Security & Privacy Strategies for Expanded Communities

Deven McGraw

Partner

Manatt, Phelps & Phillips LLP

Key Challenges in Community Data Sharing

- Patient-mediated data sharing
- Sharing data with companies whose business models include leveraging data
- Using cloud data storage models

The Patient's Right to Access Health Information

- Patients have the right to access their health information in the form or format they request, as long as the info is reproducible in that form/format (originated in Health Insurance Portability and Accountability (HIPAA) privacy and security regulations).
- Patients can get this information electronically if information is stored electronically (clarified in the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)).
- Patients can have information directly sent to a third party if the choice is "clear, conspicuous and specific." (established in HITECH)

What is acceptable digital format?

- Must have capability to provide some human readable digital copy (for ex., PDF).
- Not required to adopt every format requested by patients – negotiate re: mutually acceptable format. (From HITECH Omnibus Rule)
- Could use tools of Certified EHRs – for example, view, download & transmit – if acceptable to patient.
  - Could involve "transmit" to a patient's app, for example.

Sending to Third Parties

- "Clear, Conspicuous & Specific" means:
  - In writing (can be electronic)
  - Signed by the patient (can be electronic)
  - Clearly identifies designated person/entity and where to send the information.
- What if a patient requests a connection from an EHR to an app or device?
  - Per HIPAA Security Rule, provider should evaluate security risks as part of determining whether this format is "readily producible"
  - Taking in data from patients also triggers security concerns; should also consider whether it is data you intend to collect, act on.

Responsibilities of Sender

- Covered entities may rely on the information provided in writing by the patient and need only have reasonable procedures in place to assure that the address provided by the patient is correctly entered.
  - "For example, reasonable safeguards [to be followed by the covered entity] would not require the covered entity to confirm that the individual provided the correct e-mail address of the third party, but would require reasonable procedures to ensure that the covered entity correctly enters the e-mail address into its system." (page 5635, Federal Register, January 25, 2013)

Must be Sent Securely?

- HIPAA Security Rule ordinarily requires secure transmission of PHI – ***but:***
- If patient requests information be sent by unsecure email, provider must send "in the form or format requested by the patient."
- Yes, in this case, the patient's wishes can trump Security Rule obligations.
  - Presumption is that sending by unsecure e-mail creates security risk for patient – but not for the provider; patient has the right to choose convenience over security risk.

Really?

- Yes – but you are expected to provide a "lite" warning about security risks to make sure patient is aware of choice he/she is making.
  - "We do not expect covered entities to educate individuals about encryption technology and the information security. Rather, we merely expect the covered entity to notify the individual that there may be some level of risk that the information in the e-mail could be read by a third party. If the individuals are notified of the risks and still prefer unencrypted e-mail, the individual has the right to receive [PHI] in that way, and covered entities are not responsible for unauthorized access of [PHI] while in transmission to the individual based on the individual's request. Further, covered entities are not responsible for safeguarding information once delivered to the individual." (p.5634, Federal Register, January 25, 2013)

What can patient do with the data?

- Patients are not regulated by HIPAA, nor are the vendors who create mobile and other tools for patient use.
  - Such vendors could be covered by state health privacy laws (for example, CA).
- FTC has authority to crack down on "unfair" and "deceptive" trade practices of for profit companies
  - For example, broken commitments in a privacy policy
  - HITECH breach notification provisions for "personal health records" and related apps.
- App platform requirements may create new norms (for example, Apple's HealthKit)

Doing Business with "Data Leveragers"

- HIPAA permits providers to provide identifiable health information – protected health information (PHI) – to vendors who need PHI to perform a service or function for that provider.
- They are business associates under HIPAA and directly accountable to regulators for compliance with the Security Rule and some parts of the Privacy Rule.
- Entity covered by HIPAA must sign a business associate agreement (BAA) (most entities at least start with the model BAA from HHS).

Data leveragers

- Business Associate permitted uses of data must be set forth in the BAA.
  - Data aggregation
  - De-identification and further use of de-identified data
  - Off-shore storage (not required to be covered in BAA but most entities do include such provisions)
- Violation of BAA could be punished by regulators; also breach of contract remedies
- Also possibility: sharing of limited data set (with data use agreement) for operations, public health or research
  - But in that case, entity is NOT a BA providing a service or function for the provider

HIPAA and the Cloud – May I?

- Does HIPAA permit use of the Cloud for storage/ maintenance of PHI? Yes.
- In most cases, a cloud storage provider would be considered to be a HIPAA business associate.
  - Def. of business associate (BA): "creates, receives, maintains, or transmits [PHI]" for a covered entity.
  - Exception: mere conduits.
  - Still some confusion about this, because BAs are presumed to require access to PHI "on a routine basis."

HIPAA & the Cloud – Should I?

- Cloud service providers (CSPs) may be better positioned to provide IT, data storage services
- But provider cannot be "hands off":
  - Need to do reasonable due diligence in choosing CSP vendor, monitoring
  - Look behind marketing phrase "HIPAA Compliant"
  - Regulators look to covered entity for compliance with HIPAA – what is the CSP committing to do, what responsibilities do you still have
  - See HIPAA enforcement settlement with Phoenix Cardiac Surgery, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/pcsurgery_agreement.pdf ($100,000 fine).

Thank you!

- Deven McGraw

  Partner

  Manatt, Phelps & Phillips, LLP

  dmcgraw@manatt.com

  202-585-6552

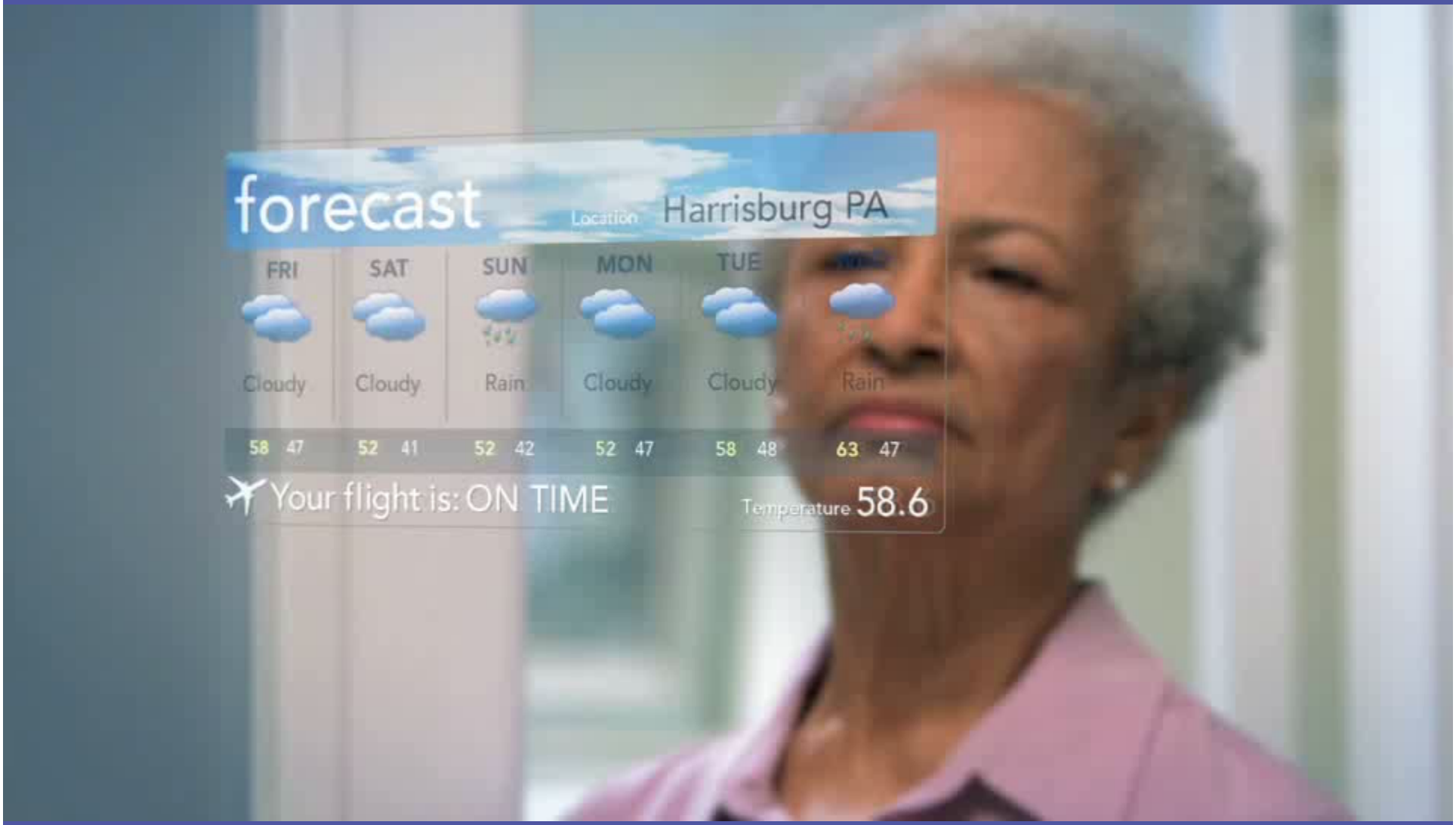
Security & Privacy Strategies for Expanded Communities

Florence Hudson

Senior VP and Chief Innovation Officer

Internet2

Let us consider an aspirational view of connected healthcare



http://www.kp-itcomms.org/mm/digitalhealth/index.html

Source: Kaiser Permanente

Connected healthcare can streamline care

- Real time remote monitoring and management
- Remote triage
- Real time remote patient/provider connectivity
- Interoperability among many devices
  - Infusion pumps
  - Refrigerators
  - Mirrors
  - Smartphones
- Sharing of PHI… everywhere
- Risks and challenges need to be addressed

Key Challenges in Community Data Sharing

- Apps on personal devices - fixed and mobile
- Protecting data from device to the “cloud”
- End to end trust and security

Apps and data on personal devices

- Fixed and mobile
- Growing number and type of connected devices
  - Smartphones
  - BYOD
  - Biomedical devices
  - Fitbits
  - Scales
  - Appliances
- Payers, Providers, Patients need to be aware

Mitigating risks in connected healthcare and expanded communities

- Multi-factor authentication
- Multi-level security, “Defense in Depth”
  - Service
  - Software
  - Firmware
  - Hardware
- TIPS for device, user, data, app, PHI
  - Trust
  - Identification
  - Privacy
  - Security

Securing data in the “cloud”

- Virtual and physical security
  - Servers
  - Storage
  - Data
  - Network
  - Physical site
- User, application, data access and security
- Hybrid clouds are growing…need to understand the system of systems architecture
- HIPAA compliant clouds

End to end trust and security

- Must consider all elements of the connected ecosystem
  - Users – patients, family, providers, payers… insider risks
  - Endpoint devices – smartphones, biomedical, health/wellness devices, sensors
  - Gateways – home clouds, in hospital, in cities
  - Communications - channel and network
  - Cloud systems – servers, storage
  - Hybrid clouds
  - Software – middleware, applications
  - Services
  - Data security, at rest and in motion

- Focus on TIPS – Trust, Identify, Privacy, Security

- Requires end to end ecosystem partnerships
  - Across the technology ecosystem – chip to device to network to servers to storage to software to cloud
  - Technologists, providers, device manufacturers, standards, policy, payers, patients

Managing realized risk

- Constant monitoring
  - Identify anomalies
  - Intrusion detection
- Quickly act to isolate the anomaly / intrusion / threat / breach
- Notify the source, if a trusted partner
- Notify the authorities, as needed
- Increase security at all levels – software, services, firmware, hardware

Data Breaches…What to do

1. Inform company personnel
2. Investigate which information and systems were compromised
3. Isolate your network and/or systems affected
4. Collect evidence
5. Notify those affected, including external partners and clients with the facts and mitigation plans
6. Address regulatory concerns

How to Prepare, Protect, Secure against a Data Breach

1. Establish company policies and train employees
2. Implement an enterprise-grade security solution – systems and processes
3. Hire a security expert
4. Contract with ethical hackers to try to breach your system, learn from this to thwart attacks
5. Maintain regulatory requirements

Thank you!

- Florence Hudson

  Senior Vice President and

  Chief Innovation Officer

  Internet2

  fhudson@internet.edu

  1-914-525-5552