Beyond HIPAA—National Trends in Health Information Exchange and Granular Consent

Marilyn Prosch, PhD, CIPP/US
Associate Professor, W.P. Carey School of Business, Department of Information Systems, Privacy By Design Research Lab, Arizona State University

Bradley F. Tritle, CIPP/US
Principal, Health-e Republic
Director, Healthcare Business Development, IGC
Co-Founder / CEO, eHealth Nexus
Agenda

I. Introductions
II. Game / Demo
III. Types of Sensitive Health Data
IV. Release of Information
V. Current State of HIE
VI. Core Consent Options
VII. How are States /HIOs Handling
VIII. Laws
IX. Comparison of HIE Consent Capabilities
X. Closing: What should the future be?
Learning Objectives

• To understand the national trends for Health Information Exchange (HIE)
• To understand the three types of HIE promoted by the US Government (ONC)
• To describe types of sensitive health data that may be sequestered, withheld, or redacted
• To understand the requirements for granular consent
• To understand the consent mechanisms generally used for each type of HIE
• To understand how HIE architectures generally operate relative to Fair Information Privacy Principles, Privacy by Design Principles, and the Hippocratic Oath
Game / Demonstration

• Consumer Participation in HIE
  – Query-based: Opt-in vs Opt-out
  – Directed: No consent for provider to provider (or consent if state law requires)
  – Consumer-mediated: Consumer proactively chooses or purchases service
Game / Demonstration

• General capabilities for control of sensitive health information
  – Query-based exchange

*authorization is currently not granular, but “all or nothing”
Game / Demonstration

• General capabilities for control of sensitive health information
  – Directed Exchange

Specific Info can be sent between 2 known persons
Game / Demonstration

• General capabilities for control of sensitive health information
  – Consumer-mediated

Patient chooses what to share with whom
Fair Information Practice Principles

1. Individual access
2. Correction
3. Openness and transparency
4. Individual choice
5. Collection, use and disclosure limitation
6. Data quality and integrity
7. Safeguards
8. Accountability
Privacy by Design Principles

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full Functionality – **Positive-Sum**, not Zero-Sum
5. End-to-End Security – **Full Lifecycle Protection**
6. **Visibility and Transparency** – Keep it Open
7. **Respect** for User Privacy – Keep it **User-Centric**
Examples of Sensitive Health Data (NCVHS)

- Domestic Violence
- Genetic information
- Mental health information (including Psychotherapy Notes)
- Reproductive health
- Substance abuse
What is ideal?

• If you could design a system to both share your health information as needed, yet protect your privacy, what would it look like?
• Imagine we needed a system to share attorney-client privileged information – what would that look like?
Current Provider Release of Information (ROI) Process Varies

AUTHORIZATION FOR RELEASE OF HEALTH INFORMATION

When you complete and sign this form, health information about you will be released as you describe in the form. Please read each section carefully and complete the required sections before signing. We encourage you to request a copy of your records and review them before authorizing the release of the records to someone other than you. Please clearly and legibly print all information when completing this form and sign on the last page.

SECTION A: Please provide the name of the patient whose records are being requested for release.

Patient’s name: ___________________________ First: ___________________________

Date of birth: ___________________________ Phone number: ___________________________

SECTION B: Please describe the specific health information you would like released by completing the appropriate information below. Certain specific health information requires a separate indication from you in order for us to release that information, such as HIV test results, hereditary disorder test results, family planning services and certain mental health information. If you would like this information released, you will need to indicate separately in the boxes B.2, B.3, B.4, B.5 and B.6 below. You must both check the box and initial next to the box to authorize the release of the information described after the box.

B.1: General Health Information Release (Please note: if you do not check any of the boxes in Sections B.2, B.3, B.4, B.5 or B.6 below and there is information in your record as described in those sections, the information described in those sections will not be included in the release. If you simply check the boxes in B.1), however, we will include mental health records, except as described in B.2.1)

- Check here and initial next to the box if you would like information related to specific dates of service released and not the entire medical record.

- Check here and initial next to the box if you would like to further describe the health information that you would like released, and please provide a description: ___________________________

- Check here and initial next to the box if you would like your entire medical record released.

- Check here and initial next to the box if you would like your Radiology Film or Radiology Compact Disk (CD) released.

- Check here and initial next to the box if you would like your billing records or billing information released.

B.2: Mental Health Information

- Check here and initial next to the box if you had inpatient psychiatric services provided in the G2 or H2 hospital unit and you would like these records released. Please note that if the physician, licensed psychologist, social worker or marriage/family therapist who was in charge of the patient's care may deny release of your information in limited circumstances.

- Check here and initial next to the box if you had outpatient psychiatric services provided in the Outpatient Psychiatric Clinic located at 401 Quarry Road and you would like these records released. Please note that the physician, licensed psychologist, social worker or marriage/family therapist who was in charge of the patient's care may deny release of your information in limited circumstances.

IMPORTANT NOTE ABOUT MENTAL HEALTH INFORMATION: If you received mental health services, such as a psychiatric consult, when you were an inpatient not on the G2 or H2 hospital inpatient psychiatric units or when you were an outpatient in one of the outpatient clinics other than Outpatient Psychiatric Clinic at 401 Quarry Road, the mental health notes in your general record will be released when you check the boxes in Section B.1. We will release all information in the general record as you indicate in B.1, which may include mental health notes if you were seen in locations other than the mental health unit or the outpatient psychiatric clinic. We will not exclude or redact information that is included in the general record for releases that you authorize under Section B.1, including mental health notes in the general record. We encourage you to request a copy of your records and review them before authorizing the release of the records.

B.3: HIV Lab Test Results

- Check here and initial next to the box if you had HIV tests performed and would like the HIV test results released.

B.4: Hereditary Disorder Test Results

- Check here and initial next to the box if you had Hereditary Disorder tests performed and you would like the Hereditary Disorder test results released. Hereditary Tests include antenatal, neonatal, childhood and adult hereditary disorder screening records and/or related genetic counseling services that were provided in the Genetic Counseling Department (all test results and records generated as part of the Hereditary Disorders Program). The release of this information may involve the following risks: re-disclosure by the recipient of Hereditary Disorder test results, loss or compromise of insurance benefits, or employment status. The release of this information may involve the following benefits: predetermination of genetic conditions, coordination of care, treatment options. You should consult your physician concerning the risks and benefits of specific tests.

B.5: Family Planning Services

- Check here and initial next to the box if you had California Family Planning, Access, Care and Treatment (FACT) services and would like this information released. FACT services may include clinical services, drug and supply services or laboratory services provided at the Gynecology Clinic (GYN) or the Reproductive Endocrinology and Infertility Clinic (REI). If a minor has received family planning services, the release of these records requires authorization from the minor.
February 20, 2008

The Honorable Michael O. Leavitt
Secretary
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Re: Individual control of sensitive health information accessible via the Nationwide
Health Information Network for purposes of treatment

Dear Secretary Leavitt:

Individual control of sensitive health information accessible via the Nationwide Health
Information Network (NHIN) is a matter of great concern to patients, practitioners, insurers,
policymakers, and others, and there is no federal law or policy that specifically addresses this
issue. Over the course of four years, the National Committee on Vital and Health Statistics
(NCVHS) has deliberated extensively about how best to ensure that appropriate privacy
protections are included in the emerging NHIN. With the increasing adoption of electronic
health information networks in the public and private sectors and development of the NHIN, it is
imperative to address this matter now.

This letter recommends that you adopt a policy for the NHIN to allow individuals to have
limited control, in a uniform manner, over the disclosure of certain sensitive health information
for purposes of treatment. The discussion and recommendations that follow are based on several
critical considerations: protecting patients’ legitimate concerns about privacy and
confidentiality, fostering trust and encouraging participation in the NHIN in order to promote
opportunities to improve patient care, and protecting the integrity of the health care system.
Congress States (ARRA 2009)

“...the HIT Policy Committee shall make recommendations for at least the following areas:

(i) Technologies that protect the privacy of health information and promote security in a qualified electronic health record, including for the segmentation and protection from disclosure of specific and sensitive individually identifiable health information with the goal of minimizing the reluctance of patients to seek care (or disclose information about a condition) because of privacy concerns, in accordance with applicable law, and for the use and disclosure of limited data sets of such information.”

ARRA HITECH Sec 3002(b)(2)(B)
November 10, 2010

The Honorable Kathleen Sebelius
Secretary
Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Madam Secretary:

Re: Recommendations Regarding Sensitive Health Information

The National Committee on Vital and Health Statistics (NCVHS) is the Department of Health and Human Service’s statutory public advisory body on health data, statistics, and national health information policy. The NCVHS has historically made recommendations about health information privacy, confidentiality, and security, and has responsibility under federal law for making recommendations to HHS on the Health Insurance Portability and Accountability Act (HIPAA).

Based on the Committee’s collective hearings and deliberations in recent years, we are writing to recommend that HHS explore the use of technology that can assist with the management of sensitive health information. Such analysis is critical to inform effective policy development around this central topic. Our nation is committed to deploying interoperable health records to improve patient health, health care, and public health. Patient trust is critical to patient participation in this deployment, and, therefore, we must invest in technologies that will promote this trust.

The sensitivity of data is often influenced by the context in which it appears. The ability to transfer health information with contextual data restrictions is an important part of the trust relationship. In order for such restrictions to be meaningful, a key strategy is the identification of categories of sensitive information that can be assigned special handling. In this letter, NCVHS
Health Information Exchange

• Why is it growing in importance and popularity?
  – Pre-2009, many had launched / considered query-based HIE initiatives to provider better care/reduce costs*
  – After 2009, HIE became a part of Electronic Health Record Meaningful Use incentive requirements
  – The Stimulus gave over $600M to states to ensure HIE available

Health Information Exchange

• 3 Types
  o Query-based Exchange ("pull")
  o Directed Exchange ("push")
  o Consumer-mediated Exchange ("share")


HIMSS report: http://www.himss.org/ASP/ContentRedirector.asp?ContentId=79816&type=HIMSSNewsItem
Financial Jury is Still Out

• Query-based ("traditional")
  – Enterprise (hospital system); sustainable
  – Community-based; many failures; few long-term successes to point to

• Directed
  – Required of state governments
  – Subscription-based; beginning of adoption
  – Secure messaging (email-like)
Financial Jury is Still Out

• Consumer-mediated
  – Personal Health Record-based
  – Variety of business models possible
    • Employer-sponsored
    • Payer-sponsored
    • Consumer-paid
    • “Free” (subsidized by commercial entities making money elsewhere)
    • Government sponsored
    • Others? Financial Banks?
  – Exits (Google Health)
  – Entrants (Aetna CarePass)
Core Consent Options

- No Consent (HIPAA allows; some state laws don’t)
- Opt-Out
- Opt-Out with Exceptions
- Opt-In
- Opt-In with Restrictions

*Goldstein, Rein. *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis*
States/HIOs are Doing (literally all over the map)

- No Consent – (e.g., Indiana, Delaware lab results)
- Opt-Out – (AZ, Maryland CRISP, Delaware patient queries)
- Opt-In – Rhode Island, New York, Massachusetts

*How do we handle interstate exchange?*
Existing Laws / Regs

• HIPAA – allows sharing of data for Treatment, Payment, Operations
• HITECH – out-of-pocket exemption
• Federally-funded drug and alcohol abuse centers (42 CFR part 2)
• Mental Health
• HIV/AIDS
• Genetic Information (GINA 2008)
Query-based Exchange Consent

• The ability for healthcare providers to look up information on a patient when delivering unplanned care (e.g., emergency department)
• Data sharing agreements between organizations (i.e., hospitals, physician groups, labs); not individual physicians/users
• State laws determining consent; other regulations
Query-based Exchange Consent

• Community-based Health Information Organizations (HIOs) may provide governance

• Fair Information Practice Principles prescribed by HHS ONC – can they follow them?

• Larger institutions currently participating; wide-spread physician office sharing not yet occurring
Query-based Exchange Consent

- Consumers limited to opt-in, opt-out, no consent, or combination
- Meta-data tagging of sensitive data types (PCAST recommends)
  - Developed in theory by “Data Segmentation for Privacy” initiative
  - Complex implementation (not possible for some time)
  - Implementation Guide Released
  - Pilots
Query-based Exchange Consent

• In some cases, may opt-out by provider
• Some providers have “mixed” data (sensitive / not-sensitive PHI)
• Consumers largely un-engaged and unaware, unless required to opt-in (so how do they follow FIPPs?)
Directed Exchange Consent

• Known party to known party
• Single user (individual) sends to single user (individual), generally.
• Secure email address
  (e.g., b.tritle@direct.shc.org)
• Referrals (e.g., primary care to specialist)
• Laboratory results delivery
Directed Exchange Consent

• Hospitals to Primary Care
• Providers to Consumers or PHR
  (e.g., brad_tritle@direct.healthvault.com)
• Mimics paper exchange of PHI for treatment; consent not required under HIPAA, but may occur (some states may require)
Consumer-Mediated Exchange Consent

- Consumer-controlled Personal Health Record (PHR)
  - Privacy policy “contract” between PHR provider and consumer
- Automate Blue Button Initiative (ABBI) facilitating data View, Download, and Transmit (VDT)
- Consumer may choose to share with family, home health, patient advocate, healthcare providers
Consumer-Mediated Exchange Consent

• In one sense, stricter control than HIPAA. Unless otherwise allowed by privacy policy, consumer controls sharing

• Not regulated under HIPAA, however:
  – ECPA applies to for-profit (FTC governs)
  – FTC Breach Notification Law
  – Non-profit (private right of action)
  – Some welcoming regulation
    • Health Record Banking / Trusts
Consumer-Mediated Sharing

Sharing

You control access to your health information. Use Sharing to decide which people can access selected types of information in your HealthVault record.

Learn more

Share health information with someone you trust

Want to share information with your healthcare provider?

Learn more

People who can see Bradley's info

Bradley Trite
Access granted: Custodian

Change access | View history
Invite someone to access Bradley's information

You control the information in this record. To allow another person to see the information, you must complete this form to send them a sharing invitation. When you click Send Invitation, HealthVault sends the recipient an email containing a link that allows them to add this record to their HealthVault account.

*Recipient's email address:

*Retype email address:

Create a passcode: (optional)

(Minimum 4 characters)

If you create a passcode, the email recipient will need to enter it to accept this invitation. To protect your invitation, don't email the passcode. Use another method to tell it to the recipient. If you forget the passcode, you'll need to resend the invitation with a new one.

Select sharing level

- View Bradley's information
- View and modify Bradley's information
- Act as a custodian of Bradley's record (What can a record custodian do?)

Select information type

- Share all items in this record
- Share only the types of information selected below

Information Types select all | clear all
Granularity in Action!

![Image of a computer screen showing a webpage with a list of information types for sharing, including options like Health information, Apps & Devices, Sharing, and History. The page is from HealthVault, and the specific types of information available for sharing include Advance Directive, Medical Device, Diabetes Profile, etc. There is also an option to set access expiration with a date of 9/14/2012.](image-url)
What is the floor: Hippocratic Oath or HIPAA?

“Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private.”

Hippocratic Oath excerpt as translated by Michael North of National Library of Medicine, 2002

Fair Information Practice Principles

1. Individual access
2. Correction
3. Openness and transparency
4. Individual choice
5. Collection, use and disclosure limitation
6. Data quality and integrity
7. Safeguards
8. Accountability
Privacy by Design Principles

1. **Proactive** not Reactive; **Preventative** not Remedial
2. Privacy as the **Default Setting**
3. Privacy **Embedded** into Design
4. Full Functionality – **Positive-Sum**, not Zero-Sum
5. End-to-End Security – **Full Lifecycle Protection**
6. **Visibility and Transparency** – Keep it **Open**
7. **Respect** for User Privacy – Keep it **User-Centric**
Choose Wisely

• How would you rank HIE types according to privacy - FIPPs, PbD Principles and the Hippocratic Oath?
  – Consumer-mediated Exchange
  – Directed Exchange
  – Query-based Exchange

• Which one(s) might consumers feel best protect(s) their privacy (assuming they know about it)?
Barriers?
What is holding the future back?

• What will hold us back from extensively deploying the type(s) of HIE just chosen?
  – Existing Stakeholders
  – Falling back on HIPAA (the way we’ve always done it)

• How can we as a country overcome these barriers?

• What specific things should be done?
Resources

- HHS ONC PIN 3

- Health Affairs Article by ONC on HIE (3 types)
  - http://content.healthaffairs.org/content/31/3/527.abstract

- NCVHVS letter on Sequestration (Feb 20, 2008)
  - http://www.ncvhs.hhs.gov/080220lt.pdf

- Data Segmentation for Privacy (IG)
  - http://wiki.siframework.org/Data+Segmentation+for+Privacy+Homepage

- GWU Consent White Paper
  http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_911197_0_0_18/ChoiceModelFinal032610.pdf

- GWU Segmentation White Paper
  http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_950145_0_0_18/gwu-data-segmentation-final.pdf

- Direct Project http://wiki.directproject.org/

- Health Record Banking Alliance
  - www.Healthbanking.org
Closing

Thank you!
Comments, Questions, Interest?

Brad Tritle, CIPP/US, CPHIT
brad@healtherepublic.com

Marilyn Prosch, PhD, CIPP/US
Marilyn.prosch@asu.edu