

Managing the Privacy and Security of Patient Portals

Jacki Monson, JD, CHC
Chief Privacy Officer



Adam H. Greene, JD, MPH
Partner



Mayo's Experience with EHR portal

- Mayo Clinic's biggest site (Rochester) implemented in 2011
- Over 200,000 patients are currently using the portal
- Feedback is extremely positive, especially as new features are added
- Mobile application
 - Includes appointment reminders

HIPAA's Right of Access

- HIPAA: Patient is entitled to “designated record set”
 - Medical record
 - Billing record
 - Other records used to make decisions about patient
- EHR portal is limited to portion of medical record
 - Patient is entitled to more information than is available through EHR portal

Mayo's Experience with Use of Portal

- Positive feedback from patients who can read their records at their convenience, including sharing electronically with their home provider
- Employees who are patients are being encouraged to use it instead of accessing through the EMR

HIPAA's Right of Access

- HIPAA provides that individual is entitled to requested form or format, if readily producible
 - If not readily producible, default is hard copy or electronic copy, depending on whether maintained electronically
- EHR portal is not everyone's requested form or format
 - Covered entity must continue to provide alternatives, such as hard copies

Mayo's Experience with Form of Requests

- The portal has resulted in 50% increase in medical record requests
 - Most patients still want paper copies



HIPAA's Right of Access

- HIPAA permits covered entity to deny access for numerous reasons
 - Reasonably likely to endanger life or physical safety
 - References another person and reasonably likely to cause substantial harm to such person
 - Request by personal representative and access is reasonably likely to cause harm
 - Obtained from non-health care provider under promise of confidentiality

HIPAA's Right of Access

- To what extent does EHR portal include information that may cause harm?
- Can clinicians act proactively to flag information that could cause harm?



Mayo's Experience with Denial of Access

- Not all clinical notes are released to the portal
 - Providers can mark notes confidential, which prevents the release to the portal
 - Mayo balances risk when reviewing types of clinical notes to release to determine confidentiality concerns
- Areas that pose the most challenge:
 - Family Medicine
 - Women's health
 - Psychiatry
 - Transplant

Who May Access the Portal?

- Individual
- Authorized person
 - Authorization must comply with HIPAA
 - There may be state law requirements
- Designee
 - Must be in writing (including electronic)
 - Must designate who and to what address

Personal Representatives and Minors

- Personal representative has rights of individual – including right to access in form or format requested if readily producible
 - Personal representative rights should cut off at age of majority
- Personal representative can authorize access by third party
 - Guidance indicates that authorization survives age of majority, so third party can continue to access EHR

Strategies for Personal Representatives

Parent may not be personal representative for certain information (e.g., when minor can consent under state law)

- Segment data (e.g., parent does not get access to certain PHI)
 - Include with restricted access; or
 - Exclude from portal
- Restrict certain ages
 - Exclude certain ages (e.g., 15 to 18) from portal; or
 - Only include with minor's authorization

Mayo's Experience with Personal Representatives

- Both authorizations and minors pose significant challenges to Mayo
 - Mayo requires authorization before establishing proxy rights to the portal
 - Continued challenges with:
 - Revocation of authorization
 - Restriction requests

Minors at Mayo Clinic

- Age 0-12
 - Release most clinical notes to portal
 - Parents have full access
- Age 12-17
 - Family medicine, women's health, and psychiatry is generally not available
 - Have granted access to minors with parent's permission
 - Parents have access to financial information
 - Make exceptions for more access for critically ill minors
 - Transplant
 - Cancer
 - Right to self-pay
- Age 18 and Over
 - Revoke parent's access to all except financial proxy right

HIPAA's Right of Amendment

- Patient has right to request amendment of designated record set information
- Covered entity has limited basis for denial
 - PHI was not created by the covered entity
 - Outside of designated record set
 - Accurate and complete
- If denial, individual can add statement of disagreement to record

HIPAA's Right of Amendment

- EHR portal provides potential means for submission of amendment requests
- Amendment functionality of EHR may differ significantly



Mayo's Experience with Amendments

- 100% increase in HIPAA amendment requests
- Trend
 - Information is readily available to review
 - Convenient to submit request through portal



Mayo's Experience with Amendments

- Benefits
 - Some corrections are important (R leg vs. L leg) and prevent future patient safety concerns
 - Patients are easily able to exercise their HIPAA right
- Challenge
 - Unsigned notes are released to portal (significant corrections prior to physician sign off)
 - Difficult to manage the volume and follow up

Security Issues of EHR Portals

- Include patient portal in risk assessment:
 - What is risk of interception during transmission?
 - What is risk of unauthorized access?
 - What are risks of Internet-facing interface?
 - Has your EHR portal vendor's software been independently tested?



Security Issues of EHR Portals

- What is appropriate level of authentication?
 - Does there need to be initial in-person authentication?
 - How strong do passwords need to be?
 - How to balance security vs. patient usability
 - Do patients have option of higher security (e.g., multifactor authentication)?
 - What is policy for consecutive failed login attempts?
 - How are password resets handled?
 - How to avoid “social engineering”?

Security Issues of EHR Portals

- What is appropriate level of auditing?
 - Are audit logs turned on?
 - Is there reasonable random review (e.g., significant sample)?
 - Is there reasonable focused review (e.g., based on suspicious patterns)?

Security Issues of EHR Portals

- How are servers protected?
 - Physical safeguards?
 - Encryption?
- What if patient causes security failure?
 - Patient uses weak password
 - Patient shares credentials
 - Patient loses mobile device with access to portal

Mayo Clinic's Experience with Portal Security

Lessons Learned :

- Online validation challenges
- Proxy rights without a limit on the viewable information even if restrictions were requested
- Patient accounts with similar names or clinic numbers merged
- Tips
 - It's important to have good audit logs to determine what was viewed / accessed when security issues arise
 - Important to have privacy and security members of portal team to help when issues arise
 - Privacy by Design is important

PHRs and EHR Portals

- Personal health record (PHR) is patient controlled record
- EHR portal is window into EHR
- PHR and EHR portal can work together
 - Patient gets to see EHR portal
 - EHR portal feeds into PHR
 - Patient gets to add information in PHR and decide whether to share through EHR portal

PHRs and EHR Portals

- Is PHR considered PHI of covered entity?
 - Is it on covered entity's servers?

- Does covered entity have right to view PHR?
 - Potentially not without patient permission

State Law and EHR Portals




- Will portal include sensitive information subject to state law restrictions?
 - HIV test results or other HIV or STD information
 - Mental health information
 - Genetic test results
 - Alcohol or substance abuse treatment information (also subject to further federal restrictions)
- Will a more detailed authorization suffice?
 - Is separate authorization required for each disclosure?







Mayo's Experience with State Authorization Laws

- Because Mayo is across many states, we rely on the most restrictive state law that's applicable to determine how to treat the information in the portal
- Currently, types of clinical information that trigger a strict state law are not being released on the portal eg. Emancipated minor
- Mayo is currently working on creating an authorization in hopes of resolving some state law concerns

Challenge: Mobile Patient Portal

- In mid 2012, Mayo implemented a mobile application for iPhones & iPads which helps Mayo Clinic meet MU requirements.
- Security Challenges:
 - Authentication
 - Encryption
 - Passwords
- Privacy Challenges:
 - Appointment information – reminder pop ups & calendar agendas
 - Portal messages to patients

	<h2>The Future</h2>
	<ul style="list-style-type: none"> ▪ Meaningful Use <ul style="list-style-type: none"> ▪ Stage 2 pushes for use of patient portals ▪ Stage 2 promotes inclusion of amendments ▪ Health information exchange <ul style="list-style-type: none"> ▪ When HIE maintains centralized EHR record or centralized view, will HIE provide portal directly to patients? <div style="text-align: right; margin-top: 20px;">  </div>
	<div style="display: flex; justify-content: space-between; align-items: center;"> <div data-bbox="370 907 553 961">  <p>Sutter Health We Plus You</p> </div> <div data-bbox="812 919 839 940"> <p>29</p> </div> <div data-bbox="1065 907 1243 961">  <p>Davis Wright Tremaine LLP</p> </div> </div>

	<h2>Thank You!</h2>
	<div style="margin-bottom: 20px;">  <p>Jacki Monson, JD, CHC</p>  <p>Sutter Health We Plus You</p> <p>monsonja@sutterhealth 916.286.6616</p> </div> <div>  <p>Adam H. Greene, JD, MPH</p>  <p>Davis Wright Tremaine LLP</p> <p>adamgreene@dwt.com 202.973.4213</p> </div>
	<div style="display: flex; justify-content: space-between; align-items: center;"> <div data-bbox="370 1778 553 1833">  <p>Sutter Health We Plus You</p> </div> <div data-bbox="812 1791 839 1812"> <p>30</p> </div> <div data-bbox="1065 1778 1243 1833">  <p>Davis Wright Tremaine LLP</p> </div> </div>