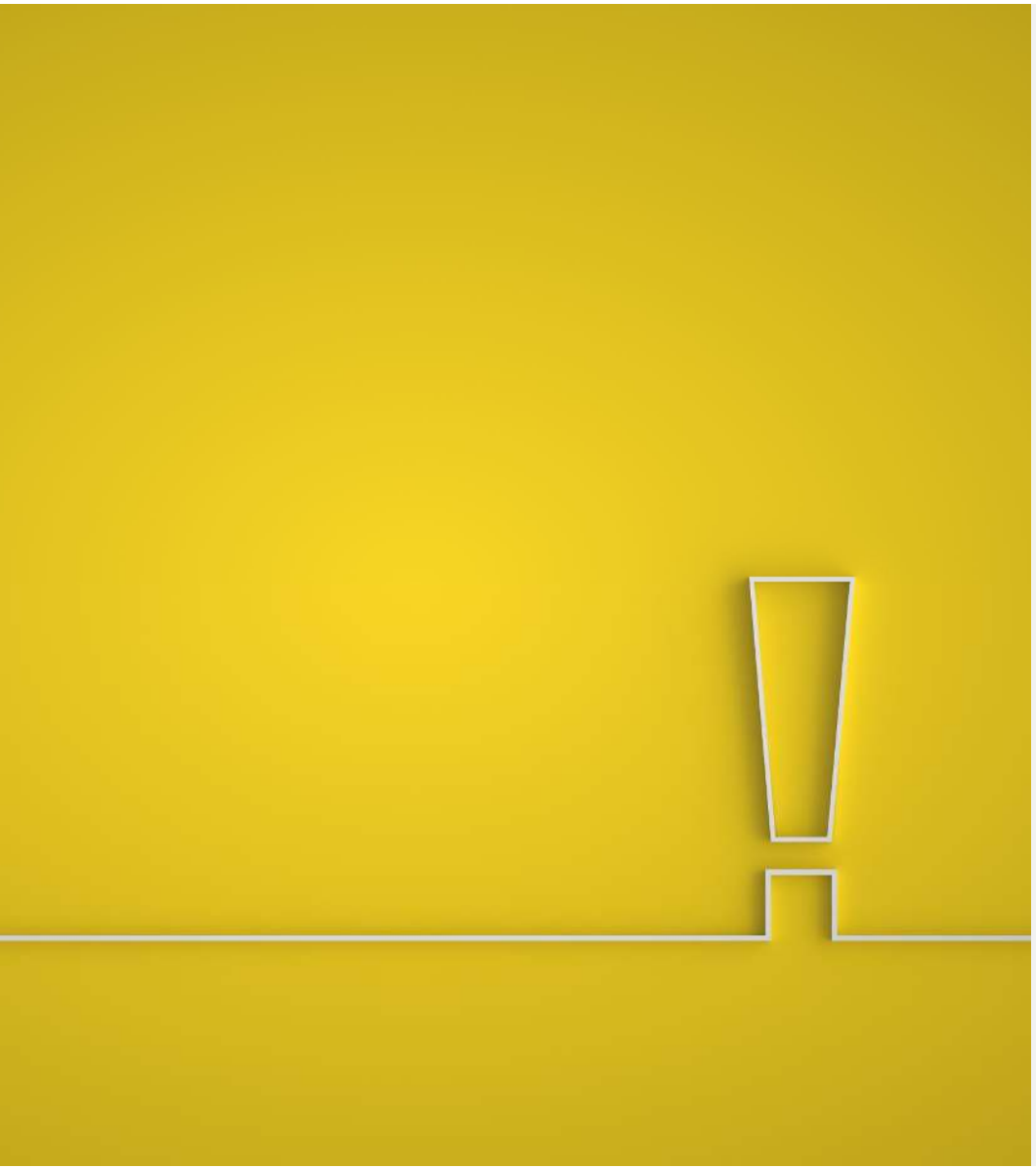
ETHICS II: CONFIDENTIALITY AND ACCOUNTABILITY

CHANDLER JONES, MSHA, RRT, RRT-ACCS, RRT-NPS, CPFT, PDE

PULMONARY DISEASE NAVIGATOR AND RESPIRATORY EDUCATOR



OBJECTIVES

- Take a look at confidentiality in healthcare
- Review common violations, or breaches
  - Case 1 and 2
- HIPAA, PSQI (2005), and more
- Understand the exceptions and why

RECAP EPISODE 1

- Ethics is a means of running a business with healthcare.
- Beneficence: The duty to act in the best interest of patients, promoting their well-being and health outcomes.
- Nonmaleficence: The obligation to avoid causing harm or injury to patients.
- Autonomy: Respecting the patients right to make their own decisions about their care and treatment.
- Justice: Fair distribution of healthcare resources and equitable access to care.

- Three-step decision making model and the James Rest model for ethical decision making.
  - Is it legal, is it free of extremes, and how does it make you feel?
  - Gut feeling
- Ethics and law are different, but one builds the other.

ITS THAT OLD GOSSIP

- Even Hippocrates understood how important it was to keep an individuals health information private and secure.
  - "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about"
- Patients have a given right to dictate what they want done with their health information – for it to be shared, studied, etc.

- Think of the consequences speaking about someone's health.
  - Ask yourself – would I want everyone and their distant cousins to know I have scabies, ring worm, AIDS, chlamydia, heart failure, COPD.
  - When health information is released without the patients consent it creates an atmosphere of distrust - and misuse

EMR

- Electronic Medical Record
- Documentation and retrieval of health information on a computer
- the idea is to improve patient care, increase efficiency, enhance communication, data collection, and patient engagement
- EMRs can provide patients with secure access to their own medical records, allowing them to take a more active role in their healthcare. This can improve patient engagement and satisfaction.

- What is included
  - Health data
  - Insurance information
  - Sensitive information such as DOB, SS, address, etc.
  - Hopefully HIPAA forms
  - Diagnostic results and imaging
  - Personal and in some cases familial medical hx
  - Other notes and recordings
  - A leak or inaccuracy with any of this data can cause discrimination, embarrassment, loss of trust, medical errors, and more

WHICH ETHICS ARE WE WORKING WITH

- Autonomy - Patients have the right to make decisions about their healthcare, and EMR systems must respect patients' autonomy by providing them with access to their own health information and allowing them to control how their information is shared.
- Beneficence – remove from harm, right? Communication and continuity of care is a form of removing the patient from an less effective means of receiving care.
- Non-maleficence - EMR systems should not cause harm to patients. Healthcare providers must ensure that patient data is accurate and up-to-date and that EMR systems are secure and reliable.
- Justice - EMR systems should promote justice by ensuring that patients have equal access to healthcare services, regardless of their social or economic status. Healthcare providers must also ensure that patient data is used in a fair and ethical manner, without discrimination or bias.
- Fidelity – loyalty – is it fair to think that fidelity may be at risk if records may be hacked or stolen?

CONFIDENTIALITY LAW AND POLICY

- Through out the many years since Hippocrates there has been an ever-growing push to hone and expand this practice.
- With the emergence of more and more technology – policy regarding health information must also mold around it
- Look at social media, implantable, uploading, downloading, sharing, etc. of health information now
- It is easy to see how a breach, or violation, may occur

- 1960s – feds believed it be necessary to retain patient data → folks didn't like this, so they went to work on it
- 1970s – around 73' – 74' the Privacy Act (not just health related) was signed, which was spurred by a report via the Department of Health, Education, and Welfare (HEW).
  - One can imagine how this monumental accomplishment inspired HIPAA
- 1980s - COBRA
- 1990s – HIPAA comes about under Clinton around 96' – essentially gave people more control over their health information and it also addressed insurance lapses
- 2000s – Privacy Rule (2001), Healthcare Integrity and Protection Data Bank (2000), Patient Safety and Quality Improvement Act (2005), HITECH, GDPR, and more

PRIVACY ACT AND COBRA

- Remember, at some point the US Government was like, I think I want to keep this data and do stuff with it.
- Privacy Act – This addressed how a plethora of information could be distributed the the federal government has, such as social security, without consent – there are 12 exceptions
- It protects American citizens by granting the right to request records, request a change to those records, the right to be protected against unwarranted invasion of privacy

- Before HIPAA there was COBRA, or short term health insurance – Consolidated Omnibus Budget Reconciliation Act – which paid insurance at the expense of the company or the employee – which one do you think likely paid for it in respect to general insurance.
- A big idea or hope here is that employees, once they leave the organization for whatever reason, they can apply for COBRA and continue with benefits until hired somewhere else
- Generally lasts 18-36 months

HIPAA

- HIPAA stands for Health Insurance Portability and Accountability Act, a federal law enacted in 1996 to protect patients' privacy and ensure the security of their medical information.
- HIPAA requires healthcare providers, health plans, and healthcare clearinghouses to implement safeguards to protect the confidentiality, integrity, and availability of patients' health information.

- HIPAA sets national standards for the privacy and security of patients' health information, including rules for how healthcare providers can use and disclose this information.
- HIPAA requires healthcare providers to obtain written authorization from patients before sharing their health information with anyone other than those involved in their care, unless otherwise required by law.
- HIPAA establishes penalties for non-compliance with its provisions, including fines and imprisonment, depending on the severity of the violation.
- HIPAA also includes provisions that allow patients to access and obtain copies of their medical records, request corrections to their records, and file complaints with the Department of Health and Human Services if they believe their privacy rights have been violated.

HITECH AND MORE

- The Patient Safety and Quality Improvement Act (PSQIA) was enacted in 2005 to encourage the reporting and analysis of medical errors and other adverse events in healthcare facilities.
- The law provides protections for the confidentiality and privilege of information submitted to Patient Safety Organizations (PSOs), which are entities that collect and analyze data related to patient safety.
- The PSQIA also requires healthcare providers to develop and implement quality improvement initiatives to prevent future errors and improve patient outcomes.

- Incentives for adoption of HIT: HITECH established financial incentives for healthcare providers who adopt and meaningfully use electronic health records (EHRs). It also introduced penalties for those who do not comply with the regulations.
- Privacy and security of health information: HITECH strengthened the HIPAA (Health Insurance Portability and Accountability Act) Privacy and Security Rules to ensure the protection of patient health information in electronic form. It also established breach notification requirements for covered entities and business associates.
- Focus on health information exchange (HIE): HITECH promoted the exchange of health information between healthcare providers, with the aim of improving the quality and coordination of care. It established grant programs to support the development of statewide HIE infrastructure and standards for interoperability.

CASE 1

- Dr. Johnson is a family physician who works at a clinic that serves a small town. One day, Dr. Johnson accidentally sends an email containing medical information of several of his patients to the wrong email address. The email contained information such as patient names, diagnoses, and treatment plans.
- The person who received the email was not authorized to view the information and promptly reported it to the clinic. The clinic then investigated the incident and determined that it was a breach of HIPAA regulations. They notified the affected patients and reported the breach to the U.S. Department of Health and Human Services (HHS).
- As a result of the breach, Dr. Johnson faced disciplinary action from the clinic and was required to undergo additional HIPAA training. The clinic also implemented additional safeguards to prevent similar incidents from occurring in the future. Additionally, the breach was investigated by HHS, and the clinic was required to pay a fine for the violation of HIPAA regulations.
- The incident caused a great deal of stress for the affected patients, as their private medical information had been exposed to an unauthorized person. It also damaged the reputation of the clinic, as patients lost trust in their ability to keep their information safe.

ACCOUNTABILITY

- The EMR is a foot trail of ideally all encounters a person has in medicine.
- One way accountability takes a seat is in terms if documentation
- The medical record is a legal document
- The record can contain everything from date of birth and social security number to orthopedic surgery and gene therapy.

- Factual
- Legible
- Objective – no personal opinions
- Accurate
- Timely
- it is important to note that EMRs are not a panacea for accountability in healthcare. They are only as good as the information entered into them, and there are still concerns about the accuracy and completeness of EMRs.

FLOAT

- Factual – makes sense that everything you place in the legal document of a medical record is true
- Legible - this one is fazing out with a great majority of major medical facilities adopting EMR software
- Objective – we encounter all walks of life in the hospital – no one needs your two cents
- Accurate – spelling and grammar are critical, especially to a critically ill patient
- Timely – don't document 0800 vent check with your 1600 vent check

- How do hospital systems take accountability for well..Accountability?
- I know you've heard of the good ol Joint Commission (1951)
  - These folks among other things, review records to validate all of the mentioned
  - Site visits at least one a year, one every two years for lab
  - A report is delivered after the site visit with an audit of "violations" in which a time frame is established for correction

CASE 2

- A hospital employee, Jane, was tasked with transferring patient records from the hospital's electronic medical records system to an external hard drive. Jane did not follow proper protocols and did not encrypt the data or securely transfer the hard drive. She then left the hard drive on her desk, unattended, and unlocked.
- As a result, the hard drive was stolen, and the patient records of over 10,000 individuals were compromised. The compromised data included personal information such as names, addresses, dates of birth, social security numbers, medical diagnoses, and treatment information.
- Consequences: The hospital reported the breach to the Department of Health and Human Services' Office for Civil Rights, as required by HIPAA regulations. The hospital also informed affected individuals of the breach and offered them free credit monitoring services. The breach was found to be a serious violation of HIPAA, and the hospital was fined $1.5 million by the Office for Civil Rights. The hospital also faced significant reputational damage, loss of patient trust, and potential lawsuits from affected individuals.
- Lessons Learned: This case highlights the importance of following proper HIPAA protocols and taking data security seriously. Hospitals and healthcare providers should regularly train their employees on HIPAA regulations, including proper handling and transfer of patient data. They should also have strict policies and procedures in place to protect patient data and respond quickly and effectively to any breaches that occur.

CHARTING FOR ACCOUNTABILITY

- S – situation and the patients chief complaint
- O – objective from labs and other dx
- A – conclusions based on both subjective and objective data
- P – plan of action – generally based on guidelines or protocols
- Narratives are thorough and concise but tends to lose the purpose
- Updated progress notes are best
- Sets clear and concise charting

CURRENT CONDITION
COPD/pneumonia

GOALS
1. Pt. will demonstrate productive cough in seated position, 3/4 trials. 2. Pt. will ambulate 150ft with supervision, no assistive device, on level indoor surfaces.

S	Pt. reports not feeling well today, "I'm very tired".
O	Auscultation findings: scattered rhonchi all lung fields. Chest PT was performed in sitting (ant. and post.). Techniques included percussion, vibration, and shaking. Pt. performed a weak combined abdominal and upper costal cough that was nonbronchospastic, congested, and non-productive. The cough/huff was performed with VC. Pectoral stretch/thoracic cage mobilizations performed in seated position. Pt. given towel roll placed in back of seat to open up ant. chest wall. Strengthening exercises in standing - pt. performed hip flexion, extension, and abduction; knee flexion 10 reps x 1 set B. Pt. performs HEP with supervision (in evenings with wife). Pt. instructed to hold tissue over trach when speaking to prevent infection and explained importance of drinking enough water.
A	Pt. continues to present with congestion and limitations in coughing productivity. Pt. has been compliant with evening exercise program, which has results in increased tol to therapeutic exercise regime and an increase in LE strength. Amb. not attempted to 20 to pt. report of fatigue. Pt. should be able to tolerate short distance ambulation within the next few days.
P	Cont. current exercise plan including CPT; emphasize productive coughing techniques; increase strengthening exer reps to 15; attempt amb. again tomorrow.

OTHER EMR USES FOR ACCOUNTABILITY

- Tracking and reporting
  - Audit trails
  - Quality and performance reporting
- Overall, tracking and reporting EHRs can help promote healthcare accountability by ensuring accuracy and completeness of patient information, providing audit trails for documentation and investigations, identifying areas for improvement in quality and performance, and ensuring compliance with regulations and standards.

- Compliance
  - Access to complete medical records for one
  - Reminders and alerts can be set
  - Communication and coordination is easier
  - Data analysis can yield trends

FINES AND PENALTIES

- For violations that are not willful, the minimum penalty is $100 per violation, up to a maximum of $50,000 per violation. For willful violations, the minimum penalty is $50,000 per violation, up to a maximum of $1.5 million per year. In addition to financial penalties, violators may also face criminal charges and imprisonment.

- One example of a breach in health information with consequences occurred in 2015 when Anthem Inc., one of the largest health insurance companies in the United States, experienced a cyber-attack that resulted in the theft of personal information of approximately 80 million individuals, including customers and employees.
- Anthem Inc. faced severe consequences as a result of the breach, including investigations by multiple state and federal agencies, lawsuits by affected individuals, and a $115 million settlement with state attorneys general. The company also had to spend millions of dollars to improve its cybersecurity and prevent future breaches.

PROTECTING INFORMATION

- How can we avoid some of these penalties and fines?
- We have to constantly change with the ebb and flow of technology

- Use encryption
  - Helps prevent unauthorized access
- Use secure networks –firewalls, updated software and all
- Use two factor authentication
  - Just like your amazon account
- Regularly audit these security systems
  - Yes – its time to change your password
- Secure disposal of information
- Use access controls – determine who can see what
- Train employees to be cognizant of PHI
  - Yep – Mandatory (insert hospital here) edu coming up 12/31 am I right?

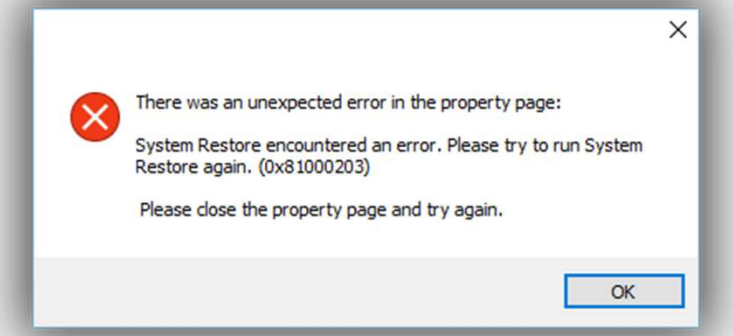
EXCEPTIONS

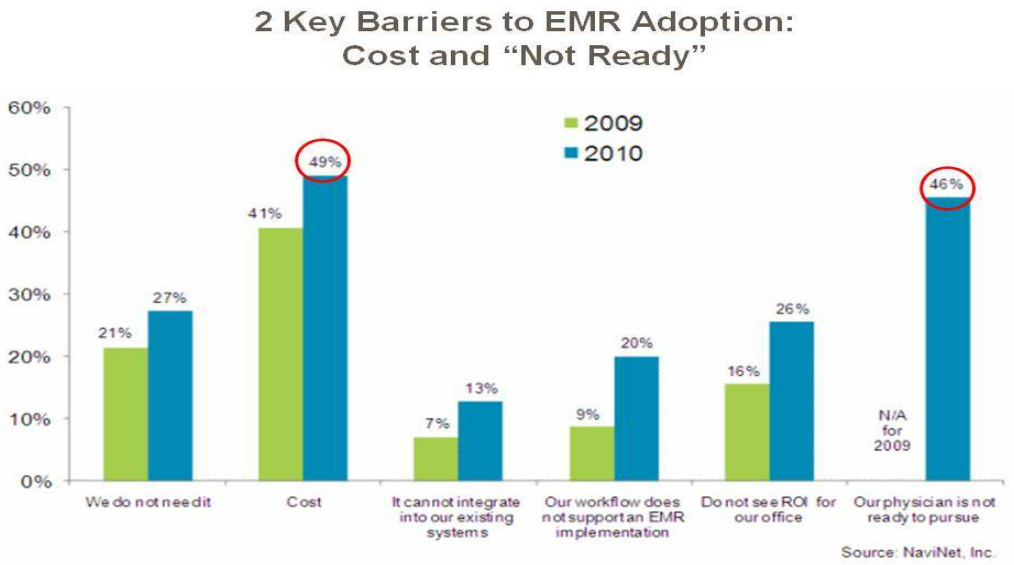
- There are a few exceptions to the lock down of sensitive patient information
- Law enforcement, abuse, danger, or other legal matters – of course
- If it is a public health concern – COVID, TB, malaria
- Research – strict restrictions
- Parent/legal guardian, etc.
- Payment
- Treatment

- United States v. Stefonek. In this case, the defendant was suspected of illegally distributing prescription drugs.
- During the investigation, law enforcement officers obtained a warrant to search the defendant's home and found evidence of drug distribution. The officers also discovered a locked safe in the defendant's bedroom, which they believed contained additional evidence of drug distribution.
- The defendant refused to provide the combination to the safe, so the officers sought a court order to compel him to disclose the combination. The court granted the order, and the defendant eventually provided the combination.
- However, the combination that the defendant provided was incorrect, and the officers were unable to open the safe. The officers then obtained a second court order to compel the defendant to provide the correct combination, but the defendant again refused.
- The officers then sought a third court order to obtain the defendant's medical records, which they believed would contain information about the defendant's medical conditions and the prescription drugs that he was taking. The court granted the order, and the officers obtained the defendant's medical records.
- The medical records confirmed that the defendant had been prescribed the prescription drugs that were found in his home, and the defendant was ultimately convicted of drug distribution

DOWNSIDES

- I think it is safe to say that privacy is a concern as well as the states legal and ethical problems that arise
- Training and implementation costs: Implementing and training staff to use EMRs can be costly and time-consuming, which can be a barrier for smaller healthcare providers or those with limited resources.
- User error: User error is a common issue with EMRs, which can result in inaccurate data entry or incorrect documentation. This can lead to medical errors, misdiagnosis, and potential harm to patients.





DOWNSIDES

- Technical issues: Technical glitches and system failures can lead to delays in accessing patient information or even loss of data, which can negatively impact patient care and safety.

- Increased workload and decreased face-to-face interaction: EMRs can increase the amount of time required for documentation, which can decrease the amount of time healthcare providers have for direct patient care.
- Additionally, the use of EMRs may decrease the amount of face-to-face interaction between healthcare providers and patients, potentially negatively impacting patient satisfaction and outcomes.

CONCLUSION

- You just though it was a computer program, eh?
- Confidentiality is as old as the books, especially regarding medicine.
- There is an ever growing concern for privacy, specifically as it relates to EMR.
- Accountability brings the whole thing together.
- Its not only shameful to gossips but can cost you your license, career, home, and life (metaphorical).