Policy and Technology Checklists for Procurers and Implementers

MARKLE

Policy Checklist

The recommended policies and practices of the Markle Connecting for Health Common Framework for Networked Personal Health Information are designed to protect consumers, and to guide services, organizations, applications, or health information exchanges that collect, store, or share personal health information on the individual's behalf. The Markle Common Framework for Networked Personal Health Information proposes a set of practices that, when taken together, encourage appropriate handling of personal health information as it flows to and from personal health records (PHRs) and similar applications or supporting services.

The Policy and Technology Checklists for Procurers and Implementers document, derived from this framework, provides recommended practices that may be used in requests for information (RFI), requests for proposals (RFP), procurement requirements or implementation checklists.

The policy practices include:

- Protecting Consumer Data Through Chain-of-Trust Agreements
- Protecting Consumers with Timely Notification of Misuse or Breach
- Providing a Dispute Resolution Process
- Preventing Discrimination and Compelled Disclosures
- Providing Access to and Control of Information
- Writing Consumer-friendly Policies
- Getting Consumer Consent

Protecting Consumer Data Through Chain-of-Trust Agreements

PRACTICE AREA CP4: Chain-of-Trust Agreements

RELATED CORE PRINCIPLE: Accountability and Oversight

The following recommended practices relate to policies protecting consumer data through chain-of-trust agreements with third parties.

Are third parties with which consumer data of any kind is shared <u>contractually bound</u> to...	Add comments here:
• Prohibit unauthorized use and disclosure of such data?	
• Protect the data in accordance with policies and authorizations agreed to by the consumer, when applicable?	
• Prohibit unauthorized attempts to identify de-identified data by, among other things, combining it with other databases of information? • See CT4: Limitations on Identifying Information.	
• Notify the Service if a breach or misuse of information in a form that carries significant risk of compromising the security, confidentiality or integrity of personal information is discovered? • See CP5: Notification of Misuse or Breach.	

Protecting Consumers with Timely Notification of Misuse or Breach

PRACTICE AREA CP5: Notification of Misuse of Breach

RELATED CORE PRINCIPLES: Individual Participation and Control, Security Safeguards and Controls, Accountability and Oversight, Remedies

The following recommended practices relate to policies for notifying consumers in the event of breach or misuse of their information.

Are these policies…	Add comments here:
• Posted as part of the part of the publicly available notice of privacy and security policies? • See CP2: Policy Notice to Consumers.	
Do consumers understand…	Add comments here:
• Under what circumstances they will receive a notification?	
• How they will receive a notification?	
• What recourse they have in the event of a breach?	
When personal information was, or is reasonably believed to have been, disclosed or acquired by an unauthorized person or party in a form that carries significant risk of compromising the security, confidentiality, or integrity of personal information…	Add comments here:
• Are consumers individually notified?	
• Are notifications made as quickly as possible? • Notifications should be made without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.	
• Are notification practices consistent with state-of-the-art security standards and "risk-based" – tailored to the potential risk to the consumer and the size, complexity, and nature of the Service?	

Providing a Dispute Resolution Process

PRACTICE AREA CP6: Dispute Resolution

RELATED CORE PRINCIPLES: Data Quality and Integrity, Accountability and Oversight, Remedies

The following recommended practices relate to policies for providing a process to resolve questions or disputes.

Are consumers provided...	Add comments here:
• Clear expectations for how to address complaints?	
• Clear and logical pathways to address and resolve complaints?	
• OPTIONAL: An ombudsman to accept and manage disputes in a fair and convenient manner?	

Preventing Discrimination and Compelled Disclosures

PRACTICE AREA CP7: Discrimination and Compelled Disclosures

RELATED CORE PRINCIPLES: Use Limitation, Individual Participation and Control

The following recommended practices relate to policies for preventing discrimination and compelled disclosures.

Do the policies...	Add comments here:
• Explain that consumers' information will not be used to discriminate and deny care, benefits or services?	
• Explain that internal practices have been developed against using information in consumer data streams for purposes of discrimination?	
• Explain that partners must comply with anti-discrimination clauses as part of their contracts?	
• Explain that "firewalls" between consumer data streams and business data streams (or other similar practices) have been implemented to prevent even the appearance of being able to use consumer information for purposes of discrimination?	
• Indicate the Service's legal stance protecting consumers against being forced to disclose information as a condition of employment, benefits, or other services important to their well-being.	

Providing Access to and Control of Information

PRACTICE AREA CP8: Consumer Obtainment and Control of Information

RELATED CORE PRINCIPLES: Individual Participation and Control, Data Quality and Integrity

The following recommended practices relate to policies for providing consumers access to and control of their personal health information stored by the Service.

AREA 1: Consumer Requests for Personal Health Information in Electronic Format	Add comments here:
• Do consumers have the tools or the means to easily obtain copies of their personal health data in electronic formats?	
• Do consumers have the ability to authorize a proxy to obtain electronic copies of their information? • Such requests should conform to standard formats and protocols as such standards and protocols become available.	
AREA 2: Proxy Access to Account	Add comments here:
• Do consumers have the ability to define and designate authorization, such as read-only, write-only, read/write, or read/write/edit?	
• Do consumers have the ability to define and designate access to data types (e.g., access to all information, access only to medications, etc.)?	
• Do consumers have the ability to define and designate access to functions (e.g., send a message to a provider, grant/revoke proxy access to someone else, etc.), when appropriate?	
• Do consumers have the ability to define and designate role permissions (e.g., health professionals, elective proxies selected by consumer, legal proxies determined by law such as parents or guardians of minors)?	
• Do consumers have the ability to further designate proxies (e.g., can those serving as proxies designate others as proxies)?	
• Do consumers have the ability to grant separate authentication and/or login processes for proxies?	
• Do consumers have the ability to track specific proxy access and major activities in immutable audit logs? • See CT3: Immutable Audit Trails.	
• Do consumers have the ability to designate time limits for proxy access and to easily revoke access?	

AREA 3: Requests to Amend or Dispute Entries	Add comments here:
• Do consumers have the ability to communicate requests for changes to the original source of information when they identify errors or omissions in the posted information?	
• Do the policies clearly inform consumers who want to modify their records whether their request must be submitted to the service or directly to the appropriate Health Data Source?	
• If consumers must submit a request to the service, are they provided an easy and convenient method to request corrections?	
• If consumers must submit a request directly to the appropriate Health Data Source, are they provided appropriate contact information (e.g., the original source's toll-free customer service phone number)?	

• Are data correction requests and responses between consumers and Health Data Sources routed electronically? Do standard messages include:
  • Consumer requests for emendation or removal of data?
  • Response back from Health Data Source confirming concurrence with request or reason for denial of request?
  • Consumer's dispute of data not changed, to be appended to data in question?	

AREA 4: Retention of Health Information	Add comments here:
• Are data-retention practices clearly communicated to the consumer? • See CP2: Policy Notice to Consumers.	
• For inactive accounts, are notices sent to those consumers providing them with the option to renew or extend the retention period, or to close out their accounts?	
• If consumers do not respond to such notices, is there one final notice shortly prior to the expiration of the data-retention period, explaining that the account will be rendered inactive unless they take action?	
• To reduce the risk of re-identification of individuals, is passively generated information that can be used to re-identify individuals (IP addresses, cookies, and web beacons) retained for shorter periods than information that is actively provided by the consumer or authorized Health Data Sources as part of a longitudinal health record? • See CT4: Limitations on Identifying Information.	

AREA 5: Expunging of information	Add comments here:
• Do consumers have the option to request that their information be expunged, and are such requests honored without delay and within a reasonable timeframe? • See CP8: Consumer Obtainment and Control of Information for more on "expunging" information.	
• Do consumers have the option to have all or some of their information be expunged?	
• Upon making such a request, can consumers make copies of their information before it is expunged? • See CT5: Portability of Information.	
• Are consumers provided a timely notice of the status of requests for account termination and/or expunging of information, and does that notice clearly state the consequences and actual definition of "expunging" of information?	
• If full deletion of information is not possible, is the information rendered inaccessible from live servers and stripped of personally identifying data?	
AREA 6: Termination of account	Add comments here:
• Do consumers have the option to request that their accounts be terminated, and are such requests performed without delay and within a reasonable timeframe?	
• Are consumers informed of the consequences and actual definition of account termination?	
• Are consumers provided timely notice of the status of their requests and any necessary follow-up communications until the terminations are completed?	
• Are consumers provided, prior to account termination, an easy-to-use option to export their information to a personal computer, device or other service? • See CT5: Portability of Information.	
• Are consumers provided with an option to expunge information (as an alternative to account termination)?	

Writing Consumer-friendly Policies

PRACTICE AREA CP2: Policy Notice to Consumers

RELATED CORE PRINCIPLES: Openness and Transparency, Purpose Specification, Collection Limitation and Data Minimization, Use Limitation

The following recommended practices relate to written privacy policies, terms and conditions of use, and other relevant policies.

Are privacy policies, terms and conditions of use, and other relevant policies clearly communicated...	Add comments here:
• Without excessive jargon and tested for ease of understanding among the target populations?	
• At 4th to 6th grade reading ability?	
• In the language(s) of the target populations?	
Are consumers clearly informed about...	Add comments here:
• What, how, and why information is collected, used, or shared?	
• How long the information will be kept?	
• How they may exercise choices or controls over the information?	
• Whether and how they can dispute, delete, request corrections, or add comments to information about them?	
• How and under what circumstances they'll be notified if there is a security breach?	
• What is considered to be personally identifying information and what information is not?	
• Whether personal information will be stored in computers and databases located in foreign countries?	
• Whether personal information will be combined with other information about the individual collected from other sources, services, or contexts?	

• The organization's general policy for complying with reasonable law enforcement requests for disclosure of personal information without the consumer's consent?	
• For de-identified information, what limits are in place to prevent making this information "re-identifiable," such as by combining it with other databases?	
Are key policies and protections presented in summary form?	Add comments here:
• Can consumers easily click from a summary to a more detailed version, and vice versa?	
• Is the information tested and presented in different formats (video, interactive, etc.) to reach target populations?	
Do policies clearly show how consumers are protected by explaining…	Add comments here:
• What technologies and practices are in place to protect security, confidentiality, and privacy?	
• What the service is permitted and not permitted to do with personal information?	
Are policy notices accessible…	Add comments here:
• From every page on the web site (links in site's global navigation, footer, or other standard location)	
• From the home page and appropriate screens on which the consumer sets up an account or makes key decisions?	

If the policies have been updated or changed...	Add comments here:
• Are consumers provided adequate notice of changes to policies?	
• Do the notices specifically identify the changes made?	
• Are the version number and effective date clearly shown?	

• Are additional authorizations obtained when policies are materially modified?
  • Each time the policies are modified, consider whether new authorization from the consumer is necessary.
  • The more sensitive or personally exposing the changes to policy, the more specific and discrete the mechanism should be to capture a consumer's consent, and vice versa.
  • Refer to CP2: Policy Notice to Consumers, which provides more information on material and non-material changes.	

• Are users told clearly the consequences of opting-in and opting-out of the new policies? • For example, opting-out may require the consumer to terminate use of the Consumer Access Service. In such cases, the Service should provide the consumer with an easy process for both downloading and printing the user's records.	

Getting Consumer Consent

PRACTICE AREA CP3: Consumer Consent to Collections, Uses and Disclosures of Information

RELATED CORE PRINCIPLES: Purpose Specification, Collection Limitation and Data Minimization, Use Limitation, Individual Participation and Control

The following recommended practices relate to offering consumers consent mechanisms that address the specific uses of personal health information, its sensitivity to the consumer, and the potential benefits and risks of its disclosure and use. Please see CP3: Consumer Consent to Collections, Uses and Disclosures of Information for an explanation on the difference between "general consent" and "independent consent."

When collecting or using identifiable information directly from consumers…	Add comments here:
• Are consumers provided adequate notice of the policies regarding personal data? • See CP2: Policy Notice to Consumers.	
• Are consumers' consent obtained prior to collection or use of such data? • Collections or uses that would be unexpected by a reasonable user should be subject to additional independent consent, which should be obtained from users in advance of the unexpected collection or use.	
In addition to the above, when collecting or using indirectly identifying information about consumers…	Add comments here:
• Are all collections of indirectly identifying information, as well as the purposes and uses of such collections, clearly specified in policy notices?	
• Are consumers' independent consent obtained prior to disclosing to unaffiliated third parties any information that can be directly or indirectly identifiable? • See CT4: Limitations on Identifying Information.	

In addition to the above, when collecting or using identifiable information about consumers from unaffiliated third parties…	Add comments here:
• Are consumers' consent obtained prior to collecting or using information about them from unaffiliated third parties?	
• Is an independent consent mechanism used for collections or uses of third-party data that are likely to be unexpected by a reasonable consumer?	
In addition to the above, when disclosing identifiable information to unaffiliated third parties…	Add comments here:
• Are consumers provided notice and consent mechanisms specifying all disclosures of personal information to third parties – including the purpose for, the uses of, and the policies governing such disclosures?	
• Are mechanisms in place to prevent disclosing or exposing to a third party information sufficient to identify a consumer, or to enable the third party to target the user directly (unless and until the consumer has provided independent consent to do so)?	
In addition to the above, when collecting, using or disclosing "de-identified data"…	Add comments here:
• Are consumers provided adequate notice of the collections, uses, and disclosures of information designated as "de-identified data"—including the purposes for such collections, uses, and disclosures. • Such notice should define what information is considered "de-identified," describe what processes are employed to make it so, and explain the potential risks of "re-identification."	
• Are consumers' general consent obtained prior to collection, use, or disclosure of such "de-identified data"?	
• Are any unaffiliated third parties to which "de-identified data" is disclosed, prohibited contractually and/or through other means, from attempting to "re-identify" the data by, among other things, combining it with other databases of information? • See CT4: Limitations on Identifying Information.	

Policy and Technology Checklists for Procurers and Implementers

MARKLE

Technology Checklist

The recommended policies and practices of the Markle Connecting for Health Common Framework for Networked Personal Health Information are designed to protect consumers, and to guide services, organizations, applications, or health information exchanges that collect, store, or share personal health information on the individual's behalf. The Markle Common Framework for Networked Personal Health Information proposes a set of practices that, when taken together, encourage appropriate handling of personal health information as it flows to and from personal health records (PHRs) and similar applications or supporting services.

The Policy and Technology Checklists for Procurers and Implementers document, derived from this framework, provides recommended practices that may be used in requests for information (RFI), requests for proposals (RFP), procurement requirements or implementation checklists.

The technology practices include:

- Managing and Protecting the Individual's Identity
- Protecting Consumers by Giving Them Audit Trails
- Limiting the Exposure of Identifying Information
- Ensuring the Portability of Consumer Health Information
- Providing Strong Security and System Requirements

Managing and Protecting the Individual's Identity

PRACTICE AREA CT2: Authentication of Consumers

RELATED CORE PRINCIPLES: Data Quality and Integrity, Security Safeguards and Controls

The following recommended practices relate to policies for properly authenticating consumers to ensure that each transaction is associated with the right person.

Identity proofing	Add comments here:

• Are consumer identities verified to an acceptable level of certainty? Which methods are used for establishing the individual's identity?
  • In-person proofing—a face-to-face encounter with the consumer presenting verified current primary government identification that contains a picture and either address of record or nationality (e.g., driver's license or passport)?
  • "Bootstrapped"—in-person proofing by other organizations—partnering with institutions that use in-person proofing or other similar authentication process to establish the consumer's identity?
  • An alternative to in-person proofing?	

• See "Approach 1C: Consider alternatives to in-person proofing" of CT2: Authentication of Consumers for guidelines.	
Issuing tokens or identifiers	Add comments here:

• Once their identity has been established, what tokens or identifiers are issued to consumers? Please indicate whether and how your service performs the following:
  • Binding the consumer's identity in such a way as to facilitate later authentication?
  • Choosing an appropriate token or identifier, such as PINs, cards, tokens, fobs with RF chips, antennas, and fingerprints?
  • Enforcing "strong" passwords if passwords as used as tokens?
  • Limiting attempts on passwords?
  • Establishing a clear policy on requirements for password changes?	

Ongoing monitoring	Add comments here:

• Are periodic or ongoing processes performed to continually improve upon the initial proofing and to weed out compromised identities? Are any of the following performed:
  • Conducting appropriate ongoing monitoring, similar to how credit card companies have algorithms to detect sudden changes in charging behavior, then triggering alerts to consumers?
  • Providing authenticated consumers with online access to an immutable audit log displaying all accesses and data transactions involving their account?	

External audit and enforcement	Add comments here:

• Do you rely on a third party or third parties to perform identity proofing, issuing of tokens, or monitoring? If yes, what audit and redress mechanisms are in place to establish a chain of trust?
  • Are third parties "observable" in how and how well they are performing identity proofing, token-issuing, and ongoing monitoring or any related services to authenticate consumers?
  • Is there a contractual commitment for the parties to notify each other if either detects system compromise above a certain threshold or fails to comply with agreed procedures?
  • Are there mechanisms for enforcement and redress?
  • Have you entered into, or does your service conform to, any a federation or trust framework for identity proofing, token issuing, monitoring, redress or other activities related to authentication?	

Protecting Consumers by Giving Them Audit Trails

PRACTICE AREA CT3: Immutable Audit Trails

RELATED CORE PRINCIPLES: Use Limitation, Individual Participation and Control, Data Quality and Integrity, Accountability and Oversight

The following recommended practices relate to policies for protecting consumers with audit trails and demonstrating compliance with use and disclosure authorizations.

Do the policies ensure the following?	Add comments here:
• Do consumers have access to easy-to-comprehend and clearly labeled electronic audit trails containing immutable entries pertaining to their account, information, and policy consent?	
• Does each entry identify, at a minimum, who has accessed the consumer's records, a date, time, and source stamp for each such access, and the source of each significant transaction?	
• Are consumers informed of how long the audit trail is retained? • The audit trail should be retained at minimum according to the data retention practice of the service.	

• Are the following tracked as "auditable" events/activities?
1. Account:
  a) Access attempts and outcomes (i.e., successes or failures, length of session), including those by proxies.
  b) Logout events, including those by proxies.
2. Transactions and data:
  a) Creation (e.g., self-reported allergy).
  b) Modification (e.g., self-reported downward adjustment to a medication's dosage frequency).
  c) View (e.g., access of a problem list).
  d) Export (e.g., export of data to any third party, or to a device or desktop).
  e) Import (e.g., import of data from a health care provider, claims clearinghouse, or third-party service).
  f) Deletion (e.g., removal of a medication the consumer no longer takes).
  g) Dispute (e.g., the consumer challenges the accuracy of a professionally sourced data element).
  h) Proxy (e.g., setting up access to the record by a proxy, such as a caregiver).	

3. Policy: a) Consent (e.g., capture of the consumer's general and independent consents, with roll-back access to versions of applicable policies to which the consumer consented). b) Revocation (e.g., the consumer decides to terminate a previously authorized consent that allowed sharing of data with a third-party service provider).	

Limiting the Exposure of Identifying Information

PRACTICE AREA CT4: Limitations on Identifying Information

RELATED CORE PRINCIPLES: Purpose Specification, Collection Limitation and Data Minimization, Use Limitation, Security Safeguards and Controls

The following recommended practices relate to policies for protecting consumers by limiting identifying information exposed to partners.

Do the policies ensure the following?	Add comments here:
• Are disclosures of identifying data limited to only those data that are necessary to perform the specified function(s) that the data recipient is authorized to perform?	
• Are policies in place to limit the release or exposure of information that can be directly or indirectly tied to an individual, including electronic identifiers such as IP address, cookies, and web beacons? • Any release of such indirectly or directly identifying information should be consistent with all nine Markle Connecting for Health Core Principles and all of the Practice Areas of the Markle Common Framework for Networked Personal Health Information, particularly specification of purpose, limitation of use to only specified purpose, and no unauthorized combining of data to create a more complete profile of individuals.	

Ensuring the Portability of Consumer Health Information

PRACTICE AREA CT5: Portability of Information

RELATED CORE PRINCIPLE: Individual Participation and Control

The following recommended practices relate to policies for making consumers' personally identifiable information available to any and all applications to best meet their needs.

Export of data to the consumer: Do consumers have an easy-to-use mechanism to export their information that...	Add comments here:
• Provides information in human-readable form?	
• Includes exports and imports in audit trail information? • See CT3: Immutable Audit Trails.	
• Includes a printer-friendly format?	
• Enables data to be exported into industry standard software, such as spreadsheets, PDFs, or text files?	
Export and import data among consumer access services and PHRs: Do consumers have an easy-to-use mechanism to export their information that...	Add comments here:
• Provides storage options for documents gathered from past services or other health data sources? • For example, a consumer could export information from one Consumer Access Service into a standard software format such as PDF and store it on her desktop, then upload those PDF documents into a secure account at a new Consumer Access Service.	
• Conforms to industry standards for health data subsets as they become available and broadly implemented?	

Providing Strong Security and System Requirements

PRACTICE AREA CT6: Security and Systems Requirements

RELATED CORE PRINCIPLE: Security Safeguards and Controls

The following recommended practices relate to policies for strong security and systems requirements to maintain trust among all network participants handling personal health information.

Do policies ensure the following?	Add comments here:

• Are industry best practices[1] and the HIPAA Security requirements adopted for data transaction and storage security? For example:
  • Is sensitive data encrypted within the equipment that holds the data so as to prevent unauthorized access and disclosure in the case of a physical loss?
  • Are facilities that house equipment (e.g., servers, backup devices, etc.) which store health data physically secured and attended at all times?
  • What steps are taken to ensure a secure transmission of the user's data, including use of encryption protocols such as Secure Socket Layer (SSL) technology?	

• Is there continuous monitoring of industry practices and threats? • Are there regular risk assessments and systems audits?	

• Are there strict policies and ongoing personnel training in the following areas?
  • Who can access consumer data?
  • Limitations on data that can be accessed by authorized persons for specified purpose? Are such accesses auditable?
  • Consequences of and for security violations?
  • Is there regular training and reminders of such policies?	

• Are endorsed third-party applications and services held to the same security and system requirements, whether those applications are browser-based or mobile devices?	

[1] National Institute of Standards and Technology, "Recommended Security Controls for Federal Information Systems and Organizations," *Department of Commerce*. NIST Special Publication 800-53, Revision 3, August 2009. http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf (accessed on March 12, 2012).