Patient Portals: Privacy & Security Considerations

David Holtzman, JD, CIPP/G
VP, Compliance Strategies
CynergisTek

Adam Bennett
Vice President
Cloudburst Security

Michael Berwanger, JD
Director, Quality Management & Compliance
MedCost, LLC
Agenda

1. HIPAA Right of Access
2. Who is Authorized to Access?
3. Patient Right to Amend
4. Information Security
5. PHRs & EHRs
HIPAA Right of Access
HIPAA’s Right of Access to PHI

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

• To what extent does EHR portal include information that may cause harm?

• Can clinician act proactively to flag information that could cause harm?
Who is Authorized to Access?
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 (physical or electronic)
Personal Representatives and Minors

• Personal representative has rights of individual—including right to access in form or format requested if readily producible
  – Personal representatives’ rights should cut off at age of majority

• Personal representative can authorize access by 3rd party
  – Guidance to Privacy Rule that authorization survives age of majority, so a 3rd party can continue to access EHR
Strategies for Personal Representatives

• Parent may not be personal representative for certain information
  – When minor can consent under state law

• Segment data
  – Parent does not get access to certain PHI
    • Include with restricted access; or,
    • Exclude from portal

• Restrict certain ages
  – Exclude certain ages from portal
  – Only include with minor’s authorization
Patient Right to Amend
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 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 requirements
- Amendment functionality of EHR may differ significantly
Information Security
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?
    • Multifactor authentication
      – What is policy for consecutive failed login attempts?
      – How are password resets handled?
      – How to avoid “social engineering”?
Portal Vendor Selection and Management

- Requirements Definition
- Pre-Contract Due Diligence
- Contract Security Specifications
- Performance Monitoring
- Breach Notification
- Contract Termination
- Documentation
Challenge of Mobile Patient Portal

• Security Challenges:
  – Authentication
  – Encryption
  – Passwords

• Privacy Challenges
  – Appointment information
    • Reminder pop-ups & calendar agendas
    • Portal messages to patients
    • 3rd party sharing, cookies, adware, location beacons
Security Issues of EHR Portals

• What is appropriate level of auditing?
  – Are audit logs turned on?
  – Is there reasonable random review?
    • What is a significant sample?
  – Is there reasonable focused review?
    • Based on suspicious patterns
    • How are criteria for review determined?
Security Issues of EHR Portals

• How are servers and storage media protected?
  – Physical safeguards
  – Encryption

• What if patient causes security failure?
  – Patient uses weak password
  – Patient shares authentication/unique user credentials
  – Patient loses mobile device with “remember me” access to portal
PHRs and EHRs
PHR and EHR Portals

• Personal health record (PHR) is patient controlled record
• EHR portal is window into EHR
• PHR and EHR portals can work together
  – Patient gets to see EHR portal
  – EHR portal feeds into PHR
  – Patient gets to add information in PHR & chooses whether to share through EHR portal
PHRs and EHR Portals

- Is PHR considered PHI of covered entity?
  - Is PHR operating on servers of the covered entity or their business associate?
- Does covered entity have right to access PHR?
  - Patient permission required?
PHR Use and Access to Patient Information

- PHRs not covered by HIPAA can be lightly regulated
  - FTC PHR Breach Notification Rule
  - FTC Act Section 5 prohibition on Unfair and Deceptive Trade Practices
    - Jurisdiction limited to for-profit entities
  - State law breach notification reporting
  - Model PHR Privacy Notice
    - PHR companies can use to communicate their privacy and security policies and data sharing practices to individuals.
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 federal confidentiality requirements
• Will a more detailed authorization suffice?
  – Is a separate authorization required for each disclosure?
Agenda

Questions?

David Holtzman, JD, CIPP/G
David.Holtzman@cynergistek.com
(240)720-1365
@HITPrivacy

Adam Bennett
Adam@cloudburstsecurity.com
(703) 224-8966

Michael Berwanger, JD
mberwanger@medcost.com
(336) 774-4359