CONNECTING FOR HEALTH
COMMON FRAMEWORK

Resources for Implementing Private and
Secure Health Information Exchange

Policies for Information Sharing

HIT SYMPOSIUM AT MIT

July 18, 2006

Marcy Wilder
Hogan & Hartson LLP
mwilder@hhlaw.com

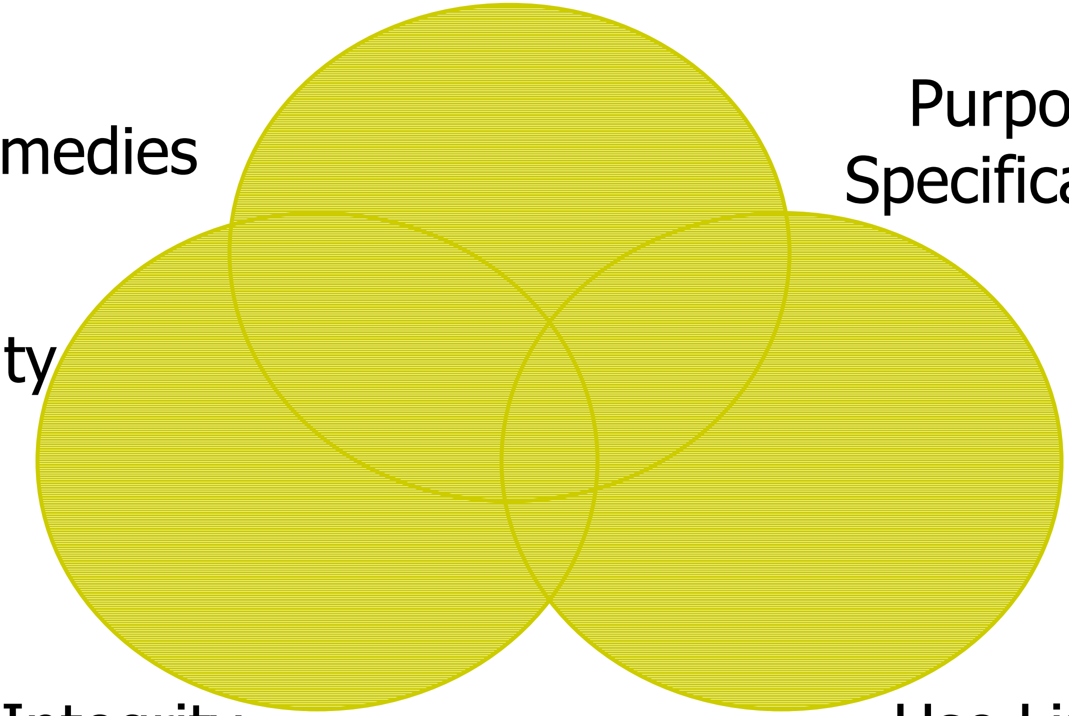
Overview of Connecting for Health Architecture

- A sub-network organization (SNO) brings together a number of providers and other health information sources
- They are linked together by contract
- Agree to follow common policies and procedures

Connecting for Health: Privacy Principles

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

The Privacy Principles are Interdependent



Openness

Purpose Specification

Collection Limitation

Use Limitation

Individual Participation and Control

Data Integrity

Security

Accountability

Remedies

Model Privacy Policies and Procedures

- To be used in conjunction with the *Model Contract for Health Information Exchange*
- Establish baseline privacy protections – participants can follow more protective practices
- Based on HIPAA, although some policies offer greater privacy protections
- Rooted in nine privacy principles
- Should be customized to reflect participants' circumstances and state laws

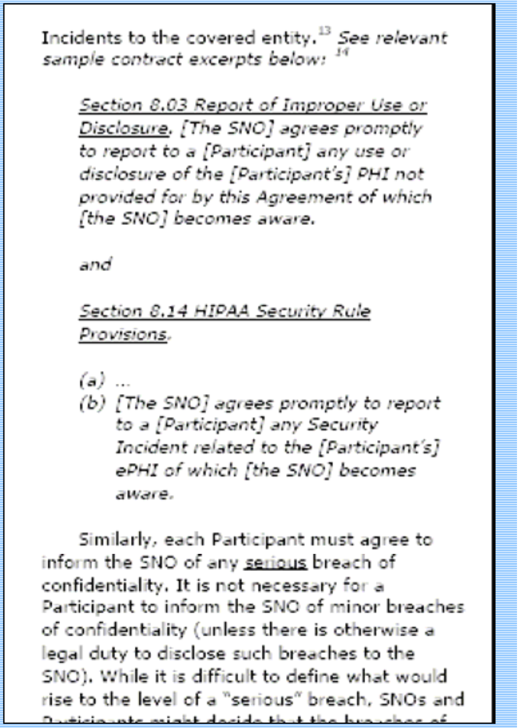
Common Framework
Policy Topics Addressed

- Notification and consent
- Uses and disclosures of health information
- Patient access to their own information
- Breaches of confidential information

Sample Policy Documents

Sample policy language

CFH Recommended policy

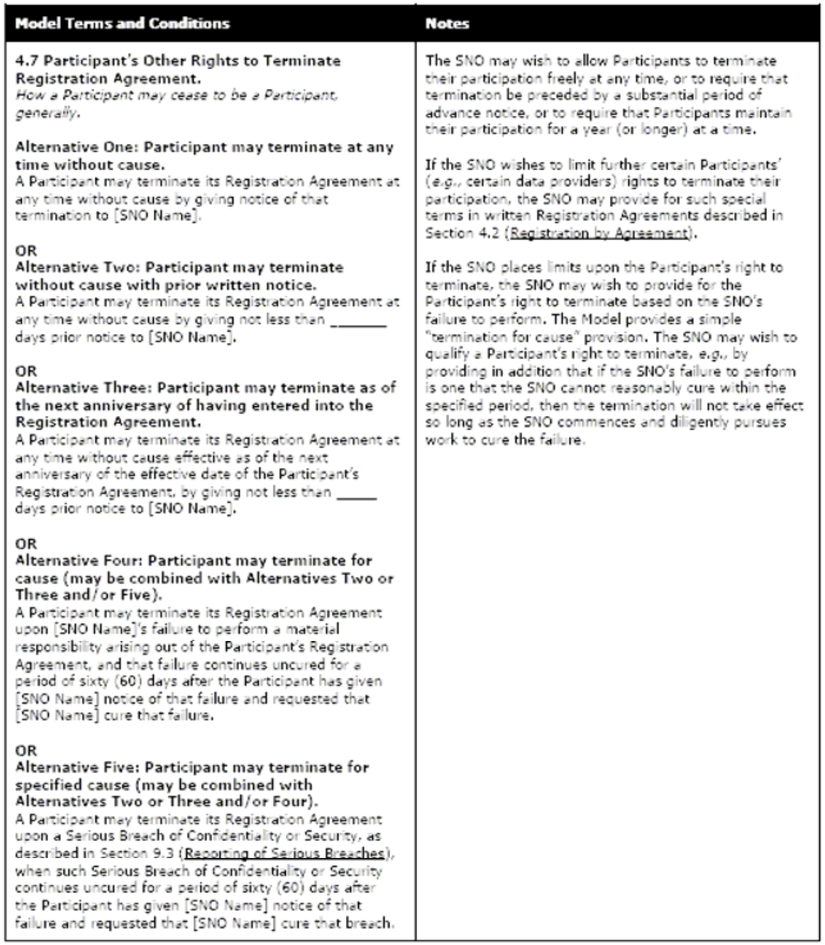


Incidents to the covered entity.[13] *See relevant sample contract excerpts below:* [14]

> *Section 8.03 Report of Improper Use or Disclosure. [The SNO] agrees promptly to report to a [Participant] any use or disclosure of the [Participant's] PHI not provided for by this Agreement of which [the SNO] becomes aware.*
>
> *and*
>
> *Section 8.14 HIPAA Security Rule Provisions.*
>
> *(a) …*
> *(b) [The SNO] agrees promptly to report to a [Participant] any Security Incident related to the [Participant's] ePHI of which [the SNO] becomes aware.*

Similarly, each Participant must agree to inform the SNO of any serious breach of confidentiality. It is not necessary for a Participant to inform the SNO of minor breaches of confidentiality (unless there is otherwise a legal duty to disclose such breaches to the SNO). While it is difficult to define what would rise to the level of a "serious" breach, SNOs and

From P8 – Breaches, p. 4



Model Terms and Conditions	Notes
4.7 Participant's Other Rights to Terminate Registration Agreement. *How a Participant may cease to be a Participant, generally.* **Alternative One: Participant may terminate at any time without cause.** A Participant may terminate its Registration Agreement at any time without cause by giving notice of that termination to [SNO Name]. **OR** **Alternative Two: Participant may terminate without cause with prior written notice.** A Participant may terminate its Registration Agreement at any time without cause by giving not less than _______ days prior notice to [SNO Name]. **OR** **Alternative Three: Participant may terminate as of the next anniversary of having entered into the Registration Agreement.** A Participant may terminate its Registration Agreement at any time without cause effective as of the next anniversary of the effective date of the Participant's Registration Agreement, by giving not less than _____ days prior notice to [SNO Name]. **OR** **Alternative Four: Participant may terminate for cause (may be combined with Alternatives Two or Three and/or Five).** A Participant may terminate its Registration Agreement upon [SNO Name]'s failure to perform a material responsibility arising out of the Participant's Registration Agreement, and that failure continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that failure. **OR** **Alternative Five: Participant may terminate for specified cause (may be combined with Alternatives Two or Three and/or Four).** A Participant may terminate its Registration Agreement upon a Serious Breach of Confidentiality or Security, as described in Section 9.3 (Reporting of Serious Breaches), when such Serious Breach of Confidentiality or Security continues uncured for a period of sixty (60) days after the Participant has given [SNO Name] notice of that failure and requested that [SNO Name] cure that breach.	The SNO may wish to allow Participants to terminate their participation freely at any time, or to require that termination be preceded by a substantial period of advance notice, or to require that Participants maintain their participation for a year (or longer) at a time. If the SNO wishes to limit further certain Participants' (*e.g.*, certain data providers) rights to terminate their participation, the SNO may provide for such special terms in written Registration Agreements described in Section 4.2 (Registration by Agreement). If the SNO places limits upon the Participant's right to terminate, the SNO may wish to provide for the Participant's right to terminate based on the SNO's failure to perform. The Model provides a simple "termination for cause" provision. The SNO may wish to qualify a Participant's right to terminate, e.g., by providing in addition that if the SNO's failure to perform is one that the SNO cannot reasonably cure within the specified period, then the termination will not take effect so long as the SNO commences and diligently pursues work to cure the failure.

From M2 – Model Contract, p. 10

Notification and Consent

- Inclusion of a person’s demographic information and the location of her medical records in the RLS raises privacy issues and issues regarding personal choice
- What should an institution participating in the RLS be required to do to inform patients and give them the ability to decide not to be listed in the RLS index?

Notification and Consent

- Easy to fall into trap of opt-in/opt-out debate, but question is really about enabling individual choice

Notification and Consent: recommendations

- Subcommittee recommendations are more protective of privacy than HIPAA – HIPAA is a floor but not always sufficient in this environment
- Patient must be given notice that institution participates in RLS and provided opportunity to remove information from index
- Revision of HIPAA Notice of Privacy Practices should reflect participation in RLS

Notification and Consent

- Recommendations strike balance between burden on SNO participants, individual patient choice and control, and maximizing the benefits of a networked health information environment
- Encourages participation in system by engendering patient trust
- Separation of clinical record from locations included in the RLS add layer of privacy protection

Uses and Disclosures of Health Information

- Networked health information environments include higher volumes of easily collected and shared health data – thereby increasing privacy risks
- Issues raised include proper purpose specification, collection, and use of health information

Uses and Disclosures of Health Information

- HIPAA is a floor but not always sufficient in this environment
- Focus should be on proper and improper uses of health information – not on *who* is allowed to participate in any particular SNO

Uses and Disclosures of Health Information: recommendations

- Integrate HIPAA permissible purpose and minimization premises
- Uses for treatment, payment and operations are permissible
- Uses for law enforcement, disaster relief, research, and public health are generally permissible
- Marketing and discrimination not permissible

Uses and Disclosures of Health Information

- Recommendations require monitoring of access to health information and an ability to determine and record who has accessed health information and when. These provisions exceed those required by HIPAA.

Patient Access

- Patients have a vital interest in accessing sensitive information about their own health care
  - Enables informed choices about who should get such information, under what circumstances
  - Facilitates awareness of errors that the records my contain
- Ability to effectively access personal health information could be significantly enhanced with the use of new technologies

Patient Access

- How can we facilitate patients’ access to their own health information in health information exchange networks?
- Involves issues of openness and transparency and individual control of health information

Patient Access

- HIPAA – the baseline
  - Right to See, Copy, and Amend own health information
  - Accounting for Disclosures
  - Covered entities required to follow both Privacy Rule and related state laws
  - Allows stronger privacy safeguards at state level

Patient Access

- As a matter of principle, patients should be able to access the RLS.
  - Access will empower patients to be more informed and active in their care
- However, significant privacy and security concerns exist regarding giving patients direct access at this stage

Patient Access: recommendations

- Patient access to the information in the RLS
  - Each SNO should have a formal process through which information in the RLS can be requested by a patient or on a patient’s behalf
  - Participants and SNOs shall consider and work towards providing patients direct, secure access to the information about them in the RLS

Patient Access

- Recommendations strike balance between current security and authentication challenges and principle that patients should have same access to their own information as health care providers do
- RLS could ultimately empower patients to access a reliable list of where their personal health information is stored

Breaches of Confidential Health Information

- Networked health information environments include higher volumes of easily collected and shared health data – thereby increasing privacy risks
- Security experts assure us that breaches will occur in even the most secure environments

Breaches of Confidential Health Information

- What policies should a SNO have regarding breaches of confidentiality of patient data?
- Involves issues of purpose specification, collection, and use of health information, accountability, and remedies
- Who should be notified of breaches, and when?
- Is breach a reason for a participant to withdraw from the SNO? Should special rules for indemnification apply in the case of a breach?

Breaches of Confidential Health Information: recommendations

- SNO should comply with HIPAA Security Rule. SNO Participants should comply with applicable federal, state, and local laws
- Responsibility of Participants to train personnel and enforce institutional confidentiality policies and disciplinary procedures

Breaches of Confidential Health Information: recommendations

- SNO must report any breaches and/or security incidents. SNO Participants must inform SNO of serious breaches of confidentiality
- Participants and SNOs should work towards system that ensures affected patients are notified in the event of a breach

Breaches of Confidential Health Information: recommendations

- SNO contract could include provision allowing participant withdrawal from SNO in case of serious breach of patient data
- SNO contract could include indemnification provisions pertaining to breach of confidentiality of protected health information

Breaches of Confidential Health Information

- Recommendations strike balance between levels of institutional and SNO responsibility for breaches and goal of notifying patients in the event of a breach
- Model language for SNO policies regarding breach is provided

Thank You

MARCY WILDER
Hogan & Hartson LLP
mwilder@hhlaw.com