PRACTICING ON THE GRID

Cyber Liability Issues, EHR, Telemedicine and Patient Portals

Justin Joy, JD
Attorney, Lewis Thomason

Jeff Woods, JD
Director of Risk Education
Cyber Liability Issues
Cyber Crime

- How bad is it, really?
- HIPAA requirements for analyzing risks to your practice and PHI
- Data hostage events
- Getting your practice “cyber ready”
<table>
<thead>
<tr>
<th>Totals for Category:</th>
<th>Medical/Healthcare</th>
<th># of Breaches: 306</th>
<th># of Records: 14,457,012</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>% of Breaches: 35.7</td>
<td>% of Records: 48.5%</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Totals for All Categories:</th>
<th># of Breaches: 858</th>
<th># of Records: 29,835,478</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>% of Breaches: 100.0</td>
<td>% of Records: 100.0%</td>
</tr>
</tbody>
</table>

Used with permission from Identity Theft Resource Center.
Nearly 90% of healthcare lawyers say industry is at greater risk of data breaches than others

By Maria Castellucci | October 14, 2016

About 87% of health law attorneys think their healthcare clients are at a greater risk for cybersecurity attacks than other industries, a survey released Thursday found (PDF).

The survey, conducted by the American Health Lawyers Association, a nonpartisan organization with 13,500 members, along with media research company Bloomberg Law, found attorneys overwhelmingly think the healthcare industry is vulnerable to hacks and they have since become “intimately” involved in managing cybersecurity issues for their clients.
FOR IMMEDIATE RELEASE
October 18, 2016

$2.14 million HIPAA settlement underscores importance of managing security risk
Healthcare's Digital Divide Widens, Black Book Consumer Survey

PRESS RELEASE  UPDATED: JAN 3, 2017

Outwardly great technologies are failing to have a penetrating effect on the healthcare system as patient IT adoption declined in 2017.

Tampa, Florida, January 3, 2017 (Newswire.com) - Black Book’s national panel poll of consumers aims to judge patient adoption and acceptance of technology, as well as measure those impacts on the healthcare industry. The survey, conducted from September through December 2016, asked consumers to evaluate the technology they were exposed to, know of or interacted with as an active patient in the last twelve months.

57 percent of consumers with contact experience to hospital, physician or ancillary provider’s technology in 2016 report being skeptical of the overall benefits of health information technologies such as patient portals, mobile apps, and electronic health records mainly because of recently reported data hacking and a perceived lack of privacy protection by providers. The national survey which included 12,090 adult consumers. Key findings include:
Healthcare's Digital Divide Widens, Black Book Consumer Survey

In a follow up to an Office of the National Coordinator (ONC) survey, Black Book found this year that 70 percent of American distrust health technology, sharply climbing from only 10 percent in 2014.

89 percent of consumers with 2016 provider visits report withholding health information during visits. 93 percent responding expressed concerns over the security of their personal financial information, as high deductible Obamacare plans and co-pays have more banking and credit card data passing from providers.
Athens Orthopedic Clinic reported a data breach of patients medical and personal information. (Photo/John Roark, Athens Banner Herald)
Analyzing the Risk to Your Electronic Protected Health Information (ePHI)

- Any time risks change due to operational conditions or organization changes, re-start the process
- Remember mobile devices and remote access (Home PCs)
- Office of the National Coordinator for Health Information Technology Security Risk Assessment Tool (October 2016 update)

HIPAA Security Rule requires covered entities conduct Risk Analysis

Use it to develop Security Management Plan & other procedures.
ePHI in the Cloud

- ePHI in the cloud **most likely** requires a business associate agreement
- “Conduits” vs. “business associates”
- Consider where your ePHI is stored

<table>
<thead>
<tr>
<th>Storage Location</th>
<th>In Use?</th>
<th>BAA?</th>
<th>Last Review Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>E.H.R.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Back-up</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud-connected Mobile Devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient Portal</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Don’t Forget about Paper Medical Records

- About 80 paper breaches each affecting over 500 individuals were reported in 2016
- Evaluate how paper is handled in your office
- Ways to reduce risk?
- Changing template forms to eliminate certain information (full SSN, health insurance information)
- Implement and follow paper document retention policies
Is it Really a Breach?

FOR IMMEDIATE RELEASE
January 9, 2017

Contact: HHS Press Office
202-690-6343
media@hhs.gov

First HIPAA enforcement action for lack of timely breach notification settles for $475,000
Is it Really a Breach?

- Breach vs. unauthorized disclosure?
- If there is an unauthorized disclosure, presumption is a breach
- Every unauthorized disclosure should be analyzed by performing a written HIPAA Breach Notification Rule risk assessment
- Burden is on the covered entity to prove that notification is not required
- Retain assessment documents for 6 years
- Unauthorized disclosures happen. To everyone. Use them in risk analysis and procedure improvement!
## Is it Really a Breach?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification</td>
</tr>
<tr>
<td>2</td>
<td>The unauthorized person who used the protected health information or to whom the disclosure was made</td>
</tr>
<tr>
<td>3</td>
<td>Whether the protected health information was actually acquired or viewed</td>
</tr>
<tr>
<td>And 4</td>
<td>The extent to which the risk to the protected health information has been mitigated</td>
</tr>
</tbody>
</table>
Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

The assault on Hollywood Presbyterian occurred Feb. 5, when hackers using malware infected the institution’s computers, preventing hospital staff from being able to communicate from those devices, said Chief Executive Allen Stefanek.

The hospital said it alerted authorities and was able to regain control of all its computer systems by Monday, with the assistance of technology experts.
Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating

“The malware locks systems by encrypting files and demanding ransom to obtain the decryption key. The quickest and most efficient way to restore our systems and administrative functions was to pay the ransom and obtain the decryption key,” Stefanek said. “In the best interest of restoring normal operations, we did this.”

The attack forced the hospital to return to pen and paper for its record-keeping.

Phil Lieberman, a cybersecurity expert, said that, while ransomware attacks are common, targeting a medical institution is not.

“I have never heard of this kind of attack trying to shut down a hospital. This puts lives at risk, and it is sickening to see such an act,” he said. “Health management systems are beginning to tighten their security.”

Stefanek said patient care was never compromised, nor were hospital records.
Ashland Women’s Health, a solo obstetrician-gynecologist practice in Ashland, Kentucky on April 4 reported to the Department of Health and Human Services a hacking incident affecting 19,727 patients, according to the HHS Office for Civil Rights’ wall of shame website listing major breaches impacting 500 or more individuals.

That incident involved a recent ransomware attack that encrypted data on the practice’s electronic health record system, including its patient scheduling application, an Ashland Women’s Health spokeswoman says.

The practice was able to mitigate the attack and restore data by using backup systems, and did not pay a ransom, she says. Patient care was impacted for “a couple days,” as the practice was unable to access its EHR and scheduling software, and relied on paper charts, while its systems were being restored, she says.

The incident was reported to local law enforcement and the FBI, and investigators told the practice the attack involved HakunaMatata, a variant of NMoreira ransomware, the spokeswoman says.

The practice is preparing to send out notification letters to affected patients, but has not determined whether it will offer free credit or identity monitoring, she says. Impacted data included patient names, addresses and “other” protected health information, she says.
Data Hostage Events

- What is a “data hostage event”?
- Is a ransomware attack a breach? HIPAA is implicated!
- Affects the availability of health information
- Security Rule requires security measures be in place that can help prevent ransomware, particularly through unknown malware deployments
- Just another threat that needs to be considered as part of your regular risk analysis
- A good backup helps but . . . better to try to avoid attack in the first place through employee awareness
Get Your Practice Cyber Ready

- It’s your practice – make sure it’s ready to respond and recover
- Not just for ransomware but required for any potential breach under HIPAA
- If your group does not have an incident response plan, you need one
- When and how do you activate your plan?
- Who do you need to call?
Get Your Practice Cyber Ready

- When was the last time you went over your incident response plan with those on your breach response team or response call list?
- Who in your practice was involved in the response readiness exercise?
- Breach Notification Rule requires notification within 60 days
- Other state laws may require faster response
Cyber Liability Summary

◆ Continue to focus on HIPAA compliance – Privacy Rule *and* Security Rule
◆ Know where your data is stored and determine whether you need a BAA
◆ Perform a risk analysis and update it
◆ Get your practice cyber ready – it’s not a matter of *if* but a matter of *when* a data incident will happen
◆ How prepared is your practice to respond?
ECRI Institute Names Top 10 Patient Safety Concerns for 2017

New report examines root causes for serious patient safety events

This year’s list includes:

1. **Information Management in EHRs**
2. Unrecognized Patient Deterioration
3. Implementation and Use of Clinical Decision Support
4. Test Result Reporting and Follow-Up
5. Antimicrobial Stewardship
6. Patient Identification
7. Opioid Administration and Monitoring in Acute Care
8. Behavioral Health Issues in Non-Behavioral-Health Settings
9. Management of New Oral Anticoagulants
10. Inadequate Organization Systems or Processes to Improve Safety and Quality
“One man’s meat is another man’s poison.”

- Lucretius

~ or ~

“One man’s trash is another man’s treasure.”

But, who is the “other man?”
Five ways technology, and the use of electronic medical records, may be increasing the risk of medical malpractice:

1. Design Flaws.
2. Input Issues/Copy and Paste.
3. Not Using the Product Correctly.

The Law Offices of Tim Misny

I’LL MAKE THEM PAY!

http://misnylaw.com/is-technology-increasing-the-risk-of-medical-malpractice/
Using Medical Records in Your Case

Documentation Issues In Your Case

For Plaintiffs...
The medical record could be the most important piece of physical evidence in a malpractice trial.
EHR mistakes are the accelerant equivalent of rocket fuel.
Classic Attorney Question:
“Are You Still Beating Your Spouse?”

- Do you agree that an accurate record is important to patient safety?
- Do you agree your records contain inaccuracies?
- Do you even bother to look at your records?
- Do you provide the same level of attention to patient care as you do to your record-keeping?
- How can we trust anything in this record? (i.e. How can we trust you?)
Shortcuts to Trouble

- Templates
- Cloned Notes
- Cut and Paste
- Pre-populated Entries
- Post-populated Entries
- Auto-populate/Autofill
- Auto-correct
- Macros
- Drop-down Menus
Every patient is UNIQUE

Every encounter is UNIQUE

DOCUMENTATION of every patient encounter should be UNIQUE
The Problem with Digital Dependency

Every Patient, Every Encounter Looks the Same

- Inaccurate
- Unreliable
- Redundant
- Contradictions
- Irrelevant over-documentation
- Only provides limited options
- Information carryover
- Removes intuition and clinical experience
- Copying/pasting perpetuates incorrect/outdated information
What You Don’t Want to Read

Weak Points:

- “Real problems from staff getting accurate medical records”
- “It seems like every time the staff was asked to produce records to us and to plaintiffs, a different set of records would be produced”
- “Created doubt, confusion and legal hurdles”
- “Led to confusion…further increased suspicion”
- “Doctors don’t know what is in their own records”
Copy & Paste- Contradictory EHR Notes

CHIEF COMPLAINT/HISTORY OF PRESENT ILLNESS: 01/01/2012 11:02
Presented to the emergency department at 11:03 by AMB – POV. The patient was triaged at 11:03 with the following vital signs T: 97, PO: P: 114 regular rate, Resp: 23, unlabored, BP: 148/96, SPO2: 90, pain: 0 denies pain.

Chief complaint — DYSPNEA—ADULT

Exam time: 11:08
History obtained from: patient.
History limited by: patient is a difficult historian.

Onset of symptoms was one week ago, symptoms came on gradually. Symptoms are present and increased from onset. Patient states symptoms are of mild severity. Patient admits to cough, relates chest pain, but fleeting and only present with cough. Patient denies shortness of breath at rest but becomes symptomatic with exertion. Patient admits to shortness of breath while at rest. On 0 to 10 scale patient rates severity of symptoms as 0/10.

Associated signs and symptoms: negative calf pain, negative chest pain, negative fever, negative proximal nocturnal dyspnea, negative orthopnea, negative wheezing, negative vomiting, positive chills, positive dyspnea on exertion, positive dyspnea, positive myalgias, positive nausea, positive sinus pain/pressure, positive sore throat.

REVIEW OF SYSTEMS: SHI 01/01/2012 11:12
Musculoskeletal: negative extremity pain, positive myalgias.
Psychiatric: General: anxious.
Cardiovascular: negative chest pain, negative proximal nocturnal dyspnea, positive edema, negative orthopnea, negative palpitations, negative edema, negative syncope.
Psychological: negative anxious.
Copy & Paste - Contradictory EHR Notes

CHIEF COMPLAINT/HISTORY OF PRESENT ILLNESS: 01/01/2012 11:02
Presented to the emergency department at 11:02 by AMB—POV. The patient was triaged at 11:03 with the following vital signs T: 97, PO: 114, resp: 23, unlabored, BP: 148/96, SpO2: 90, pain: 0 denies pain.

Chief complaint — DYSPNEA—ADULT

Exam time: 11:08
History obtained from: patient
History limited by: patient is a difficult historian.

Patient denies shortness of breath

Patient admits to shortness of breath

Symptoms one week ago, symptoms came on gradually. Symptoms are present and increased from symptoms are of mild severity. Patient admits to cough, relates chest pain, but fleeting and only present with cough. Patient denies shortness of breath at rest but becomes symptomatic with exertion. Patient admits to shortness of breath while at rest. On 0 to 10 scale patient rates severity of symptoms as 0/10.

Associated signs and symptoms: negative calf pain, negative chest pain, negative fever, negative proximal nocturnal dyspnea, negative orthopnea, negative wheezing, negative vomiting, positive chills, positive dyspnea on exertion, positive dyspnea, positive myalgias, positive nausea, positive sinus pain/pressure, positive sore throat.

REVIEW OF SYSTEMS: SHI 01/01/2012 11:12
Musculoskeletal: negative extremity pain, positive myalgias.
Psychiatric: General: anxious.
Cardiovascular: negative chest pain, negative proximal nocturnal dyspnea, positive edema, negative orthopnea negative palpitations, negative edema, negative syncope.
Psychological: negative anxious.
Copy & Paste - Contradictory EHR Notes

CHIEF COMPLAINT/HISTORY OF PRESENT ILLNESS: 01/01/2012 11:02
Presented to the emergency department at 11:03 by AMB – POV. The patient was triaged at 11:03 with the following vital signs T: 97, PO: P: 114 regular rate, Resp: 23, unlabored, BP: 148/96, SPO2: 90, pain: 0 denies pain.

Chief complaint – DYSPNEA—ADULT

Exam time: 11:08
History obtained from: Patient
History limited by: patient is a difficult historian.

Patient denies shortness of breath
Relates chest pain

Patient admits to shortness of breath

Negative chest pain

Evaluates symptoms one week ago, symptoms came on gradually. Symptoms are present and increased from one week ago. Symptoms are of mild severity. Patient admits to cough, relates chest pain, but fleeting and only present with cough. Patient denies shortness of breath at rest but becomes symptomatic with exertion. Patient admits to shortness of breath while at rest. On 0 to 10 scale patient rates severity of symptoms as 0/10.

Associated signs and symptoms: negative calf pain, negative chest pain, negative fever, negative proximal nocturnal dyspnea, negative orthopnea, negative wheezing, negative vomiting, positive chills, positive dyspnea on exertion, positive dyspnea, positive myalgias, positive nausea, positive sinus pain/pressure, positive sore throat.

SYSTEMS REVIEW: SHI 01/01/2012 11:12
Musculoskeletal: negative extremity pain, positive myalgias.
Psychiatric: General: anxious.
Cardiovascular: negative chest pain, negative proximal nocturnal dyspnea, positive edema, negative orthopnea negative palpitations, negative edema, negative syncope.
Psychological: negative anxious.
Copy & Paste - Contradictory EHR Notes

CHIEF COMPLAINT/HISTORY OF PRESENT ILLNESS: 01/01/2012 11:02
Presented to the emergency department at 11:03 by AMB – POV. The patient was triaged at 11:03 with the following vital signs T: 97, PO, P: 114 regular rate, Resp: 23, unlabored, BP: 148/96, SPO2: 90, pain:0 denies pain.

Chief complaint — DYSPNEA—ADULT

Exam time: 11:08
History obtained from: patient.
History limited by: patient is a difficult historian.

Patient denies shortness of breath
Patient admits to shortness of breath
Relates chest pain
Negative chest pain
Negative edema
Positive edema

Associated signs and symptoms: negative calf pain, negative chest pain, negative fever, negative proximal nocturnal dyspnea, negative orthopnea, negative wheezing, negative vomiting, positive chills, positive dyspnea on exertion, positive dyspnea, positive myalgias, positive nausea, positive sinus pain/pressure, positive sore throat.

SYSTEMS REVIEW: 01/01/2012 11:12
Musculoskeletal: negative extremity pain, positive myalgias.
Psychiatric: General: anxious.
Cardiovascular: negative chest pain, negative proximal nocturnal dyspnea, positive edema, negative orthopnea negative palpitations, negative edema, negative syncope.
Psychological: negative anxious.
Copy & Paste- Contradictory EHR Notes

CHIEF COMPLAINT/HISTORY OF PRESENT ILLNESS: 01/01/2012 11:02
Presented to the emergency department at 11:03 by AMB – POV. The patient was triaged at 11:03 with the following vital signs T: 97, PO: P: 114 regular rate, Resp: 23, unlabored, BP: 148/96, SPO2: 90, pain:0 denies pain.

Chief complaint — DYSPNEA—ADULT

Exam time: 11:08
History obtained from: patient.
History limited by: patient is a difficult historian.

States one week ago symptoms came on gradually. Symptoms are present and increased from symptoms are of mild severity. Patient admits to cough, relates chest pain, but fleeting and only present with cough. Patient denies shortness of breath at rest but becomes symptomatic with exertion. Patient admits to shortness of breath at rest. On 0 to 10 scale patient rates severity of symptoms as 0/10.

Associated signs and symptoms: negative calf pain, negative chest pain, negative fever, negative proximal nocturnal dyspnea, negative orthopnea, negative wheezing, negative vomiting, positive chills, positive dyspnea on exertion, positive dyspnea, positive myalgias, positive nausea, positive sinus pain/pressure, positive sore throat.

SKU OF SYSTEMS: S1 01/01/2012 11:12
Musculoskeletal: negative extremity pain, positive myalgias.
Psychiatric: General: anxious.
Cardiovascular: negative chest pain, negative proximal nocturnal dyspnea, positive edema, negative orthopnea negative palpitations, negative edema, negative syncope.
Psychological: negative anxious.
**Weak points:**

These are numerous. I'll just start at the beginning. (1). The group’s EMR has a massive issue, such that when you enter an allergy at one visit it then retroactively flags every other visit with that allergy. Therefore this allergy appears on every note beginning with the very first visit. Fortunately, the separate physician notes show a history of no known drug allergy.
“I documented the exception as the norm.”
Template Language

“The patient did complain of leg paresthesias on the affected side. The needle was withdrawn slightly, about 1 mm, and the symptoms improved.”
Defense Attorney Report

Weak Points:

- “All six reports are identical. Dr. James acknowledged that he used a template, and he further admitted to error in its use.”
- “Dr. James admitted that this was a ‘meaningless paragraph’”
- “This casts doubt on the entire procedure report…”
- “…ordered two injections, yet three were scheduled…”
- “A valuable defense tool has been compromised.”
Defense Attorney Report

Conclusion:

The defense of any malpractice case is helped greatly by contemporaneous record of events. It can overcome the contrary memory of the plaintiff, refresh the memory of the defendant and corroborate the physician’s description of his routine practices, even though the doctor has no specific memory of the event.

In this instance, the jury will be told that they cannot trust the reports to be a reliable account of what Dr. James did on a given day, or a reliable indicator that Dr. James followed his invariable routine. A valuable defense tool has been compromised.
CARRY-OVER VIDEO

“I can explain it away later if I need to.”
Defense Attorney Report

General Issues:

- “This practice group utilizes an EMR which pulls up a previous finding”
- “He pulled information forward from Dr. Hall’s visit, reflecting information gathered on her first post-op visit”
- “Dr. Gibson’s review of symptoms notes she c/o drainage from incision, fever, frequency and urgency with urination”
- “Dr. Gibson does not recall her making these complaints at that visit…Nonetheless that is what the chart reflects”
Issues that warrant an attempt to settle the case:

- “Plaintiff has seized on the fact that there are entries in our pre-operative physical examination that did not happen”
- “Entries were pulled over by mistake from a template”
- “Make our records not only suspect, but patently untrue”
- “Attempting to raise medical fraud”
Expert Review

Weak Points:

“The presence of incorrect documentation in the electronic medical records is certainly a weak point. If the records indicate that a pelvic and rectal exam were done, and they were not, this will be pointed out as fraudulent by the plaintiff’s team. That said, the electronic medical record has been forced upon caregivers who are just now learning to use it properly. I am afraid it is not unusual for caregivers to use templates and inadvertently misdocument. The most diligent physicians, I believe, will avoid this, however.”
The Audit Trail Is Unforgiving

The Timeline Is No Longer a Guessing Game

- Date and time stamp records
- For how long
- Who accessed the information
- What records were accessed
- On what occasion(s)
- What records were not accessed
Plaintiff’s Expert

- He will specifically discuss discrepancies in the EHR and problems raised by the audit trails.
- Additionally, the audit trails show different dates as “last saved”...no indication of authorship...entries made after the patient was last seen, some by individuals not even employed by Dr. Johnson.
- The numerous discrepancies make the record untrustworthy, incomplete and inaccurate.

Memorandum
From: Sean Garrett, Esquire
RE: Dr. Michael Smith, Medical Informatics Expert

September 7, 2023

Dr. Michael Smith is a multi-disciplinary Medical Informatics professional with expertise in healthcare information technology design and implementation errors, systems defects and other factors that create a risk and cause patient injury and in electronic medical record integrity. He has developed expertise in establishing a forensic search for modification, alteration, deletion and other spoliation of medical records both within and outside the electronic medical record system. He is expected to testify regarding electronic medical records of patient, Mr. Long as well as problems raised by the audit trails for these records. He also testified about numerous discrepancies in the records produced by Dr. Johnson, including but not limited to the absence of the date and time of the e-signatures for the office visit, the fact that each set of electronic medical records produced by the Johnson are materially different and later productions contain additional information including phone messages, blank phone messages, handwritten annotations, additional nursing notes and a medication summary list. Additionally, the audit trails for these records show different dates as “last saved” for some audit trail sections with no indication of authorship, as well as entries made after Mr. Long was last seen in the office, some of which were entered by individuals they were not even employees of Dr. Johnson. The numerous discrepancies make the record untrustworthy, incomplete and inaccurate.

Sincerely,

Sean Garrett

Sean Garrett, Esquire
“About a Minute and a Half”
Audit Trail Video

“I just learned the bare minimum I needed to know in order to get by.”
Defensibility Issues

Weak Points:

- "Dr. Morgan admitted he does not, as a matter of routine, review all orders of the emergency-room physician for patients who are admitted to his service. Instead, he relied upon the presence of the Imaging Services Progress Note to be informed of tests that were not ordered by him."

- "Dr. Morgan conceded, however, that the x-ray report was sent to his office."

- "On cross examination from the hospital’s attorney…"

- "Dr. Morgan testified that no hospital representative had ever told him to use the Image Services Progress Notes as a mode of communication."
Contemporaneous Documentation

Plaintiff Attorney-Cross Examination

Q: Why did you wait nearly 8 hours after the emergency consult was called to see the patient?

A: I saw the patient within 30 minutes but wrote the chart note later.

Q: So you claim you saw this critically ill patient, spent an hour with him and then waited over 6 hours to write your note after you had seen other patients and your memory had faded?
Communicating Information

**TASKING**

- Do you check your in-box/task box at least daily?

- If a staff member is not in the office (sick or on vacation), is another employee designated to check his/her task box?

- Do you realize tasking/messaging is a legal part of the medical record?
  
  *Be prudent with your choice of words.*
Reading an EHR Is Like Taking a Drink from a Fire Hydrant

Information Overload

Provider is presumed to know the entire chart

Information is available immediately
User Error

- Incorrect Information Input
- Lack of Training/Familiarity
- Over-documentation
- Digital Dependence
- Alert Fatigue
- E-signature
- Sharing Login/Password
- Screen Differs from Printout
Take-Aways EHR-Specific

- Be aware of how the printed record reflects care
- Train and re-train/keep your system updated
- Use dropdowns and templates sparingly
- Customize templates to each patient (especially for H & P)
- Utilize narrative text option
- Manage alert overrides responsibly

Be aware of how the printed record reflects care
Train and re-train/keep your system updated
Use dropdowns and templates sparingly
Customize templates to each patient (especially for H & P)
Utilize narrative text option
Manage alert overrides responsibly
Take-Aways – Documentation
(Electronic or Paper Records)

- Prepare notes at same time as encounter
- Update problems and medication lists each visit
- Document consistently in the same location
- Use patient’s own words whenever possible
Telemedicine
Our doctors commonly treat a wide range of conditions through our telemedicine service.

**Conditions we treat by telemedicine:**

- Acne
- Allergies
- Constipation
- Cough
- Diarrhea
- Ear problems
- Fever
- Flu
- Headaches
- Insect bites
- Nausea / vomiting
- Pink eye
- Rashes
- Respiratory problems
- Sore throats
- UTI
- Vaginitis
- and more
Who is it guiding patients away from you?

- Employers
- Insurance plans
- Telemedicine companies
- Schools
- Others
Telemedicine

- Concepts and definitions
- Payment considerations
- Telemedicine in Tennessee
- Establishing the provider-patient relationship in telemedicine
- Telehealth liability considerations
“Telehealth”

or

“Telemedicine”?
Concepts and Definitions

- **Telehealth** includes telemedicine and communication with medical monitoring devices.

- **Examples:**
  - Blood Glucose Monitors
  - Activity Trackers
  - Blood Pressure Monitors
  - Smartphone Apps
Concepts and Definitions

- **Telemedicine** refers to bilateral and interactive communications between a provider and a patient, including communications between clinicians on both ends of the exchange.

- **Examples:**
  - Images transmitted between radiologists
  - In some circumstances, direct patient to provider contact
  - Consultations where a practitioner presents a patient to a specialist remotely
Concepts and Definitions

Telehealth Modalities

- Live video (synchronous communication)
- Store-and-forward
- Remote patient monitoring
- Mobile health
Concepts and Definitions

- Telemedicine is practicing medicine

- Telemedicine is not
  - A patient accessing their records via a patient portal
  - A phone call from a nurse to a patient reminding of an appointment
  - Providing an informal opinion to an attending physician and not directly to patient
What do patients say about telemedicine?

- 59% would choose a primary care doctor who offers a patient mobile app over one that does not.
- 62% “strongly” or “somewhat agree” that they would use virtual care treatments such as a video conference call instead of in-office visits.
- 52% of Millennials (18-34) would choose a primary care doctor who offers virtual care treatment options over one that does not.
- 78% would want their doctors to have access to health data from their wearable devices.

Source: Salesforce Research, 2016 Connected Patient Report
This survey was conducted online within the United States by Harris Poll on behalf of Salesforce from June 8-10, 2016, among 2,025 U.S. adults ages 18 and older, among whom 1,736 have health insurance and a primary care doctor. Used with permission from Salesforce.
Payment for Telehealth Services

- Tennessee’s “payment parity law” became effective January 1, 2017
- Tennessee law provides for parity in health insurance coverage for telemedicine services and traditional medical services
- Requires health insurers providing coverage in Tennessee to “provide coverage under a health insurance policy or contract for covered healthcare services delivered through telehealth”
- Commercial payers cannot exclude coverage for service solely because it is provided through telehealth
Is it Telemedicine?


Used with permission from NBC News.
Telemedicine in Tennessee

Licensure/Regulatory Requirements

- New regulations effective October 31, 2016
- MBE Telemedicine FAQ
- Consult with an attorney familiar with telemedicine regulations regarding the specifics of your practice
- Must be a licensed Tennessee physician
Telemedicine in Tennessee
MBE Definition of Telemedicine

“Telemedicine is the practice of medicine using electronic communication, information technology or other means, between a licensee in one location and a patient in another location. Telemedicine is not an audio only telephone conversation, email/instant messaging conversation or fax. It typically involves the application of secure video conferencing or store-and-forward to provide or support healthcare delivery by replicating the interaction of a traditional encounter between a provider and a patient.”

Tenn. Comp. R. & Regs. 0880-02-.16(g)
Telemedicine in Tennessee
MBE Definition of Telemedicine

“Telemedicine is the practice of medicine using electronic communication, information technology or other means, between a licensee in one location and a patient in another location. Telemedicine is not an audio only telephone conversation, email/instant messaging conversation or fax. It typically involves the application of secure video conferencing or store-and-forward to provide or support healthcare delivery by replicating the interaction of a traditional encounter between a provider and a patient.”
Telemedicine in Tennessee
Practical Considerations

- Important to know whether what you are doing constitutes telemedicine practice whether you intend to bill for it or not
- By statute, held to the same standard of care that would apply to an in-person encounter
Is it Telemedicine?

- A FaceTime call by an existing patient during dinner
- A video conference in your office with an existing patient's friend while they are on vacation
- Video conferences by nurse practitioners and physician assistants
Best Practices

- Use a secure platform within your practice
- Existing patients
- EHR access available
- By appointment
A physician-patient relationship may be established whether or not there has been an in person encounter between the physician and the patient.

A healthcare provider-patient relationship is created by mutual consent and mutual communication between the patient and the provider—exception for emergencies.

Consent by the patient may be expressed or implied consent.

Unless a prior relationship exists, a provider-patient relationship is not created “simply by the receipt of patient health information by a provider.”

Duties and obligations do not arise until the healthcare provider:

- “Affirmatively undertakes to diagnose and treat the patient;”
- “Affirmatively participates in the diagnosis and treatment.”
Do I Know You?

- An existing patient who you have treated for 10 years
- New patient you will later see in the office if necessary
- A new patient you will never see in an office
- Is the patient under 18?
  - Facilitator required (follow MBE guidelines)
Telehealth Liability Considerations

- Does a telehealth encounter create a patient-physician relationship?
- Look to state statutes and regulations to determine scope and nature of patient-physician relationship
- Treatment is usually considered rendered in the jurisdiction where patient is located
- One contact can establish patient-physician relationship – likely does not require systematic or numerous contacts
Telehealth Liability Considerations

- Who is responsible for compliance?
  - Telemedicine company
  - You
Telehealth Consent Considerations

- Consider having a telemedicine consent form prepared for your practice
  - May specify or limit location of treatment to make more analogous to in-person encounters
  - Treating on vacation
  - Anywhere on mobile device
Summary

- Telemedicine and, more broadly, telehealth is a rapidly changing and growing segment of the healthcare industry.
- There are not clear answers for many areas of telemedicine.
- Understand licensure and regulatory requirements for each encounter.
- Consider the risks involved with different types of encounters and examine ways to reduce those risks.
Patient Portals

Gateway to ...
The Positives of Portals

- Encouraged by the Government
- Provides other providers to view previous communications
- Provides patients with a convenient means to access their medical records (data log verified)
- Easily incorporated into the patient’s chart
- Allows the physician and staff to work remotely
- Promotes efficiency: decreases telephone interaction; medication refills; appointment reminders; non-urgent/routine lab/test results; Informed Consent forms/Informed Refusal; etc.

Encouraged by the Government

Provides a safe, secure means to communicate with patients (and family members)

Provides patients with a convenient means to access their medical records (data log verified)

Easily incorporated into the patient’s chart

Promotes efficiency: decreases telephone interaction; medication refills; appointment reminders; non-urgent/routine lab/test results; Informed Consent forms/Informed Refusal; etc.
The Negatives of Portals

- Authentication
- HIPAA Security Rule
- Providers don’t check portal regularly
- Patients don’t use the portal
- Target of Cybercrime
- Failure to outline what services and information are available as well as limitations (set parameters)
Authentication

◆ What is it?

Process used to verify whether someone or something is who or what it purports to be in the electronic context, while keeping unauthorized people or programs from gaining access to information.

◆ Typically, this consists of user names and passwords.

◆ The Person or Entity Authentication standard of the HIPAA Security Rule requires that the covered entities and business associates implement “reasonable and appropriate” authentication procedures to verify that a person or entity seeking access to electronic health information is the one claimed.
Access Challenges

- Spouses?
- STD testing?
- Divorced parents?
- Who has access?
- Minors?
- Privacy rights relative to sexual reproduction, STD testing?
- Mental health treatment?
- Substance abuse treatment?
So, What Should You Do?
Disclaimer/Terms of Use and Privacy Policy Document

- Prepared by legal counsel
- Two to fifteen pages in length – shorter is usually better
- Typically furnished by vendor or IT professional – must be tailored to your practice
- Policy on access and release of patient’s medical record (specifically address minors if applicable)
- Discusses risks and patient’s need to keep login info secure
- Rights and responsibilities of both parties
- Warns patients not to use for communication in emergencies
Practice Responsibilities

- Familiarize yourself and ensure your co-workers have familiarized themselves with the system.
- Verify whether a particular patient is using the portal.
- Assign someone clinical to check the portals at least once per day – preferably twice per day. Have a back-up person assigned in the event of vacation or illness.
- Don’t leave orders that require patient instructions or medication changes on the portal.
- Engage the portal and use the system.
Justin Joy is an attorney with Lewis, Thomason, King, Krieg & Waldrop, P.C. in the Memphis, TN office. He has a variety of experience in the area of information privacy and cybersecurity including security incident investigation, security awareness and policy drafting, cyber risk management including insurance policy coverage consultation and breach response management. He also provides counsel in healthcare liability defense and healthcare compliance matters. As Lewis Thomason’s chief privacy officer, Justin promotes an awareness of privacy and security-related issues for the firm. Justin has earned the Certified Information Privacy Professional/United States (CIPP/US) credential through the International Association of Privacy Professionals (IAPP).
About the Speaker
Jeffrey A. Woods, JD

Jeffrey A. Woods is the Director of Risk Education in the Risk Education and Evaluation Services Department at SVMIC. Jeff received his Bachelor of Science degree from the University of Tennessee Martin and his Juris Doctorate degree from the University of Tennessee Knoxville. Following graduation, he practiced law in Knoxville, Tennessee for 15 years, advising physicians and healthcare providers and defending them in malpractice claims. He is licensed to practice in Tennessee and all Federal courts, including the United States Supreme Court. He is a member of the Tennessee Bar Association.

Jeff joined SVMIC in 2003 and was a Senior Claims Attorney until 2015 when he transferred to his current position.