The Last Mile – Bringing Privacy and Security to the Patient Experience – Opportunities and Challenges

Mitchell Parker, Exec. Dir., IS, IU Health

Amy Stiner, RN, MBA, MPA Advisor with the Defense Acquisition and Policy Department at MITRE

Indiana University Health

Purpose of Presentation

- To discuss the issues with processes not keeping up with the technologies present in Electronic Medical Records and how organizations can bring Privacy and Security to the patient experience in multiple ways

Where do we begin?

- Organizations have made large investments in Electronic Medical Records and Patient Portals
  - This is to meet the requirements of the HITECH Act and Meaningful Use Programs, yet information in them is not meaningful for physicians.
- Organizations have also made large investments in Internet of Things, Mobility, Wearables, and Applications to provide enhanced care and proactive monitoring and response
- They want to reduce length of stay and increase patient engagement and satisfaction

Where are we now?

- We have very large monolithic Electronic Medical Records systems in place
- Some of them are so customized to workflows instead of following standard models that they hold data hostage
  - It takes a long time to get data in or out as it takes programming to do so in many cases
  - Integrating new technologies becomes a challenge
- A number of applications have been developed to address corner cases the EMRs don't
- Clear legal issues with bundling EMR service with shared venue of care partnerships e.g. Satellite Locations within other health systems

Where are we now?

- We've attempted to make the EMRs fit the business, instead of examining how the business really operates and optimizing processes and workflow
  - The opposite of what many businesses did when implementing Enterprise Resource Planning and bringing on the Big 4 to help
- We have added on additional workflow with the EMR without consideration for the additional work the EMR causes
- Privacy and Security has traditionally not been involved with ancillary business processes
  - Often an outgrowth of the CISO role starting in Infrastructure
  - And Privacy being a secondary role for many staff attorneys

What does this leave us with?

- We have customized 2000's era EMR systems driving practices with 1970's era workflows and policies to meet the demands of the 2010's/2020's
- Overworked clinicians
- Processes from the distant past in a digital world
- Slow to change because the focus is on revenue generation and retention in a very financially uncertain space with very low margins
- Increasing amounts of M&A and competition
- Development of large disconnected corporate structures that make communication very difficult (e.g. clinics, ambulatory diagnostic, satellite locations)

Let's Focus - Agenda

- What are the privacy and security gaps in the patient experience?
- How do they have real life effects?
- How can we work around these for the benefit of the patients and their families?
- How can we improve workflow as providers?
  - How can we better drive change?
  - How can we better communicate?
  - How can we better and more securely transfer information between each other, the patient, external second opinions or transfer of care, and external members of a care team?

What are the gaps in the experience?

- The two big ones:
  - Patient Portals don't capture everything people need and aren't fully two-way
  - You have to be seen before given an EMR shell to store imported information and or access to the portal at many providers
    - Uploading patient-supplied data isn't allowed in many workflows
  - Release of Information at many institutions is a paper-based process with some electronic exceptions that is still roughly the same one followed from the 1970's with paper records
  - The provider culture sees faxing as a viable option for secure information exchange, but not from the patient side. Very few options exist for patients to fax forcing them to use unsecure and expensive retail locations (e.g. Pay by the faxed page at Staples, Office Depot, FedEx Office)

Security Issues

- Paper Forms sent via Fax or the Postal System
  - Multiple People can view the records
  - No audit trails on who sees what / no closed loop processes
    - Can lead to privacy issues that are impossible to trace and no time frame to determine if there has been a breach
  - Anyone can take pictures with a smartphone and anonymously transfer data
  - Paper gets lost and is difficult to organize
  - There are a lot of lost or misplaced letters in the postal system—especially in large complicated academic healthcare environments. (e.g. What is the destination provider mail box, hospital, clinic location, clinic HIM, or hospital HIM?

Security Issues

- Faxes
  - Left all over the place
  - Still a lot of junk faxes intermixed with real patient data
  - Not high quality
  - Devices are unreliable
  - Oftentimes items left on faxes and not picked up
  - Often legacy technologies that have not been updated in 10-15 years
  - Have you ever successfully faxed 20 pages or more without a glitch? (e.g. Machine jam, double pages going through, and the dreaded staple in the middle.) We expect patients to send hundreds of pages successfully this way

Security Issues (continued)

- Faxes
  - Spotty audit trails – sometimes there, sometimes not
  - Not everyone understands logging on newer phone systems for Voice or Fax over IP Networking
  - A lot of vendor misunderstanding with Accounting of Disclosure Requirements
  - CMS Administrator Seema Verma calling for their end by 2020 (yay!)
  - Like paging, yet another legacy technology that many health systems may not have the resources to fully move from nor a transformational/change management plan on how to get there

Tracking Requests

- Much of this is still done manually…if tracked at all. In speaking with several organizations over the last year.
  - Nearly all could not determine if :
    - Was a request received, processed, or sent?
    - When was it processed?
    - Where was it sent?
    - When was it sent?
    - Was it received by the intended recipient?
    - On the receiving side—was the provider and patient informed that the records arrived?
- Staff need to collate and organize papers for physician review
- Still a paper-based process

Tracking Requests (continued)

- Receiving organizations of new patients (e.g. second opinion or transfer of care)—many times have no EMR shell for the patient information to placed in electronically until the patient actually presents for the appointment.
  - There is no communication between scheduling and medical records to import the information into the EMR shell, which means the provider is not able to review the information before the first appointment.
    - Remember—patients are not being scheduled before medical records are received because its critical for the appointment.
    - -You can track your pizza order, but track your medical records? Not so much.

Tracking Requests (continued)

- Since tracking does not exist, no one knows if there has been a breach and if so when and where did it occur?
  - Is the information in HIM? The clinic?
  - Is the information in an envelop waiting to be opened in a pile?
  - Is it actually lost?
  - Was it ever sent?
  - Who is responsible for breach notification for the patient?
    - In most cases the patient notifies the organization their information is lost, missing, or maybe never sent to begin with, because the patient is tracking. We have unintentionally made breach management a patient responsibility!!

Email

- Just because it's electronic doesn't necessarily mean that it's secure
- School nurses and care providers need to be involved in the process and have copies of medical records—as a result emailing becomes the default communication style between these entities.
- Email is not a good vehicle for capturing structured information
  - Or keeping it secure
  - You're only as secure as the least secure endpoint that can access it
  - Size restrictions by institutions on attachments

The Onus is on the Patients and Care Givers

- Onus on paperwork and files for chronic patients
  - Especially special needs kids
  - Patients and Care Givers have a lot of stress to organize everything
  - Large number of requests that Patients and Care Givers need to file for each type of record or encounter

The Onus is on the Patients and Care Givers

- Redundant consenting processes “Dr. Jones, you can speak with Dr. Johnson.” “Dr. Johnson, you can speak with Dr. Jones.”
- Again, we have made the patient and care giver responsible for:
  - tracking information flow from one organization to another
  - organization breach management
  - provider to provider handoff continuity of care
  - notifying the provider that the records have been received by the provider being notified and are ready for their review
    - **“Hi Dr. Jones, I just wanted to let you know that you have those records now and you can take a look at them.” (Seriously???)**

Multiple Stakeholders

- There is an issue of multiple stakeholders for foster kids, divorced Patients and Care Givers, etc.
  - Need to validate and verify who has accessed these records
  - Need to make sure that all parties have copies
  - Foster kids – caseworkers and manages make decisions – need to get them current copies to they can make educated choices
  - Legal teams at hospitals – they need all the information possible to help make educated and informed decisions in concert with all parties
    - We have a patient consent form for each individual business process and completed for each direction of information flow
  - Care teams – they need information to help make decisions

Organizational Issues

- No easy way to organize and track everything
- Need to facilitate this as patients and care givers spend a lot of time putting everything together, even from the same hospital for different departments
- What happens when a patient or care giver loses “the folder”?
- Turn around time or service level agreements are vague for patient expectations delaying breach discovery .
  - “You’ll receive your records in 2-4 weeks.”
  - Delaying patient care because appointments aren’t scheduled

Organizational Issues (continued)

- There is a misconception that the cloud doesn't work and that it can't be used to send patient information
  - There has been a aversion to the cloud in healthcare
  - Need to convince others that it can work
  - Apple has started down this path with Apple Health
    - Others will follow!

Risk-Averse Culture

- Organizations don't want to assume responsibility or potential liability for anything they do not absolutely need or want to own
- Even though it's a benefit, people don't want to "own" patient data
- Providing "lockers" in a risk-averse space is a major potential liability for providers
- No way to validate or verify records using PKI
- Irony of the Risk Averse Culture:
  - We aren't tracking records to prevent a breach.
  - Are we trying to 'consent' our way out of accountability?

What are the Effects?

- Information in formats that cannot be used efficiently – unstructured data
- Care providers have enough issues with EMRs
  - Increase in Remote Access so doctors can chart at night and during off hours
  - Having them wade through hundreds of pages of data at 200 DPI from faxes or bad scans with no time due to having to chart with bad workflow
  - Information in formats that cannot be validated
  - Information may not even be available in the chart to be used by providers because of delays in finding and uploading the information.

What are the Effects? (continued)

- Delays in care for patients
  - Doctors won't see patients until they've had a chance to review the records
  - There is no way generally to notify patients when providers have all the records and can schedule them
  - No feedback loop closure
  - An overwhelming amount of information that can lead to follow up failure and the lack of proper diagnosis
  - Omission of critical information
  - Unrecognized and unaccounted for breaches of information

What are the Effects?

- All parties need to be involved
  - Schools are mandatory reporters
  - We don't want people called out by DYFS/DCFS for neglect
- Cybersecurity risk by having non-parent stakeholders omitted for information disclosure because of fear –remedied by poor patient workarounds without secure means of exchange—'Wild West Model'
- Information is not sent due to lack of fax machine access by patients and care givers
- We need better clarification of SAMSHA and HIPAA being sent by Patients and Care Givers and how they can effectively communicate it
  - Lack of information can lead to adverse consequences

Now that we've talked about a lot of issues, how do we solve this?

- **This is a workflow process and change management solution, not just a technology one!**
- We need to get better at improving processes around:
  - Patient Portal appointment scheduling
  - Patient Portal Scheduling for Multiple Specialists
  - Making Request Of Information requests more clear??
  - Better definitions on handoff and workflow processes of request tracking. Closed loop!
  - Clear protocols for recognizing lost, data breach mitigation, and management.

Close the Loop with Explanations and Tools for Patients!

- GDPR isn't just the Right To Be Forgotten
- Explain the whys of privacy and security practices in clear language and how we will protect their information—provide assurances
- Give them someone to reach out to, not just a number to a department voicemail
- Provide them with electronic medical record and information exchange consenting processes. We have done this for billing and now its time to do the same for information security.
- Provide the patient and providers involved with closed loop medical record status notifications
- Enable secure tools for patients to electronically contribute documents and images to their records or to HIM

Closing the Loop in Workflow Processes and Staff Skills

- Provide information on how we will contact and communicate with them and set expectations
  - We explain procedures to patients, especially children. Why not privacy and security?
  - Explain how it's like protecting credit cards at the store
  - People do not understand portals well. We need to take the time here to make it as easy as sharing their lives on Facebook
- Collect as much information as possible online before the first visit
- Reduce Paperwork
  - Why print and fill out when we can do everything online with a portal?

Closing the loop with Technology

- Start exploring use of Apple Health to accept information
  - Or an equivalent with a portal to grant access to records like Box.com can for discretionary access to involved parties
    - Box.com and other players have done a lot in the provider space, but there is still a need for consumers to take control of their own data and share it themselves
    - The processes are just too long and onerous and can lead to many delays
    - Portals need to take attachments with generous size limits (> 10 MB)

Emerging Technologies

- There's a great use for Blockchain here – verifying and validating hashes of medical records that patients are empowered to send on their own
- FHIR Transfers of data using APIs
- Give patients their records in a format they can use
- Give them power over electronic data exchange
  - When we make patients the brokers of information: it needs to be efficient, secure, and allow for sufficient information exchange that is clinically robust and meaningful.

What can providers do?

- Improve engagement and communication internally!
  - Rounding and walkthroughs by Privacy and Security Team and Practice Managers
  - Getting the Privacy and Security Teams to see the whole picture and empathize
  - Use walkthroughs as part of risk assessments and risk management plans to drive change
  - Feeding forward information to use in design process and process improvement
    - If you do not document it – it does not exist

What can providers do?

- Ambulatory care venues need to become a point of process improvement emphasis from the patient journey perspective
  - Measure current state of delays from the time of requesting records to the time of scheduling the appointment.
  - Electronic processes:
    - Requesting medical records
    - Consenting for information sharing
    - Pre-Appointment/Waiting Room Health History Forms (end verbal and handwritten disclosure of sensitive information at the front desk and waiting room)

What can we do?

- Connect To Purpose, Mission, and Values
  - Model Good Behavior
  - Make it Relevant for the Practice
  - Communicate the “whys” of privacy and security
  - Empathize with the patients and work with them – think in their shoes
  - Develop transformation and change management plans for new electronic HIM processes and migration from fax/paper. Develop HIM champions for leveraging electronic information exchange
  - Don’t hide from patients and care givers need to escalate an information exchange issue
  - Change is hard but its time!

Thank you!

- Do you have any questions?