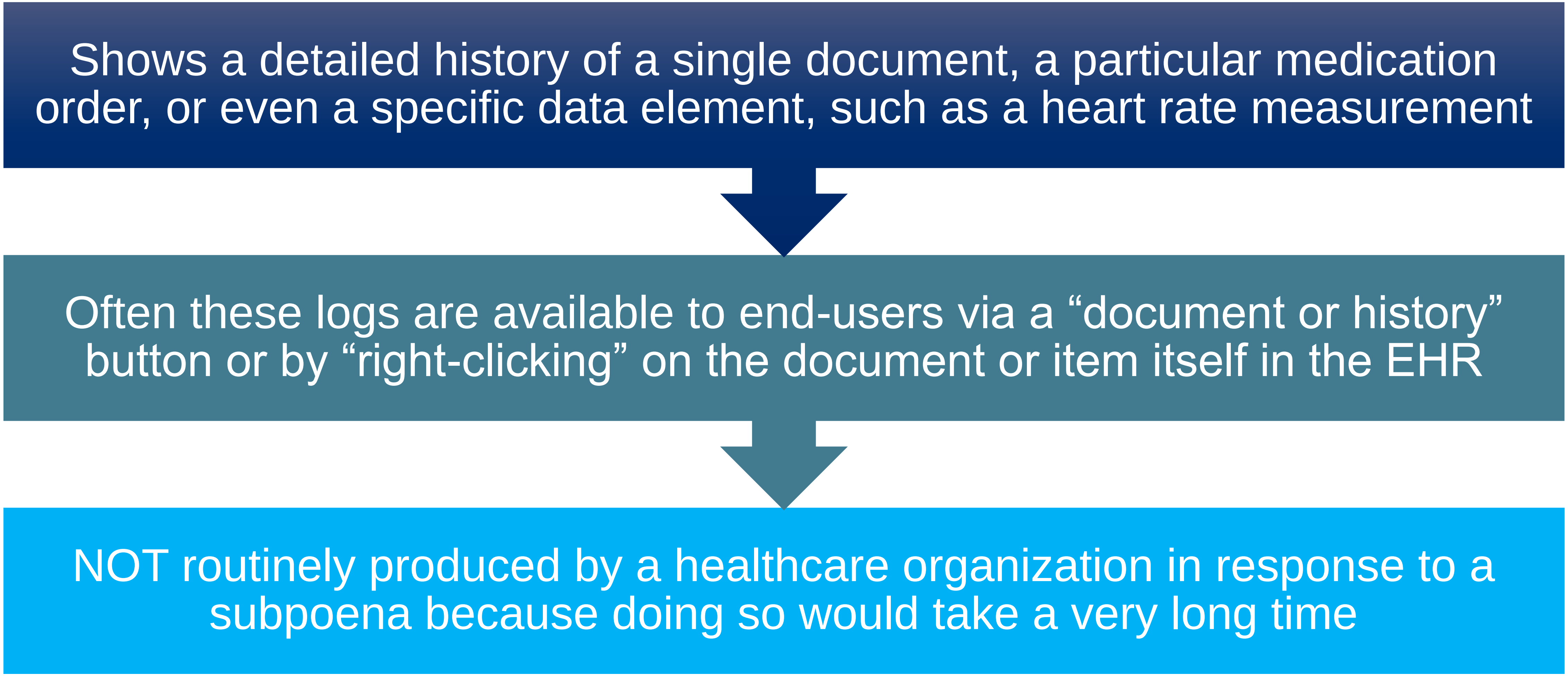
Types of audit or transaction logs

Access audit log

Shows who accessed record, what was done, and when it was done

“Audit trail” comes from here and is a small portion focused on transactions for a specified time interval involving a single patient, user, or in some instances, a specific computer

Document or data element history log



Shows a detailed history of a single document, a particular medication order, or even a specific data element, such as a heart rate measurement

Often these logs are available to end-users via a “document or history” button or by “right-clicking” on the document or item itself in the EHR

NOT routinely produced by a healthcare organization in response to a subpoena because doing so would take a very long time

Keystroke and mouse movement log

Some EHRs keep an extremely fine-grained log that records individual keystrokes, mouse clicks, and mouse movements, along with the time each event occurred

Usually kept for a relatively short time (i.e., less than 6 months)

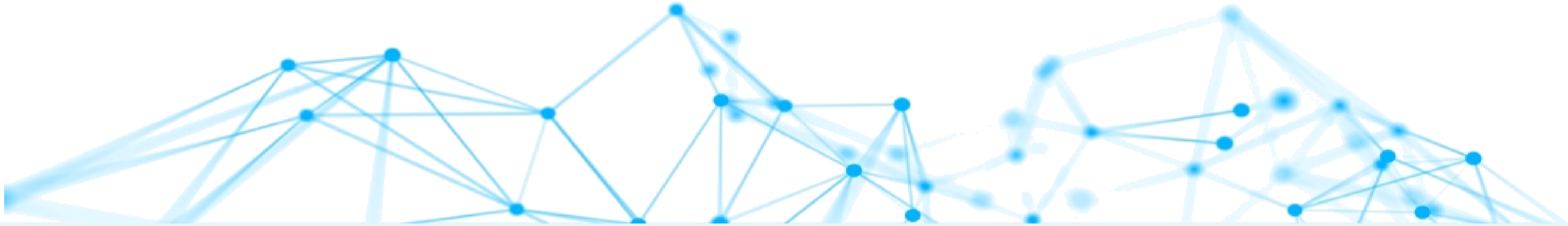
EHR subcomponents log

Used by EHR developers and those responsible for the ongoing operation and maintenance of various subcomponents of the EHR (clinical decision support alerts or software error logs)

Records successful and/or failed transactions that occurred

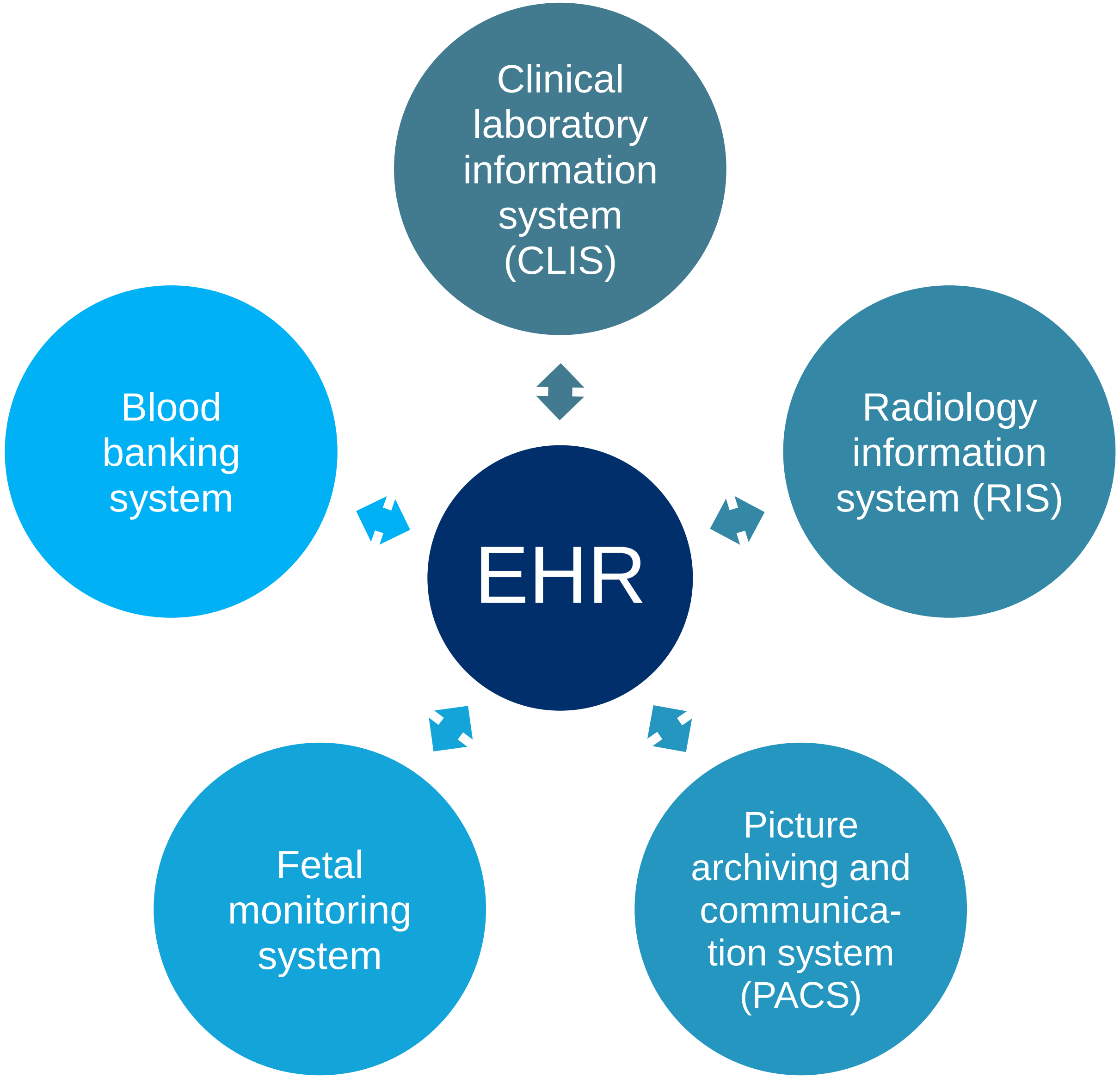
Available to EHR system developers and kept for a limited time (i.e., less than 2 years)

Examination of these logs could be useful in instances in which it is hypothesized that a particular order or result never made it to its intended recipient



Ancillary clinical systems logs

- Similar to information contained in the EHR audit log
- Often used to generate departmental management reports, such as determining the mean time to process laboratory specimens within the laboratory or calculating worker efficiency (e.g., number of X-rays or MRI studies reviewed and reported on in a given shift)
- Usually only available to system developers and administrators in the local departments
- Kept for a limited time (i.e., less than 2 years)


Clinical laboratory information system (CLIS)
Blood banking system
Radiology information system (RIS)
EHR
Fetal monitoring system
Picture archiving and communication system (PACS)

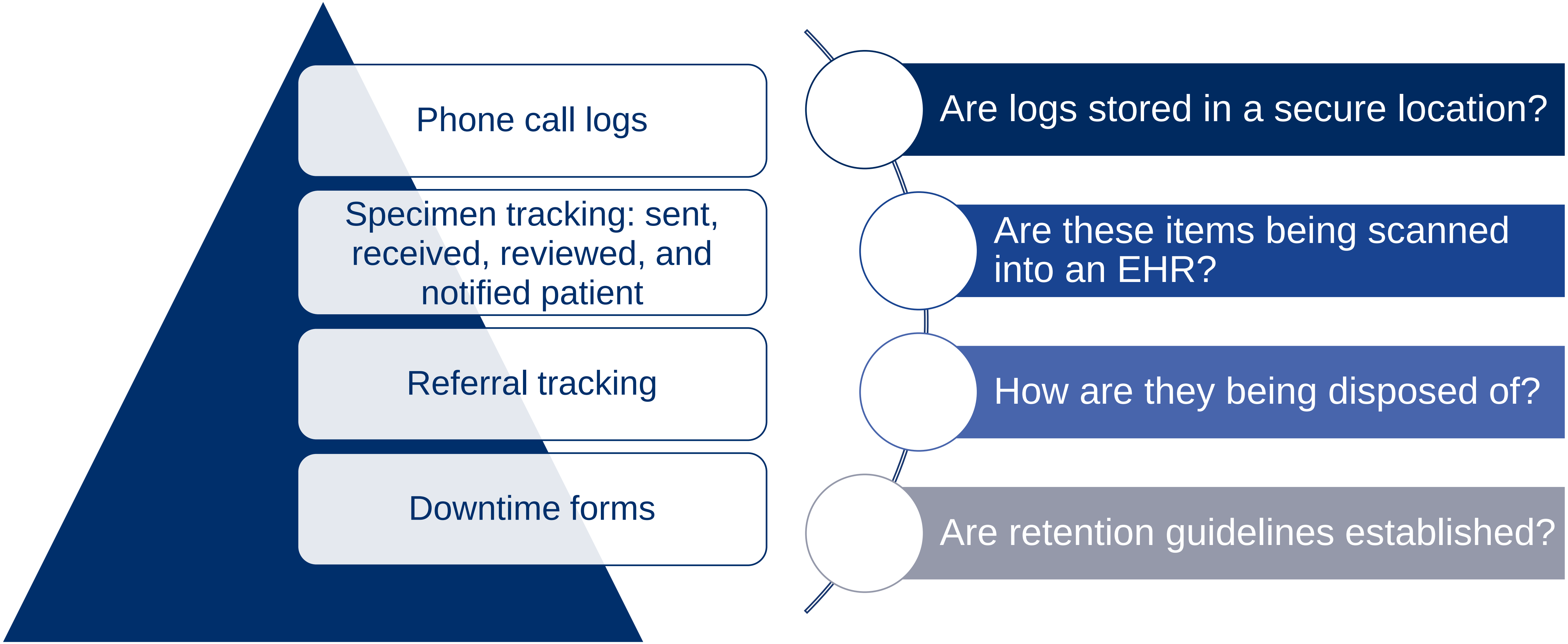
Individual computer-controlled medical device logs

Short-term transaction logs are associated with a specific device, e.g., a point of care blood gas testing device, handheld or dedicated computer, thermometer, cellphone, or fax machine

These logs are usually kept for a very short time (i.e., less than 3 months), and they are only available by interacting with the actual device

Unless the device has a unique user login with a password for each user, it is difficult to determine which transactions are associated with particular patients or users

Paper-based logs/Tracking sheets



- Phone call logs
- Specimen tracking: sent, received, reviewed, and notified patient
- Referral tracking
- Downtime forms

- Are logs stored in a secure location?
- Are these items being scanned into an EHR?
- How are they being disposed of?
- Are retention guidelines established?

Case study

Patient	Thirty-six-year-old female patient presented for a HCM visit and revealed recent changes to her bowel movements. The patient did not notice blood in her stool; however, she stated that she was not really looking for it and was unaware of a family history of colon cancer.
Summary	Hemoccult slide provided to patient for in-home use. Instructed to return slide to clinic for processing.
	Order entered into EHR.
	Patient returned slide to clinic for processing 1 week later.
	Specimen slide processed and logged on paper log with positive result.
	Result not entered into EHR.
	The provider nor patient were notified of positive finding. The ‘outstanding’ order was not ‘resulted’ in the EHR.
Outcome	The patient presented 2 years later with additional symptoms and was diagnosed with Stage IV colon cancer.

What information should an audit log include?

ASTM 2147

Always

- Date and time of access event – when it occurred
- Patient identification
- User identification
- Type of action – create, view, modify, or print

Mandatory since 2020

- Source of access – application used
- Identification of the patient data accessed – demographics, labs, meds, notes
- Date and time of activity – stated time or when data were valid
- Location of access or activity – workstation or device?
- Duration of access

Documentation versus audit logs

Human element needed to explain audit log

One must correlate audit log entries with EHR entries and human testimony.

User walks away from monitor

Entries by others under someone else’s login

User does not know record well

- Slow entries
- Makes mistakes

Human user vs. automated or programmatic data entry

The meaning of terms in the audit log can change over time

How can metadata be used?

Quality assurance or internal organization investigation

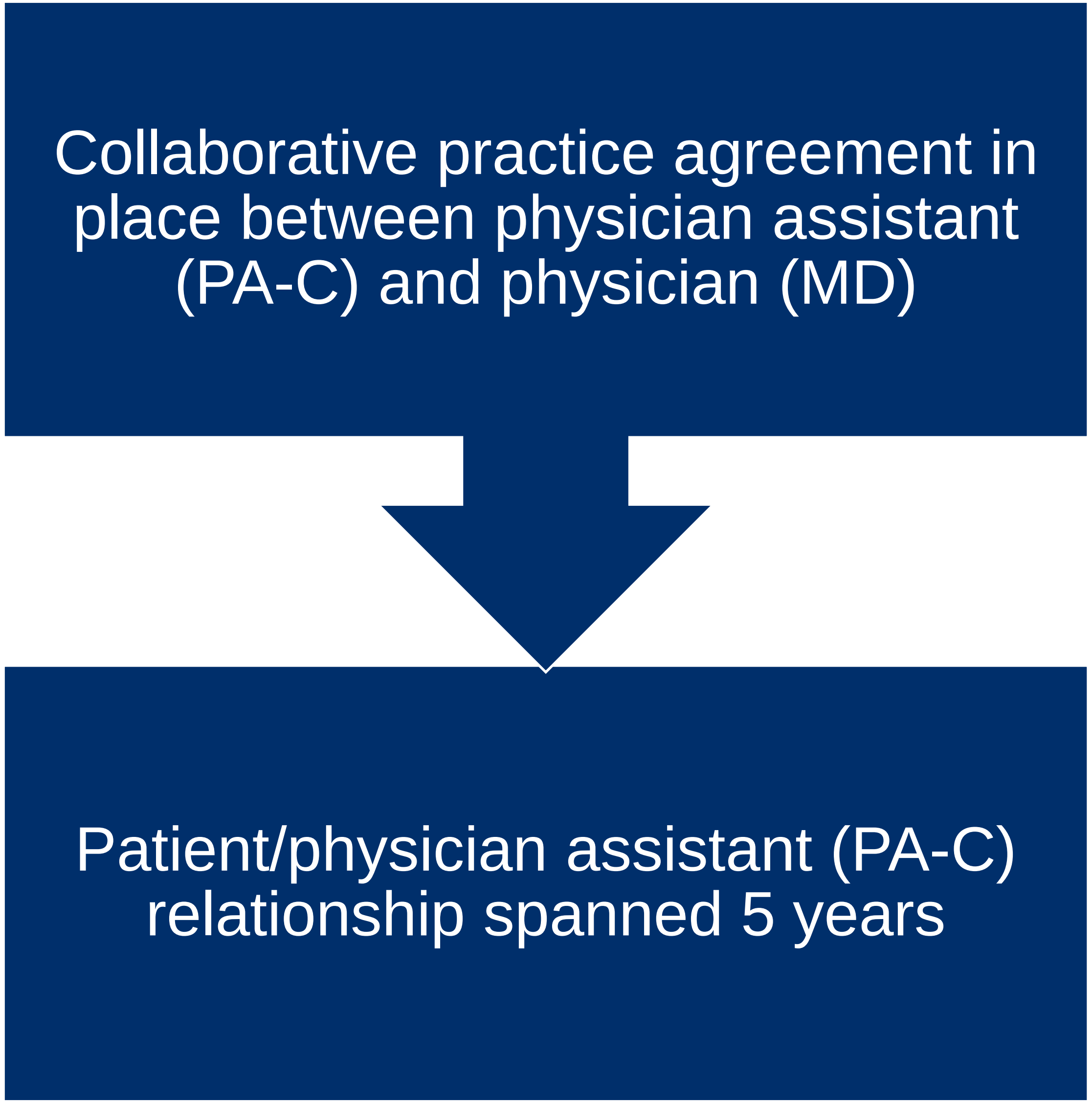
Organizational use

- Evaluate incident
- Perform general QC
- Evaluate processes and workflows
- Validate data

Legal perspective

- Prove or explore health record alteration
- Establish a medical timeline
- Determine who looked at or accessed the health record
- Ensure that the health records provided were complete
- Explain why hard chart copies look different and had conflicting information from others
- Make defendant look less truthful

Case study



Collaborative practice agreement in place between physician assistant (PA-C) and physician (MD)

Patient/physician assistant (PA-C) relationship spanned 5 years

Summary of Plan: Pt feeling depressed. Will increase vilazodone to help with mood. Will order lithium level. Pt admits to occasional suicidal thoughts, no plan or intent. Pt states that he is safe, he can contract. Pt agrees to call with any concerns.

Goal: Alleviate anxiety, alleviate depression, increase day-to-day functioning, promote decision-making, and maintain gains.

Estimated Sessions: 11

24 hour crisis reviewed.

Return to office in 2 weeks

Lithium, CMP

12/13/2020 Time in: 12:30 **Time out:** 12:45

Electronically signed by Jane Doe, PA-C

12/16/2020 Physician consulted. Read above, agree with assessment and treatment.

Electronically signed by *Scott Johnson, MD*

Interrogatories

Date	Time	User	Area	Activity	Detail
12/13/2020	12:35:00P	Doe	Document	Update	Follow-up: Depression PA, Depression
12/13/2020	12:43:20P	Doe	Document	Signed	Follow-up: Depression PA, Depression
12/13/2020	12:43:40P	Doe	Document	Entered item	Follow-up: Depression PA, Depression
12/13/2020	12:44:00P	Doe	Chart Summary	Exited	
12/13/2020	12:44:50P	Doe	Document	Updated	Follow-up: Depression PA, Depression
12/13/2020	12:45:10P	Doe	Meds	Exited Summary	
12/13/2020	12:45:30P	Doe	Meds	Entered Summary	
12/13/2020	12:48:00P	Doe	Dx. History	New Item	
12/13/2020	12:48:10P	Doe	Dx. History	New Item	
12/13/2020	1:00:20P	Doe	Document	Print	Clinical Visit Summary
12/16/2020	2:09:10P	Bloom	Appt History	Updated	
12/16/2020	4:30:20P	Johnson	Document	Updated	
12/16/2020	4:30:20P	Johnson	Document	Signed	
12/16/2020	4:45:00P	Jackson	Ref Email	Read Email	

With respect to the records concerning Plaintiff's Decedent maintained by Scott Johnson, MD, please produce the electronic audit trail and/or any compilation of data that demonstrates (i) the date and/or time on which any entries in the record were created, modified, revised, accessed, or deleted; (ii) the identities of the persons accessing the health record; and/or (iii) the information accessed, created, modified, revised, or deleted.

Risk mitigation strategies

Know your systems

What does each system track? Does it follow ASTM 2147?

How long is the data maintained?

What systems are integrated? Where do gaps exist?

Are paper logs used? If so, for what and how long, etc.?

Are policies up to date to meet standards set forth by HIPAA Privacy and Security Rules?

Audit trails and identified risk exposure

Be involved . . .

Procurement

Quality assurance

Legal review for vendors

. . . every step of the way

Should I access/review the information?

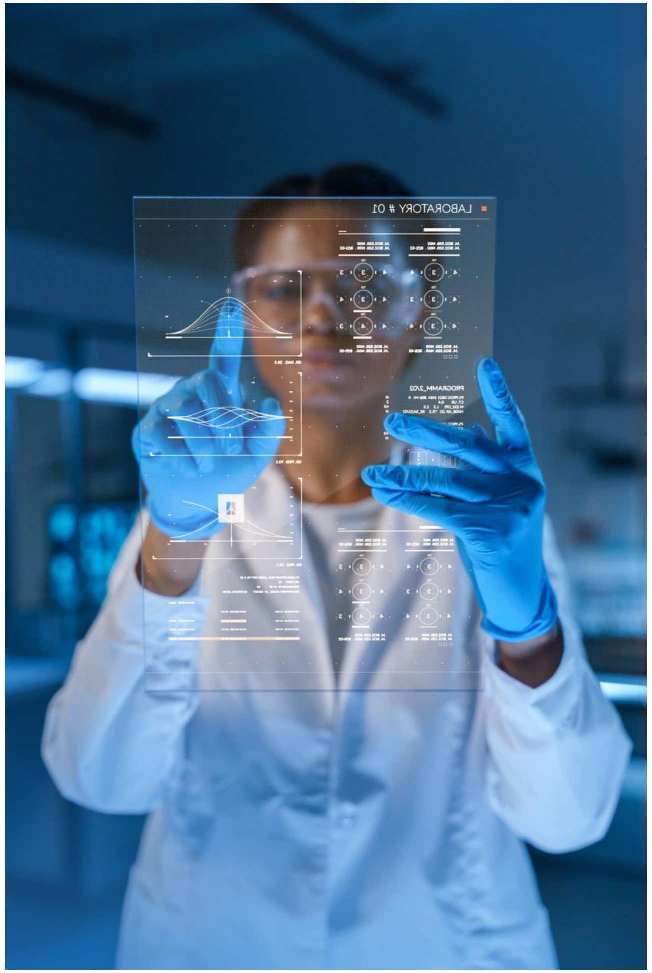
Future with artificial intelligence

Artificial intelligence (AI) is the evolution of the electronic health record

AI will automatically fill in missing information, suggest diagnoses, and even predict future health outcomes based on historical data

Already present in some platforms:

- Patient monitoring devices
- Voice recognition for dictation
- Automated appointments, test results, etc.
- Computer-aided diagnosis
- Clinical decision support – algorithms and treatment plans created based on input



Future with artificial intelligence (continued)

Unknown how AI will impact future litigation

- Audit trails will be more complex
- No legal precedent
- Will evolve much like when EHRs were introduced
- Will require updates as standards change
  - Impact is on a much larger scale - no longer one healthcare provider and one patient affected

Providers will be monitored for compliance

- Don’t “rubber stamp” everything
- Escalate concerns
- Collaborate with teams

Resources

Resources

[Department of Health and Human Services: The Security Rule]

[Department of Health and Human Services: The HIPAA Privacy Rule]

[Health Affairs: To Measure the Burden of EHR Use, Audit Logs Offer Promise – But Not Without Further Collaboration]

[MedPro Group: Electronic Health Records: Patient Safety and Liability Concerns]

[MedPro Group: Record Retention Guideline]

Disclaimer

The information contained herein and presented by the speaker is based on sources believed to be accurate at the time they were referenced. The speaker has made a reasonable effort to ensure the accuracy of the information presented; however, no warranty or representation is made as to such accuracy. The speaker is not engaged in rendering legal or other professional services. The information contained herein does not constitute legal or medical advice and should not be construed as rules or establishing a standard of care. Because the facts applicable to your situation may vary, or the laws applicable in your jurisdiction may differ, if legal advice or other expert legal assistance is required, the services of an attorney or other competent legal professional should be sought.