



eHealth Privacy and Security— National Perspective

Rochelle Woolley
SVP & Chief Communication Officer
RxHub



Markle Foundation: Connecting for Health

- Connecting for Health is working to realize the full potential of information technology in health and health care, while protecting patient *privacy* and the *security* of personal health information.
- This public-private collaborative of more than 100 organizations
- Developing tools, including technical guidance documents and model contracts and policies to protect patient privacy

Connecting for Health Achievements

- Built Broad Consensus on a "Roadmap" for Achieving Electronic Connectivity in Healthcare
- Conducted Original Research—Common Framework
- Defined Key Problems
- Response to Industry Challenges—KatrinaHealth.org

[Policy Subcommittee]

- Identity, Authentication and Authorization for System Access
- Logging and Audits for a National Health Information Network
- Patients' Access to their own Health Information
- Policy Regarding Breach of Confidentiality of Patient Data

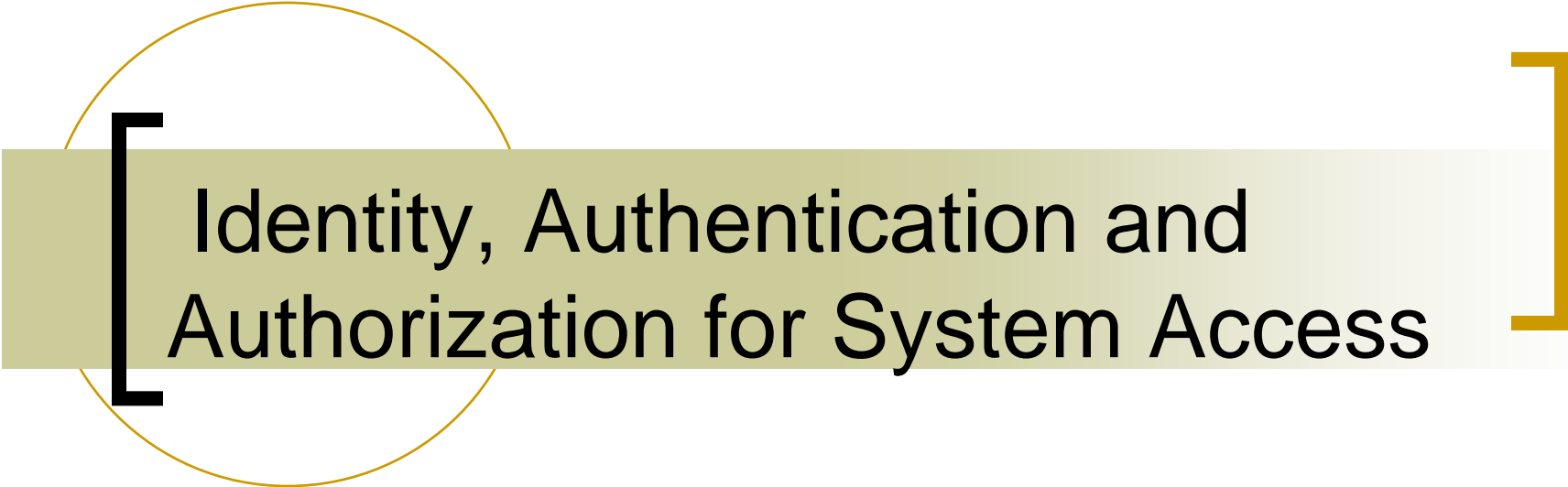
Privacy Guiding Principles

Nine principles that provide a multi-layered approach that should be built into any information-sharing system or network in order to ensure confidentiality and privacy of patient data.

1. Openness and Transparency
2. Purpose Specification and Minimization
3. Collection Limitation
4. Use Limitation
5. Individual Participation and Control
6. Data Integrity and Quality
7. Security Safeguards and Controls
8. Accountability and Oversight
9. Remedies

Markle Foundation (2005). Framework for CFH Prototype Policy Subcommittee Documents.
New York, Markle Foundation.

http://www.phrconference.org/assets/consumer_principles_101105.pdf



Identity, Authentication and
Authorization for System Access

[Identity, Authentication, Authorization]

- Who am I? (identity)
- How can I prove who I am? (authentication)
- What can I do when I prove who I am? (authorization)

[Identity]

- Any identifier that points unambiguously and uniquely to an individual person or institution
- Employee ID number
- Log-in name (no duplicates)
- Token to personhood or ‘entityhood’—not roles

Authentication

- Requires identity, and is required for authorization
- Simplest form providing token plus secret (*bank card and PIN # or user name & password*)
- SSN not acceptable in this case

Authorization

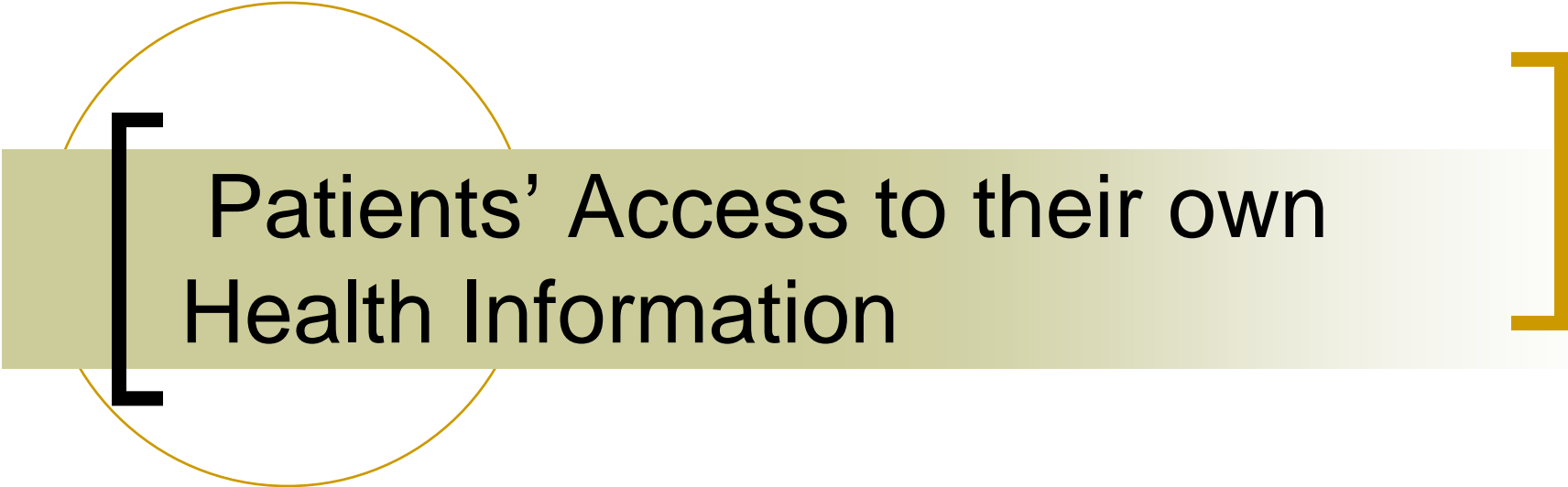
- Typically role-based
- Identifies what functions may be performed:
 - View
 - Copy
 - Update

[Auditing]

- Auditing should be done separately for Identify, Authentication and Authorization
- Who accessed the system after the fact

Requirements

- An SNO (Sub Network Organization) must have identifiers for all its participating institutions
- All users must be authenticated before they gain access to any SNO-wide resource containing patient data
- Any request for data from a remote institution (an institution other than the one the user is logged in to) must be accompanied by at least two pieces of identifying information: which institution authenticated the requesting user, and an identifier for that user.
- SNOs should review their identification, authentication and authorization policies annually. This is probably best done in conjunction with the mandated HIPAA security audit.



Patients' Access to their own Health Information

The HIPAA Privacy Rule- Accessing Protected Health Information

- In general, protected health information under the Privacy Rule correlates with what most consumers would consider their medical record.
- Whether or not their health information is paper-based or stored electronically, the Privacy Rule affords patients the right to access their medical record within 30 days of a request.
- The Privacy Rule outlines a basic process for individuals seeking access to their medical information and establishes guidelines to ensure covered entities provide access in a timely manner.

The HIPAA Privacy Rule—Amending Protected Health Information

- Under the law, after an individual has reviewed his or her medical records, he or she may request that the covered entity amend the protected health information in the designated record set.
- However, in order to protect both the integrity of the record and the patient, the individual does not have the right to request that the covered entity delete any information from the record.
- Instead, information is added to the record, identifying and amending the pertinent information.

The HIPAA Privacy Rule- Accounting for Disclosures

- Privacy Rule acknowledges the importance of allowing patients the ability to see who accessed their personal health information.
- Upon request, covered entities must provide consumers with an accounting of disclosures during the previous six years, including the date of the disclosure, the name of the person who received the information, a brief description of the protected health information disclosed, and a brief statement of the purpose of the disclosure.
- If a covered entity has made multiple disclosures to the same person for the same purpose, it may provide the above information only for the first disclosure as long as it also provides the frequency of the disclosures and the date of the last disclosure.



Policy Regarding Breach of Confidentiality of Patient Data

Notification of Breaches

- Notification of breach of confidentiality of patient data is impacted not only by HIPAA laws, but also by state breach notification laws that are becoming more common.
- Thus, any SNO policy should require that the Participants (and the SNO itself) comply with all applicable federal, state and local laws.
- In addition, the SNO must report any breaches to the particular data provider whose data was improperly used. This would not be limited to serious breaches, but would include all breaches.
- Most SNOs will be a Business Associate of the Participants who provide patient data to the SNO, in which case the SNO is required under HIPAA to report all Security Incidents to the covered

Design Principles of a Health Information Environment

- Decentralized
- Federated
- Private and Secure
- Accurate
- Reliable
- Fast
- Interoperable and built on a Common Framework
- Designed to Respect and Serve Patients (in addition to the Health System and the Public)
- Flexible

Resources

- Connecting for Health- Markle Foundation
www.connectingforhealth.org
- eHealth Initiative
www.ehealthinitiative.org
- The Vanderbilt Center for Better Health (VCBH) and Volunteer eHealth Initiative (VeHI), "Security & Confidentiality: Principles, Practices, and Implementations"
<http://www.volunteer-ehealth.org/AHRQ/12142005/resources.htm>