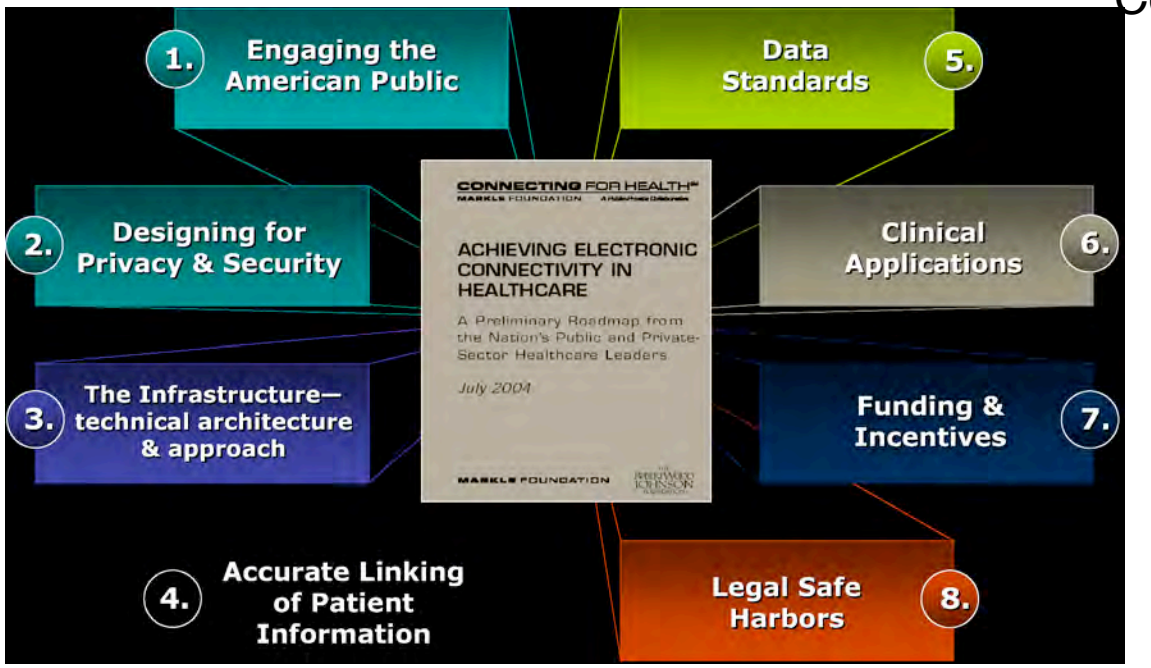
CONNECTING FOR HEALTH
COMMON FRAMEWORK

Resources for Implementing Private and Secure Health Information Exchange

Policies for Information Sharing

Common Framework



Connecting for Health principles

- Builds on existing systems ("incremental") and creates early value for doctors and patients
- Designed to safeguard privacy – imposed the requirements and then designed the solution
- Consists of an interoperable, open standards-based "network of networks" built on the Internet
- Leverages both "bottom-up" and "top-down" strategies

Connecting for Health Policy Subcommittee

- About 40 experts in
  - Law
  - Health privacy and ethics
  - Health care delivery
  - Administration
  - Technology
  - Local network development (RHIOs)

Connecting for Health Policy Subcommittee

- Looked at HIE in the context of HIPAA and existing state laws
- Developed a list of significant topics from
  - Members' experience with early information exchange networks
  - Members' own expertise

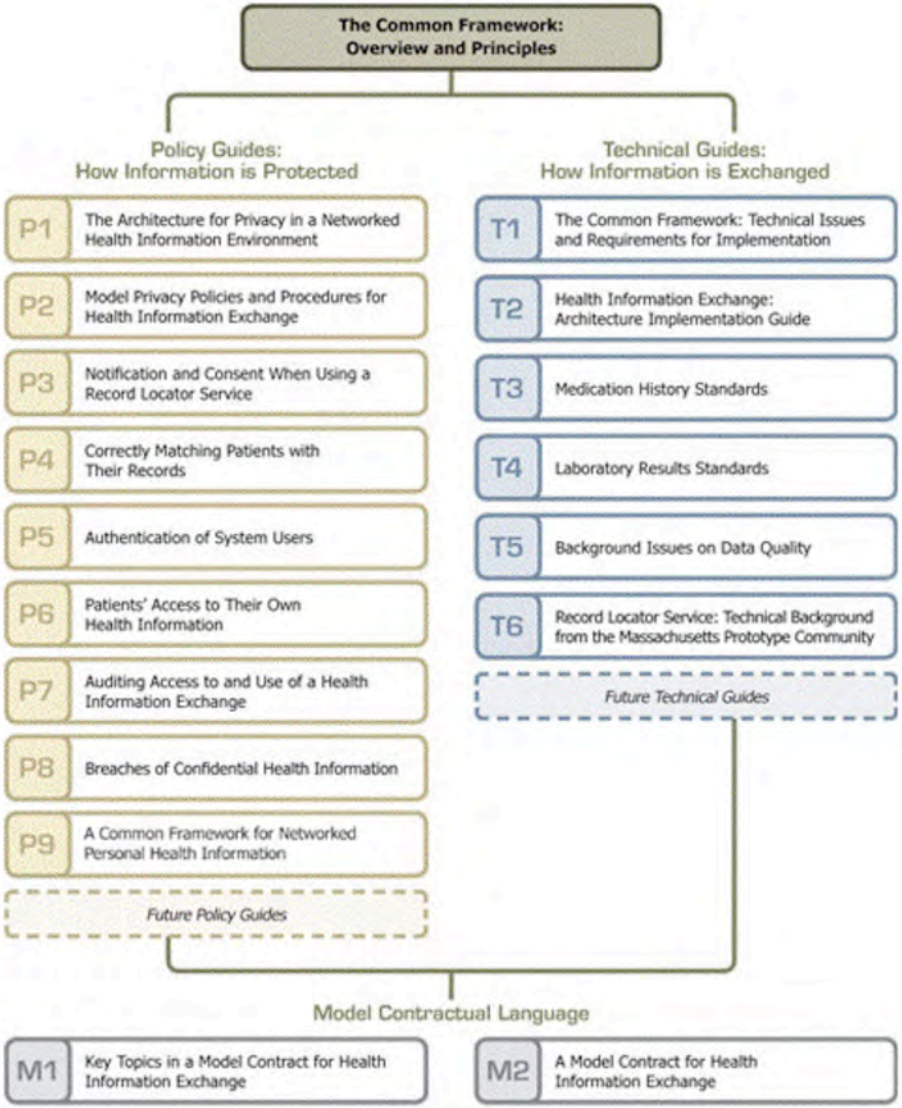
Challenges

- Who has access to what, under what circumstances, and with what protections?
- Who shares what and who bears the liability?
- How can you control access to your information?

The Connecting for Health Model for Health Information Sharing

- Sharing = linking existing sources of information
- Health information can *stay where it is* – with the doctors and others who created it
- Specific information is shared *only* when and where it is needed
- Sharing *does not* require an all new "network" or infrastructure
- Sharing *does not* require a central database or a national ID
- Sharing *does* require a Common Framework

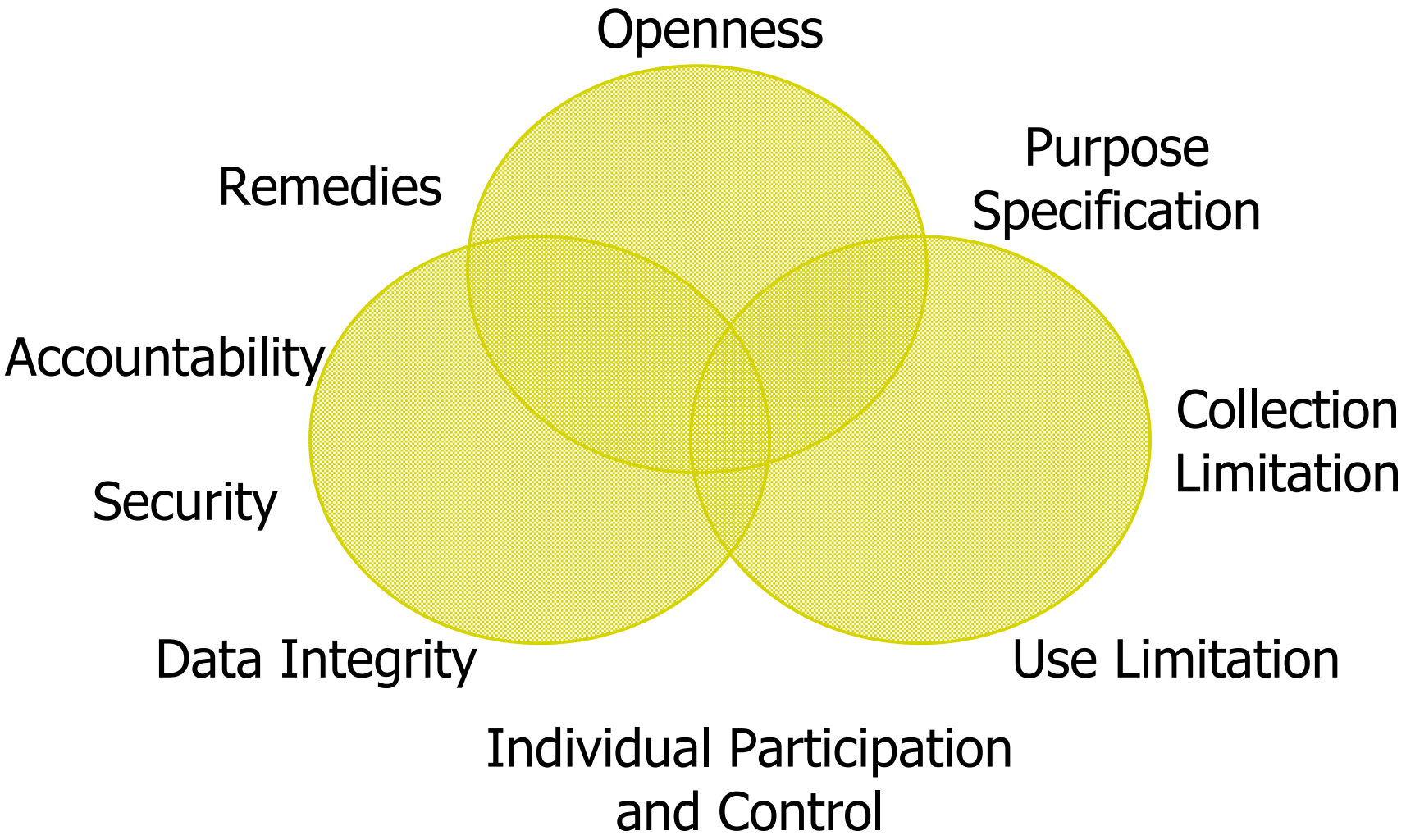
Policy Documents: P1-P9



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



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

Model Contract for Health Information Exchange

- Purpose of Model SNO Terms and Conditions
  - To assist SNOs prepare their own Terms and Conditions
  - 60-40 solution
  - Identify issues and alternatives
  - Raise questions

Model Contract: Essential Components

- Incorporates applicable terms of Common Framework Policies and Procedures
- Provides specific terms that the individual SNO may determine are appropriate for its unique needs
- Includes mechanism for making and implementing changes

Common Framework
Policy Topics Addressed

- Notification and consent
- Uses and disclosures of health information
- Matching patients with their records
- Authentication
- Patient access to their own information
- Audit
- 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 Participants might decide that the breaches of

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

- Involves issues of openness and transparency, and individuals' participation and control over their own health information
- 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

- Based on nine privacy principles
- 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 reduce likelihood of inadvertent or intentional misuses of information
- Help enhance fair and legal collection and use of data, and oversight of data use
- Help guarantee that health information is used and accessed only as authorized
- Provide workable methods and goals for SNOs regarding proper collection and use of health data

Matching Patients with their Records

- Matching patient records with patient demographic details assumes a certain amount of risk for privacy violations if records for the wrong patient are returned in a search.
- How should we optimize matching probabilities while minimizing “incidental disclosures” and clinical risk caused by false positive matches within the Record Locator Service?

Matching Patients with their Records

- Involves issues including proper use and disclosure of health information, and data quality
- HIPAA is a floor but not always sufficient in this environment
- Even though a false positive match is most likely a legal "incidental disclosure" under HIPAA such disclosures should be minimized to the greatest extent possible

Matching Patients with their Records: recommendations

- A SNO should utilize a probabilistic matching algorithm with a high probability threshold for matching (a minimal level of certainty of 1 in 100,000 before RLS returns a matching record).
- In addition:
  - No “wild-card” queries (ex. all “Smiths”)
  - Return no data not contained in query
  - No “Break the Glass” queries

Matching Patients with their Records

- Strikes appropriate balance between maximizing sharing and proper use of health information and minimizing privacy risks inherent in false positive matches
- Allows SNOs to use locally-appropriate algorithms with required high probability threshold for matching

Authentication

- In a networked health information environment, preventing unauthorized access to information and maintaining data integrity and quality requires that both the identity and authority of an entity requesting health information be verified and authenticated

Authentication

- Policy questions involved:
  - Identity (Who am I?)
  - Identifiers (How do I represent my Identity?)
  - Authentication (How can I prove who I am?)
  - Authorization (What can I do when I've proved who I am?)
- Involves issues of security safeguards and controls and accountability

Authentication

- Transactions between institutions in a SNO will operate by transitive trust, often based in contract – allowing systems to scale upwards in the number of employees covered without forcing each institution to know about every other employee in every remote institution

Authentication: recommendations

- SNO must have identifiers for all participating entities
- Users must be authenticated before given access to any SNO-wide resource containing patient data
- Any request for data from a remote institution must have two pieces of identifying information (institution authenticating user and identifier for user)

Authentication: recommendations

- “Break the Glass” function may be allowed (although not allowed in RLS itself), with restrictions
- For patient to access his or her own records, initial access must be provided by participating institution or third-party recognized by SNO

Authentication

- Strikes balance between local technical investment and control and minimum security standards for a nationwide environment
- Technical issues of security left to individual entity or SNO
- Procedures such as password recovery, log-in protections, or two-factor authentication can be set by each entity, or standardized across a SNO

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

Audit

- Effective logging and audit practices are essential safeguards as electronic health information is shared at the regional and national levels
  - Assure participating institutions of compliance with legal requirements for technical, physical, and administrative safeguards
  - Foster trust among patients and public

Audit

- What audit and logging practices should be practiced in a national health information network?
- Involves issues of openness and transparency, security safeguards, and accountability
- Challenge is to strike balance between appropriate audit practices and burden on SNO and individual institutions

Audit

- HIPAA – the baseline
  - Privacy Rule does not specifically mention audits or logging but requires covered entities to have in place “appropriate safeguards”
  - Security Rule requires audit controls as a standard
  - State laws may also exist

Audit: recommendations

- Participants in a SNO should follow HIPAA Security Rule baseline (scalable to particular security environment)
- SNO should use rigorous audit and other security practices
  - Likely to rely more heavily on electronic health records in near term

Audit: recommendations

- RLS should follow strong logging and audit control standards
  - Flow of demographic information will be carefully tracked at RLS level
  - Transfers of clinical records will not take place through RLS; subject to practices of each entity
- Additional logging and audit control functions recommended at SNO and RLS levels
  - Audit of VIP records, procedures for follow-up on suspicious activity, etc.

Audit

- Recommendations strike careful balance between appropriate audit practices and burden on SNO and individual institutions
- Based on HIPAA scalability requirement (the more sophisticated the entity and security environment, the more rigorous the audit and other required security practices)

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

Review of P9: Networked PHRs

- P9 lays foundation for how individuals become nodes on the data-sharing network under the Common Framework
- Emerging '**Consumer Access Services**' provide convenience/economies of scale for consumers
- CFH work envisions policy framework to protect both consumers and health data custodians
- Envisions two minimal but essential functions for such services:
  - Authentication of individuals
  - Collection of copies of data on the individual's behalf

What is Available?

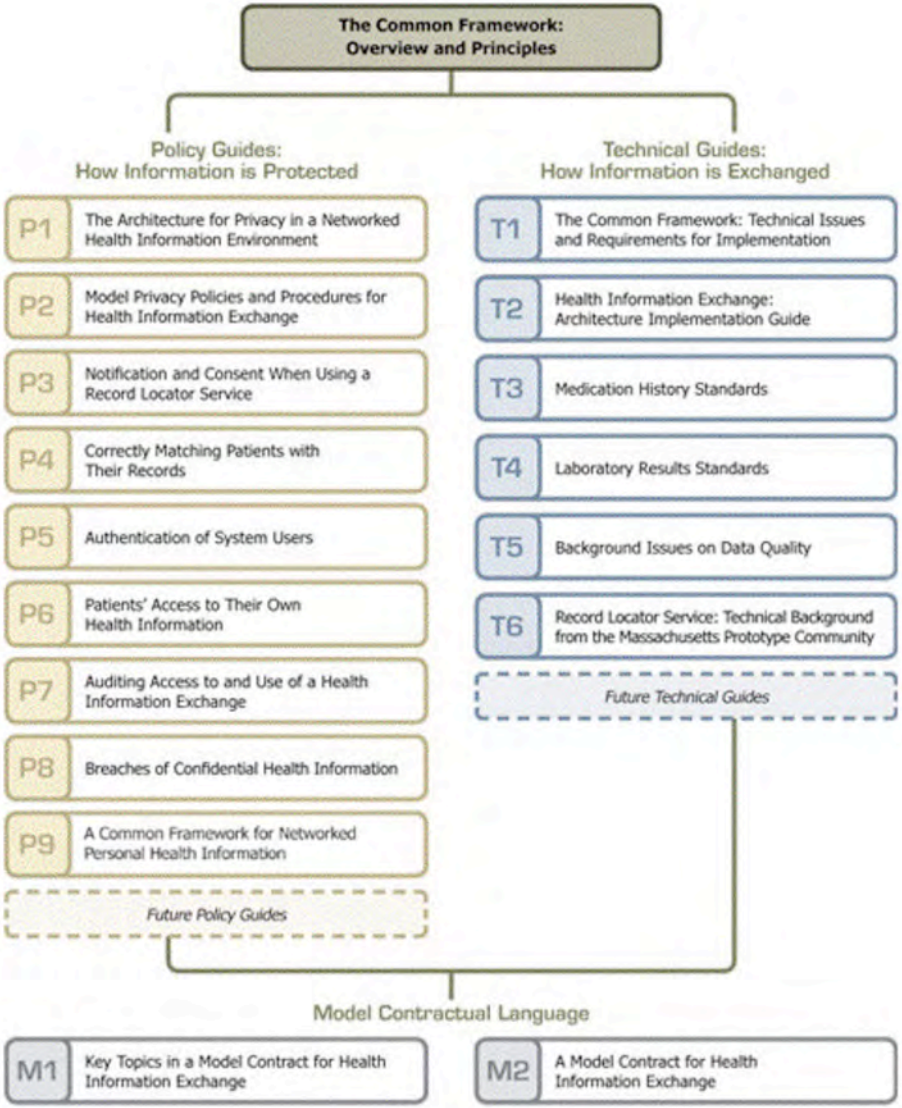
Policy Documents: 3 Categories

Background Document

- P1: Privacy Architecture for a Networked Health Care Environment

1. Specific Policy Documents
   - P2-P9: Model privacy policies, notification and consent, correctly matching, authentication, patient access, audits, breaches, and networked personal health records
2. Sample Contract Language
   - M1: Contact Topic List
   - M2: Model Contract

Policy Documents: P1-P9



Common Framework Resources

- All available free at www.connectingforhealth.org
- Policy and technical guides, model contractual language
- Software code from regional prototype sites: Regenstrief, MAShare, OpenHRE
- Email to info@markle.org