OPERATIONS MANUAL

Part 1 -- Privacy Policies

February 25, 2010

[j]

Prepared for Redwood MedNet by

minformatics.com

Operations Manual, Volume 1, Privacy Policies*

PREFACE	TOPIC
i	**Policy Topic Index**
ii	**Policy Table of Contents**
iii	**About Redwood MedNet**
iv	**About the Redwood MedNet Operations Manual**
v	**Definitions**
vi	**Connecting for Health's Nine Policy Principles**
RANGE	POLICY CATEGORY
100	**Compliance with Law and Policy**
200	**Notice of Privacy Practices**
300	**Individual Participation and Control of Information**
400	**Uses and Disclosures of Health Information**
500	**Information Subject to Special Protection**
600	**Minimum Necessary**
700	**Workforce, Agents and Contractors**
800	**Amendment of Data**
900	**Requests for Restrictions**
1000	**Mitigation**

*Derived from the Connecting for Health Common Framework

These policies are based on a seminal work entitled "Model Privacy Policies and Procedures for Health Information Exchange," which was originally published as part of **The Markle Foundation Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange** (©2006 Markle Foundation). That work is made available to the public by the Markle Foundation subject to the terms of a license (the "Markle License") which is available upon request from Redwood MedNet. The Markle License also may be viewed at: http://www.connectingforhealth.org/license.html.

These Privacy Policies are made available, subject to the limitations of the Markle License, and pursuant to a license granted by Redwood MedNet, Inc., a copy of which is available at: http://www.redwoodmednet.org/license.html

Privacy Policy Table of Contents

NUMBER	POLICY
100	**Compliance with Law and Policy**
101	Compliance with Laws and Regulations
102	Compliance with Redwood MedNet Policies
103	Compliance with Participant Policies
200	**Notice of Privacy Practices**
201	Content of the Notice of Privacy Practices
202	Provision of the Privacy Notice to Individuals
203	Individual Acknowledgement of the Privacy Notice
204	Participant Choice in Distribution of the Privacy Notice
300	**Individual Participation and Control of Information**
301	Individual Choice Not to Have Information Included in the RLS
302	Individual Choice Exercised Through the Participant
303	Revising Individual Choice
304	Documentation of Individual Choice
305	Participant Choice on Information Inclusion
306	Choice and the Provision of Coverage or Care
307	Individual Request for Patient Information from the HIE
400	**Uses and Disclosures of Health Information**
401	Definition of Disclosure
402	Disclosure Compliance with Laws and Regulations
403	Permissible Purposes Required for Use or Disclosure
404	Disclosure Compliance with Redwood MedNet Policies
405	Disclosure Compliance with Participant Policies
406	Accounting of Disclosures
407	Disclosure Audit Logs
408	Disclosure Authentication Requirements
409	Disclosure Access Process
410	Occurrence of a Health Information Breach
500	**Information Subject to Special Protection**
501	Information Subject to Special Protection
600	**Minimum Necessary**
601	Minimum Necessary Use of Health Information
602	Minimum Necessary Disclosure of Health Information
603	Minimum Necessary Health Information Requests
604	Minimum Necessary Disclosure of Entire Medical Record

700 **Workforce, Agents and Contractors**
701 Participant Access to Redwood MedNet Services
702 Participant Training for Use of Redwood MedNet Services
703 Participant Discipline for Non-Compliance
704 Participant Reporting of Non-Compliance
705 Participant Discipline for Non-Compliance

800 **Amendment of Data**
801 Amendment of Individual Data

900 **Requests for Restrictions**
901 Individual Requests for Restrictions

1000 **Mitigation**
1001 Appropriate Remedial Action
1002 Breach Notification

About Redwood MedNet

Redwood MedNet is a community based 501(c)(3) nonprofit corporation established in 2005 in the rural Lake, Mendocino and Sonoma County region of rural Northern California. The mission of Redwood MedNet is to demonstrate the secure and appropriate sharing of electronic health files and clinical data, and to develop, improve and assist in the implementation of health information technology for all health care providers, caregivers and consumers in Northern California.

Redwood MedNet Board of Directors -- January 2010

DIRECTOR	OFF.	POSITION	SITE
Mark Apfel, MD	Sec.	Medical Director	Anderson Valley Health Center
Jed Gladstein		Attorney	
Carl Henning, MD	Pres.	Orthopedic Surgeon	Ukiah Valley Primary Care
Ray Hino, MHA		CEO	Mendocino Coast District Hospital
Jack Neureuter		CEO	Alliance Medical Center
Tom Reidenbach, PharmD	VP	Pharmacist	Myer's Medical Pharmacy
Robert Rushton, MD		Family Physician	Robert Rushton, MD
Marvin Trotter, MD		Health Officer	Mendocino County Public Health
Mark Turner		I.S. Site Coordinator	Ukiah Valley Medical Center

Redwood MedNet Operations Manual

The Redwood MedNet Operations Manual is composed of three working collections of dynamically evolving policy and procedure documents which govern participation in and operation of the Redwood MedNet health information exchange ("HIE") services.

1. Privacy Policies. Derived from the "Connecting for Health Model Privacy Policies," localized and adapted by Redwood MedNet -- a public document.
2. Operating Procedures. A private internal manual of business rules. Available to participants in the Redwood MedNet HIE services -- not a public document.
3. Security Rules. Perimeter defense plan for Redwood MedNet system administrators and network engineers. Restricted access content. Distribution limited to members of the Redwood MedNet Security Team.

Definitions

The meanings of the following terms shall be consistent throughout these policies and procedures.

Authorized User (or "User") means an individual (i.e., a person) designated to access the Redwood MedNet HIE services on behalf of a Participant, such as an employee of a Participant, or a credentialed member of the Participant's medical staff.

Data Provider means a Participant who provides clinical data to the HIE services operated by Redwood MedNet.

Data Recipient means a Participant who receives clinical data from the HIE services operated by Redwood MedNet.

Health Information Exchange (or "HIE") means the Redwood MedNet electronic health information delivery and aggregation services accessed by Authorized Users.

Individual means a person, generally a patient but possibly a caregiver for a patient, who requests access to Patient Data available from the HIE services operated by Redwood MedNet.

Participant means an entity (e.g., a family practice, a community clinic, a laboratory, a hospital, a radiology center, etc.) that has signed a Participation Agreement with Redwood MedNet, and that interacts with the Redwood MedNet HIE services as a Data Provider and/or a Data Recipient.

Participation Agreement means the legally binding agreement which enables Redwood MedNet to offer HIE services to Participants.

Patient Data means electronic health, demographic and related information provided by a Data Provider to a Data Recipient via the Redwood MedNet HIE services.

Record Locator Service (or "RLS") means an electronic index of Participant locations that host access to Patient Data on a specific Individual that is available via the Redwood MedNet HIE services.

Connecting for Health's Nine Policy Principles

1. **Openness and Transparency.** Openness about developments, procedures, policies, technology and practices with respect to the treatment of personal health data is essential to protecting privacy. Individuals should be able to understand what information exists about them, how that information is used, and how they can exercise reasonable control over that information. This transparency helps promote privacy practices and instills confidence in individuals with regard to data privacy, which in turn can help increase participation in health data networks.
2. **Purpose Specification and Minimization.** Data must be limited to the amount necessary to accomplish specified purposes. Minimization of use will help reduce privacy violations, which can occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

3. **Collection Limitation.** Personal health information should be obtained only by fair and lawful means and, if applicable, with the knowledge and consent of the pertinent individual. In an electronic networked environment, it is particularly important for individuals to understand how information concerning them is being collected because electronic collection methods may be confusing to average users. Similarly, individuals may not be aware of the potential abuses that can arise if they submit personal health information via an electronic method.
4. **Use Limitation.** The use and disclosure of health information should be limited to those purposes specified by the data recipient. Certain expectations such as law enforcement or security may warrant reuse of data for other purposes. However, when data is used for purposes other than those originally specified, prior de-identification of the data can help protect individual privacy while enabling important benefits to be derived from the information.
5. **Individual Participation and Control.** Every individual should retain the right to request and receive in a timely and intelligible manner information regarding who has that individual's health data and what specific data the party has, to know any reason for a denial of such request, and to challenge or amend such personal information. Because individuals have a vital stake in their own personal health information, such rights enable them to be participants in the collection and use of their data. Individual participation promotes data quality, privacy and confidence in privacy practices.
6. **Data Integrity and Quality.** Health data should be accurate, complete, relevant, and up-to-date to ensure its usefulness. The quality of health care depends on the existence of accurate health information. Moreover, individuals can be adversely affected by inaccurate health information in other arenas like insurance and employment. Thus, the integrity of health data must be maintained and individuals must be permitted to view information about them and amend such health information so that it is accurate and complete.
7. **Security Safeguards and Controls.** Security safeguards are essential to privacy protection because they help protect data loss, corruption, unauthorized use, modification and disclosure. With increasing levels of cyber-crime, networked environments may be particularly susceptible without adequate security controls. Design and implementation of various technical security precautions such as identity management tools, data scrubbing, hashing, auditing, authenticating and other tools cal strengthen information privacy.
8. **Accountability and Oversight.** Privacy protections have little weight if privacy violators are not held accountable for compliance failures. Employee training, privacy audits, and other oversight tools can help to identify and address privacy violations and security breaches by holding accountable those who violate privacy requirements and identifying and correcting weaknesses in their security systems.
9. **Remedies.** The maintenance of privacy protection depends upon legal and financial means to remedy any privacy or security breaches. Such remedies should hold violators accountable for compliance failures, reassure individuals about the organization's commitment to information privacy, and mitigate any harm that privacy violations may cause individuals.

Policy Principle and Category Crosswalk

PRINCIPLE	*CATEGORY*	*100*	*200*	*300*	*400*	*500*	*600*	*700*	*800*	*900*	*1000*
Openness and Transparency		*X*	*X*						*X*		*X*
Purpose Specification and Minimization			*X*	*X*	*X*	*X*					
Collection Limitation			*X*	*X*	*X*	*X*	*X*				
Use Limitation			*X*	*X*	*X*	*X*	*X*	*X*		*X*	
Individual Participation and Control			*X*	*X*		*X*			*X*	*X*	
Data Integrity and Quality		*X*			*X*	*X*	*X*	*X*	*X*		*X*
Security Safeguards and Controls					*X*	*X*	*X*	*X*			*X*
Accountability and Oversight		*X*			*X*			*X*	*X*	*X*	*X*
Remedies		*X*						*X*			*X*

Policy Categories

100 *Compliance with Law and Policy*
200 *Notice of Privacy Practices*
300 *Individual Participation and Control of Information*
400 *Uses and Disclosures of Health Information*
500 *Information Subject to Special Protection*
600 *Minimum Necessary*
700 *Workforce, Agents and Contractors*
800 *Amendment of Data*
900 *Requests for Restrictions*
1000 *Mitigation*

Category 100: Compliance with Law and Policy

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Privacy Principles: Openness and Transparency; Data Integrity and Quality; Accountability and Oversight; Remedies

Purpose: Policies to establish comprehensive privacy protection, compliance, enforcement procedures, and remedies following violations are crucial to maintaining health information privacy. This policy category recognizes that formal promulgation of internal Redwood MedNet policies and procedures ("Redwood MedNet Policies") which require that Redwood MedNet participants[1] ("Participants") comply with applicable law is an indispensable feature of essential privacy protections. When there is a conflict between Redwood MedNet policies and Participant policies, the policy that is most protective of individual privacy should govern decision making. This is designed to make clear that these policies provide a floor and that Participants may choose to enhance privacy protections when appropriate. This deference to more protective policies echoes the federal pre-emption requirements of HIPAA, which do not preempt more protective state privacy laws.[2]

The requirement that Participants develop internal policies will help implement the principles of sound data management practices and accountability as well as ensure that decisions affecting individuals' privacy interests are made thoughtfully, rather than on an ad hoc basis. Written documentation of such policies facilitates the training of personnel who will handle health information and enhances the accountability of Participants and the members of their workforce. Finally, the existence of internal policies for compliance by Redwood MedNet with applicable law creates transparency surrounding the handling and safeguarding of data by entities participating in the Redwood MedNet HIE services.

Scope: These policies apply to all entities participating in the Redwood MedNet HIE services, and to any entity that may provide, make available, or request health information through the Redwood MedNet HIE services.

Policies

101. Compliance with Laws and Regulations. -- *modified January 28, 2010*

102. Compliance with Redwood MedNet Policies. -- *modified January 28, 2010*

103. Compliance with Participant Policies. -- *modified January 28, 2010*

Policy 101: Compliance with Laws and Regulations

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

101. Each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. Each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure constant and consistent compliance with all applicable laws and regulations.

Policy 102: Compliance with Redwood MedNet Policies

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

102. Each Participant shall, at all times, comply with all applicable Redwood MedNet Policies, which may be revised and updated from time to time upon reasonable written notice to Participants. Each Participant is responsible for ensuring it has a copy of and is in compliance with the most recent version of these Redwood MedNet Policies.

Policy 103: Participant Policies

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

103. Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and regulations and with the Redwood MedNet Policies. In the event of a conflict between Redwood MedNet Policies and an institution's own policies and procedures, the Participant shall comply with the policy that is more protective of individual privacy and security.

---

[1] Note that in the Redwood MedNet policies a "Participant" is a business entity contractually engaged with Redwood MedNet as a data provider and/or a data recipient. The Participant role is distinct from a "User", who is a person that is authorized by a Participant to access the Redwood MedNet online services, or from an "Individual", who is a person acting without affiliation with a Redwood MedNet Participant that requests access to patient information available from Redwood MedNet.

[2] 45 C.F.R. § 160.203.

Category 200: Notice of Privacy Practices

Version: 20071108.h *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Openness and Transparency; Purpose Specification and Minimization; Collection Limitation; Use Limitation; Individual Participation and Control.

Purpose: These policies incorporate HIPAA requirements obligating entities to provide a notice of the privacy practices to individuals upon request.[1] The policies exceed HIPAA requirements by also requiring disclosures to individuals of certain information related to the Redwood MedNet HIE and RLS.[2] For example, under these policies, the Privacy Notice informs individuals about:

- What information the Participant may make available through the HIE and RLS
- Who is able to access the information
- How an individual can have information concerning them removed from the RLS

These are not HIPAA requirements, but rather build and expand upon the privacy law to help incorporate information related to the nationwide health information network ("NHIN") and the local HIE. This policies exceed HIPAA requirements by providing suggestions for additional, voluntary protections that can be implemented at the Participant level to enhance consumer protections, such as excluding individuals from the RLS global index unless prior consent is obtained or loading information into the RLS only after a notification and opportunity to decline participation has been provided to individual patients.

In addition, these policies help ensure that information is collected and shared electronically in a fair manner with the knowledge of relevant individuals. This is particularly important in a networked environment where the technology may be unfamiliar to all users.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE and RLS, and that may provide or make available health information through the HIE and RLS.

Policies

201. Content of the Notice of Privacy Practices. -- *modified January 28, 2010*

202. Provision of the Privacy Notice to Individuals. -- *modified January 28, 2010*

203. Individual Acknowledgement of the Privacy Notice. -- *modified January 28, 2010*

204. Participant Choice in Distribution of the Privacy Notice. -- *modified January 28, 2010*

Policy 201: Content of the Notice of Privacy Practices

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

201. Each Participant shall develop and maintain a notice of privacy practices (the "Notice") that complies with applicable law and with these policies. The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule[3] and comply with all applicable laws and regulations. The Notice also shall include a description of the HIE and RLS and inform individuals regarding:

(a) What information the institution may include in and make available through the HIE and RLS

(b) Who is able to access the information in the HIE and RLS

(c) For what purposes such information can be accessed

(d) How the individual can have his or her information removed from the RLS

Policy 202: Provision of the Privacy Notice to Individuals

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

202. Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, and such policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

- For Participants that are health care providers, the Notice shall be:
  - (i) Available to the public upon request
  - (ii) Posted on all web sites of the Participant and available electronically through such sites
  - (iii) Provided to a patient at the date of first service delivery
  - (iv) Available at the institution
  - (v) Posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.[4]
- For Participants that are health plans, the Notice shall be:
  - (i) Available to the public upon request
  - (ii) Provided to new enrollees at the time of plan enrollment
  - (iii) Provided to current plan enrollees within 60 days of a material revision
  - (iv) Posted on the plan's web sites and available electronically through such sites. Participating health plan institutions also shall notify individuals covered by the plan of the availability of the Notice and how to obtain a copy at least once every three years.[5]

Policy 203: Individual Acknowledgement of the Privacy Notice

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

203. Each Participant that is a health care provider shall make a good faith effort to obtain each individual's written acknowledgment of receipt of the Notice or to document their efforts and/or failure to do so. The acknowledgment of the Notice shall comply with all applicable laws and regulations.[6] Each Participant shall have its own policies and procedures governing the process of obtaining an acknowledgment, and such policies and procedures shall be consistent with this Policy and comply with applicable laws and regulations.

Policy 204: Participant Choice in Distribution of the Privacy Notice

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

204. Participants may choose a more proactive notice distribution process than provided herein and may include more detail in their notice of privacy practices. Possible additional protections for individuals whose information may be made available through the RLS (not all of which pertain to notice policies alone) could include:

- Mailing the revised notice or a notification letter allowing for removal or exclusion of the information about that individual from the RLS to every individual prior to loading the information into the RLS or shortly thereafter
- Excluding individuals from the RLS index unless individual consent is obtained
- Loading individual information into the RLS on a going-forward, new individual encounter basis only
- Developing a method for time-stamping an RLS record to indicate when the record was loaded into the index
- Developing a method for allowing individuals to limit access to their RLS records
- Obtaining individual consent prior to each inquiry made to the RLS index by a Participant, or on a periodic basis.

---

1 45 C.F.R. § 164.520.

2 HIPAA requires the Notice of Privacy Practices to include a description, with "at least one example, of the types of uses and disclosures that the covered entity is permitted…to make for…treatment, payment and health care operations" and a description of those other purposes for which the entity "is permitted or required…to use or disclose protected health information without" individual authorization. 45 C.F.R. § 164.520(b)(1)(ii)(A). Unlike this policy, HIPAA does not require the Privacy Notice to set forth what specific information may be disclosed and who may access the information.

3 45 C.F.R. § 164.520(b).

4 45 C.F.R. § 164.520(c)(2), (3).

5 45 C.F.R. § 164.520(c)(1), (3).

6 45 C.F.R. § 164.520(c)(2)(ii).

Category 300: Individual Participation and Control of Information

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Purpose Specification and Minimization; Collection Limitation; Use Limitation; Individual Participation and Control.

Purpose: These policies provide greater privacy protection over personal health information than the HIPAA Privacy Rule by allowing individuals to elect whether or not to have information about them included in the RLS. Importantly, individuals are treated as participants in the process of health information collection and dissemination, rather than as spectators. Providing such consumer protections allows individuals to better understand the conditions under which information concerning them might be used, to restrict or allow such use, and to develop confidence in the protections surrounding the use of their data.

By enhancing reasonable individual control over the collection and use of health information these policies promote consumer confidence that their health information is being collected and used in accordance with their individual preferences.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE and RLS, and that may provide or make available health information through the HIE and the RLS.

Policies

301. Individual Choice to Opt Out of the RLS. -- *modified January 28, 2010*

302. Individual Choice Exercised Through the Participant. -- *modified January 28, 2010*

303. Revising Individual Choice. -- *modified January 28, 2010*

304. Participant Responsibility to Document Individual Choice. -- *modified January 28, 2010*

305. Participant Authority and Patient Consent. -- *modified January 28, 2010*

306. Individual Choice and the Provision of Coverage or Care. -- *modified January 28, 2010*

307. Individual Request for Patient Information from the HIE. -- *approved February 25, 2010*

Policy 301: Individual Choice to Opt Out of the RLS

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

301. Any Individual may choose not to have his or her information included in or made available through the RLS (i.e., "opt out").

Policy 302: Individual Choice Exercised Through the Participant

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

302. An Individual's choice not to have information about him or her included in or made available through the RLS shall be exercised through the Participant, as described in the institution's Notice, after which time the institution shall no longer include the individual in the RLS. If the Individual chooses to have such information excluded from the RLS, then Participants shall develop and implement appropriate policies and procedures to remove information about an individual from the RLS.

Policy 302: Revising Individual Choice

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

303. An Individual who has previously chosen not to make his or her information available through the RLS (i.e., "opt out), and who wishes to revise that choice and "opt in" to the RLS, may do so. Individual choice to opt in or to opt out of participation in the RLS shall be exercised through the Participant.

Policy 304: Participant Responsibility to Document Individual Choice

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

304. Each Participant shall maintain documentation of all individual patient decisions to exclude personal information from the RLS (i.e., opt out).

Policy 305: Participant Authority and Patient Consent

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

305. Participants shall establish reasonable and appropriate processes to enable the exercise of an individual patient's choice not to have information about him or her included in the RLS (i.e., opt out). Each Participant retains the authority to decide whether and when to obtain patient consent prior to making information available through the RLS.

Policy 306: Individual Choice and the Provision of Coverage or Care

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

306. A Participant shall not withhold coverage or care from an individual on the basis of that individual's choice not to have information about him or her included in the RLS.

Policy 307: Individual Request for Patient Information from the HIE

Version: 20100225.j *Adopted: February 25, 2010*

307. An individual patient, or an Individual acting on behalf of a patient, may request a copy of Patient Data on an individual patient that is available through the Redwood MedNet HIE services. As Redwood MedNet originates no Patient Data, and contains only Patient Data that was originated by a Data Provider, and has no direct relationship with Individuals, the proper process for an Individual to request such information is to make the request of the appropriate Data Provider who was the source of the information available via the Redwood MedNet HIE services. However, there are legitimate reasons why this process may not be practical (e.g., Data Provider has retired, or is deceased, etc.). Therefore, Redwood MedNet will allow an Individual to request Patient Data and will require adequate proof of the Individual's identity and legal right to the Patient Data.

Category 400: Uses and Disclosures of Health Information

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Purpose Specification and Minimization; Collection Limitation; Use Limitation; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight.

Purpose: These policies integrate the general premise of HIPAA that health information may be used only for permissible purposes and its more specific requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose.[1] In general, requests for disclosure of and/or use of health information for treatment, payment, and the health care operations of a covered entity, as each is defined by HIPAA, will be permitted.[2] Furthermore, subject to certain limitations, and under certain circumstances, requesting disclosure of and using health information for law enforcement,[3] disaster relief,[4] research,[5] and public health[6] purposes also may be permissible. Accessing health information through either the RLS or the HIE for marketing or marketing-related purposes is prohibited without specific patient authorization.[7] Under no circumstances may health information be accessed or used for discriminatory purposes. For example, a health plan would not be permitted to use the RLS to determine if a member has visited a health care provider for whom the health plan has not been billed. Such activity would be an impermissible and discriminatory purpose and is prohibited by applicable law and under these policies.

Requiring consideration of the purpose of a use and minimization of the use of information reduces the likelihood of inadvertent or intentional misuses of information. By ensuring that Participants have legally required documentation prior to the use or disclosure of information, these policies help enhance the fair and legal collection and use of data, the oversight of data use and accountability for privacy violations.[8] In addition, the integration of HIPAA's accounting of disclosures and individual access to information requirements allows individuals to understand how health information about them is shared and to exercise certain rights regarding information about them.[9]

These policies also require security measures essential to identify and remedy loss, unauthorized access, destruction, use, modification, or disclosure of personal health information. The audit requirement reflects the general requirements of the HIPAA Security Rule that entities implement policies to prevent security violations, assess security risks, and examine data storage and access technology.[10] In a manner more protective than HIPAA, these policies also establishe monitoring requirements to log when information is accessed and by whom. To prevent unauthorized access of information and maintain data integrity and quality, the authentication provision of this policy requires that both the identity and authority of an entity requesting health information be verified and authenticated, integrating requirements from the HIPAA Privacy Rule and Security Rule.[11]

The combination of these policies' use and security provisions helps guarantee that health information is used and accessed only as authorized and that Participants have proper measures in place to identify and address privacy violations.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE, and that may provide, make available, or request health information through the HIE.

Policies

401. Definition of Disclosure. -- *approved February 25, 2010*
402. Disclosure Compliance with Laws and Regulations. -- *modified January 28, 2010*
403. Permissible Purposes Required for Use or Disclosure. -- *modified January 28, 2010*
404. Disclosure Compliance with Redwood MedNet Policies. -- *modified January 28, 2010*
405. Disclosure Compliance with Participant Policies. -- *modified January 28, 2010*
406. Accounting of Disclosures. -- *modified January 28, 2010*
407. Disclosure Audit Logs. -- *modified January 28, 2010*
408. Disclosure Authentication Requirements. -- *modified January 28, 2010*
409. Disclosure Access Process. -- *modified January 28, 2010*
410. Occurrence of a Health Information Breach. -- *approved February 25, 2010*

Policy 401: Definition of Disclosure

Version: 20100225.j *Adopted: February 25, 2010*

401. Disclosure of health information in the Redwood MedNet policies is defined as "the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information."[12]

Policy 402: Disclosure Compliance with Laws and Regulations

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

402. All disclosures of health information through the HIE and the use of information obtained from the HIE shall be consistent with all applicable federal, state, and local laws and regulations and shall not be used for any unlawful discriminatory purpose. If applicable law requires that certain documentation exist or that other conditions be met prior to using or disclosing health information for a particular purpose, the requesting institution shall ensure that it has obtained the required documentation or met the requisite conditions and shall provide evidence of such at the request of the disclosing institution.[13]

Policy 403: Permissible Purpose Required for Use or Disclosure

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

403. A Participant may request health information through the RLS or HIE only for purposes permitted by applicable law. Each Participant shall provide or request health information through the RLS or HIE only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulations,[14] and by these Redwood MedNet Policies. Information may not be requested for marketing or marketing related purposes without specific patient authorization. Under no circumstances may information be requested for a discriminatory purpose. In the absence of a permissible purpose, a Participant may not request information through the RLS or from the HIE.

Policy 404: Disclosure Compliance with Redwood MedNet Policies

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

404. Uses and disclosures of and requests for health information via the HIE shall comply with all Redwood MedNet Policies, including, but not limited to, the Redwood MedNet policies on Information Subject to Special Protection (500s) and on Minimum Necessary Use of Health Information (600s).[15]

Policy 405: Disclosure Compliance with Participant Policies

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

405. Each Participant shall refer to and comply with its own internal policies and procedures regarding disclosures of health information and the conditions that shall be met and the documentation that shall be obtained, if any, prior to making such disclosures.

Policy 406: Accounting of Disclosures

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

406. Each Participant disclosing health information through the HIE shall document the purposes for which such disclosures are made, as provided by the requesting institution, and any other information that may be necessary for compliance with the disclosure requirements of the HIPAA Privacy Rule.[16] Each Participant is responsible for ensuring its compliance with such requirements and may choose to provide Individuals with more information in the accounting than is required. Each requesting institution shall provide information required for the disclosing institution to meet its obligations under the accounting of disclosures requirement of the HIPAA Privacy Rule.

Policy 407: Disclosure Audit Logs

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

407. Redwood MedNet and its Participants shall maintain an audit log documenting which Participants posted and accessed the information about an individual through the RLS and when such information was posted and accessed.[17] Redwood MedNet and Participants shall implement a system allowing patients to request and receive a listing of who has posted and who has accessed information about them, and when such information was accessed, through the RLS.[18] Individual patient requests for audit information are exercised through the Participant.

Policy 408: Disclosure Authentication Requirements

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

408. Each Participant shall follow uniform minimum authentication requirements for verifying and authenticating Users within their institutions who have access to, as well as other Participants who request access to, information through the Redwood MedNet HIE and/or the RLS.[19] [20]

Policy 409: Disclosure Access Process

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

409. Redwood MedNet will establish a formal process through which information in the HIE or RLS can be requested by a patient or on a patient's behalf.[21] Redwood MedNet and Participants shall consider and work towards providing patients with direct access to the information contained in the RLS that is about them.[22]

Policy 410: Occurrence of a Health Information Breach

Version: 20100225.j *Approved: February 25, 2010*

410. As set forth under HIPAA and ARRA[23], notification to individuals is required if their health information has been breached. Breach is defined as the unauthorized acquisition, access, use or disclosure of protected health information. However, it is not a breach:

- Where an unauthorized person who receives the health information cannot reasonably have been able to retain it;
- If an unintentional acquisition, access or use occurs within the scope of employment or a professional relationship and the information does not go any further (i.e, it is not further acquired, accessed, used or disclosed); or
- It is an inadvertent disclosure that occurs within a Participant facility, and the information does not go any further.

Only breaches of "unsecured" health information trigger the notification requirement.

---

1 45 C.F.R. § 164.502(b).

2 45 C.F.R. § 164.502(1)(ii), 506. Under HIPAA, treatment is defined as "the provision, coordination, or management of health care and related services by one or more health care providers ... " 45 C.F.R. § 164.501. Payment refers to "activities undertaken by: (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care." Id. Such activities include eligibility and coverage determinations; risk adjustments; billing, claims management and collection activities; medical necessity review; and utilization review. Health care operations includes activities related to covered functions for (i) conducting quality assessment and improvement; (ii) evaluating competence, qualifications and performance of health care professionals, evaluating health plan performance, training and credentialing activities; (iii) underwriting, "premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits"; (iv) "conducting or arranging for medical review, legal services, and auditing functions;" (v) business planning and development; and (vi) business management and administrative activities. Id.

3 45 C.F.R. § 164.512(f).

4 45 C.F.R. § 164.510(b)(4).

5 45 C.F.R. § 164.512(i).

6 45 C.F.R. § 164.512(b).

7 45 C.F.R. § 164.508(a)(3) & (b).

[8] 45 C.F.R. § 164.530(j).

[9] 45 C.F.R. § 164.528; 164.524.

[10] 45 C.F.R. § 164.316, 164.308(a)(1)(i).

[11] 45 C.F.R. § 164.514(h), 164.312(d).

[12] 45 C.F.R. § 160.103.

[13] 45 C.F.R. § 164.530(j).

[14] 45 C.F.R. § 164.502(a), (b).

[15] 45 C.F.R. § 164.502(b).

[16] 45 C.F.R. § 164.528. For HIPAA Covered Entities, this is currently required by law.

[17] 45 C.F.R. § 164.316, 164.308(a)(1)(i).

[18] The Markle Foundation, **Auditing Access to and Use of a Health Information Exchange**, Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange (2006).

[19] 45 C.F.R. § 164.514(h), 164.312(d).

[20] The Markle Foundation, **Authentication of System Users**, Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange (2006).

[21] 45 C.F.R. § 164.524.

[22] The Markle Foundation, **Patients' Access to Their Own Health Information**, Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange (2006).

[23] ARRA Section 13402

Category 500: Information Subject to Special Protection

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Purpose Specification and Minimization; Collection Limitation; Use Limitation; Individual Participation and Control; Data Integrity and Quality; Security Safeguards and Controls.

Purpose: These policies facilitate individualized privacy protections by requiring Participants to heed any special protections of specific information types as set forth under applicable laws or regulations. In complying with these special protections, the collection, use and disclosure of health information by Participants is limited to legitimate purposes. Moreover, in guaranteeing deference to the law or policy most protective of privacy, the provisions below echo the federal preemption requirements of HIPAA which defer to state laws that are more protective than the privacy provisions of HIPAA.[1]

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE, and that may provide or make available health information through the HIE.

Policies

501. Information Subject to Special Protection. -- *modified January 28, 2010*

Policy 501: Information Subject to Special Protection

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

501. Some health information may be subject to special protection (e.g., substance abuse, mental health, HIV, etc.). Each Participant shall determine and identify what information is subject to special protection under applicable federal, state, and/or local law prior to disclosing any information through the HIE. Each Participant is responsible for complying with such laws and regulations.

---

[1] The Markle Foundation, **Patients' Access to Their Own Health Information**, Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange (2006).

Category 600: Minimum Necessary

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Collection Limitation; Use Limitation; Data Integrity and Quality; Security Safeguards and Controls.

Purpose: These policies incorporate the HIPAA requirement that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose.[1] The policies exempt treatment disclosures from this minimum necessary requirement to balance the protection of privacy with the provision of quality health care. In assessing the smallest amount of information that is necessary to accomplish a particular purpose, Participants are less likely to collect, use or disclose information for an unauthorized purpose. Minimal collection, access, use and disclosure increases public confidence in the privacy practices of Participants, enhances information privacy, and diminishes the potential for data corruption and security violations.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE, and that may provide, make available, or request health information through the HIE.

Policies

601. Minimum Necessary Use of Health Information. -- *modified January 28, 2010*

602. Minimum Necessary Disclosure of Health Information. -- *modified January 28, 2010*

603. Minimum Necessary Health Information Requests. -- *modified January 28, 2010*

604. Minimum Necessary Disclosure of Entire Medical Record. -- *modified January 28, 2010*

Category 601: Minimum Necessary Use of Health Information

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

601. Each Participant shall use only the minimum amount of health information obtained through the HIE as is necessary for the specific purpose of such use. Each Participant shall share health information obtained through the HIE, and shall allow access to such information by only those workforce members, agents, and contractors who need the specific information in connection with their job function or duties.

Policy 602: Minimum Necessary Disclosure of Health Information

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

602. Each Participant shall disclose through the HIE only the minimum amount of health information as is necessary for the specific purpose of the disclosure. Disclosures to a health care provider for treatment purposes and disclosures required by law are not subject to this Minimum Necessary Policy.

Policy 603: Minimum Necessary Health Information Requests

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

603. Each Participant shall request only the minimum amount of health information through the HIE as is necessary for the intended purpose of the request. This Minimum Necessary Policy does not apply to requests by qualified health care providers for treatment purposes.

Policy 604: Minimum Necessary Disclosure of Entire Medical Record

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

604. A Participant shall not use, disclose, or request an individual's entire medical record except where specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or request. This limit does not apply to disclosures to or requests by a qualified health care provider for treatment purposes or disclosures required by law.

---

[1] 45 C.F.R. § 164.502(b).

RMN Policy 700: Workforce, Agents, and Contractors

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Use Limitation; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight; Remedies.

Purpose: These policies incorporate the HIPAA administrative requirements for workforce training, sanctions for privacy violations, and the reporting of complaints.[1] Because a Participant's workforce is responsible for implementation of privacy practices, proper training is vital to ensure the legitimate use of health information and the prompt identification, reporting, and correction of any security vulnerability or privacy spill. Individual accountability in the form of sanctions for those persons responsible for privacy violations is fundamental to encouraging compliance with privacy practices. Without such incentive for compliance, privacy violations and security risks may go unchecked and lead to larger privacy problems. Similarly, providing for the reporting of non-compliance enables Participants to discover and correct privacy violations and identify and sanction privacy violators. These policies helps guarantee the legitimate use of health data, the proper implementation of Participants' privacy practices, and the prompt identification of and undertaking of remedial action for privacy violations.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE, and that may provide, make available, or request health information through the HIE.

Policies

701. Participant Access to Redwood MedNet Services. -- *modified January 28, 2010*

702. Participant Training for Use of Redwood MedNet Services. -- *modified January 28, 2010*

703. Participant Discipline for Non-Compliance. -- *modified January 28, 2010*

704. Participant Reporting of Non-Compliance. -- *modified January 28, 2010*

705. Suspended Access for Persistent Non-Compliance. -- *modified January 28, 2010*

Policy 701: Participant Access to Redwood MedNet Services

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

701. Each Participant shall allow access to the HIE only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the HIE and/or release or obtain information through the HIE. No workforce member, agent, or contractor shall be provided with access to the HIE without first having been trained on these Policies.

Policy 702: Participant Training for Use of Redwood MedNet Services

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

702. Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the HIE to ensure compliance with these Policies.[2] The training shall include a detailed review of applicable Redwood MedNet Policies and each trained workforce member, agent, and contractor shall sign a representation that he or she received, read, and understands these Policies.

Policy 703: Participant Discipline for Non-Compliance

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

703. Each Participant shall implement clearly defined procedures to discipline and hold workforce members, agents, and contractors accountable to ensure that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with these Policies.[3] Such discipline measures shall include, but not be limited to, verbal and written warnings, and shall provide for retraining where appropriate.

Policy 704: Participant Reporting of Non-Compliance

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

704. Each Participant shall have a mechanism for, and shall encourage, all workforce members, agents, and contractors to report any non-compliance with these Policies to the Participant.[4] Each Participant also shall establish a process for individuals whose health information is included in the RLS to report any non-compliance with these Policies or concerns about improper disclosures of information about them.

Policy 705: Suspended Access for Persistent Non-Compliance

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

705. Each Participant shall be subject to denial of access to the RLS and the HIE if repeated efforts to train and discipline all workforce members, agents and contractors of that Participant result in persistent non-compliance with these policies.

[1] 45 C.F.R. § 164.530.

[2] 45 C.F.R. § 164.530(b).

[3] 45 C.F.R. § 164.530(e).

[4] 45 C.F.R. § 164.530(a), (d).

Category 800: Amendment of Data

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Openness and Transparency; Individual Participation and Control; Data Integrity and Quality; Accountability and Oversight.

Purpose: These policies integrate the right granted to Individuals by the HIPAA Privacy Rule to amend health information about them under certain circumstances.[1] Accurate health information not only is indispensable to the delivery of health care, but is important to individuals' applications for insurance and employment and in a variety of other arenas. Allowing individuals to verify the accuracy and completeness of information concerning them contributes to the transparency of Participants' operations and fosters confidence in Participants' privacy practices and commitment to data accuracy. These policies will enable Participants to more readily rely upon the integrity and quality of their health care data and more easily monitor, account for, and remedy systemic data inaccuracies, corruption, and other data deficiencies or privacy lapses.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE, and that may provide, make available, or request health information through the HIE.

Policies

801. Amendment of Individual Data. -- *modified January 28, 2010*

Policy 801: Amendment of Individual Data

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

801. Each Participant shall comply with applicable federal, state and local laws and regulations regarding individual rights to request amendment of health information.[2] If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant shall make reasonable efforts to inform other Participants that accessed or received such information through the HIE, within a reasonable time, if the recipient institution may have relied or could foreseeably rely on the information to the detriment of the individual.

---

[1] 45 C.F.R. § 164.526.

[2] 45 C.F.R. § 164.526.

Category 900: Requests for Restrictions

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Use Limitation; Individual Participation and Control; Accountability and Oversight.

Purpose: These policies require Participants who agree to individual requests for restrictions in accordance with the HIPAA Privacy Rule to comply with such requests with regard to the release of information from the HIE.[1] Such compliance ensures permissible use of health information and accountability on the part of Participants who agree to individually requested use restrictions. Without the ability to request restrictions and without assurance that Participants will honor these agreed-upon restrictions, Individuals may remain silent about important information that could affect their health. By creating confidence in Participants and their privacy protections and encouraging individual participation, these policies foster dialog between individuals and Participants, thereby reinforcing traditional standards of confidentiality between a patient and their health care provider. Effective communication between a provider and a patient improves the overall delivery of health care.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE, and that may provide or make available health information through the HIE.

Policies

901. Individual Requests for Restrictions. -- *modified January 28, 2010*

Policy 901: Individual Requests for Restrictions

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

901. If a Participant agrees to an Individual's request for restrictions,[2] as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions when releasing information through the HIE. If an agreed-upon restriction will or could affect the requesting institution's uses and/or disclosures of health information, at the time of disclosure, the Participant disclosing such health information shall notify the requesting institution of the fact that certain information has been restricted, without disclosing the content of any such restriction.

---

[1] 45 C.F.R. § 164.522.

[2] Under the HIPAA Privacy Rule, individuals have the right to request restrictions on the use and/or disclosure of health information about them. 45 C.F.R. § 164.522. For example, an individual could request that information not be used or disclosed for a particular purpose or that certain information not be disclosed to a particular individual. Covered entities are not required to agree to such requests under HIPAA. the individual of the disclosure of information about them or Participant request to the party who received such information to return and/or destroy the impermissibly disclosed information.

Category 1000: Mitigation

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

Principles: Openness and Transparency; Data Integrity and Quality; Security Safeguards and Controls; Accountability and Oversight; Remedies.

Purpose: These policies incorporate the HIPAA requirement that entities have procedures and take steps to mitigate harm resulting from an impermissible use or disclosure of health information.[1] Without the duty to mitigate harm from privacy violations, Participants may not promptly address data security weaknesses or breaches which could lead to greater privacy lapses in the future, diminish the confidence that Individuals have in Participants' privacy practices, and compromise the accuracy, integrity, and quality of Participants' data. Remedial action and mitigation are essential both to reassure individuals that Participants are vigilant in addressing privacy violations and ameliorating any harm from such violations and to help Participants ensure that their data oversight practices and security measures are functioning and effective.

Scope: These policies apply to all entities that are participating in the Redwood MedNet HIE, and that may provide, make available, or request health information through the HIE.

Policies

1001. Appropriate Remedial Action. -- *modified January 28, 2010*

1002. Breach Notification. -- *approved February 25, 2010*

Policy 1001: Appropriate Remedial Action

Version: 20100128.i *Adopted: November 8, 2007* *Modified: January 28, 2010*

1001. Each Participant shall recognize, mitigate and take appropriate remedial action, to the extent practicable, in response to any harmful effect that is known to the institution of a use or disclosure of health information through the Redwood MedNet HIE in violation of applicable laws and/or regulations and/or these Redwood MedNet Policies by the institution, or its workforce members, agents, and contractors. Steps to mitigate could include, among other things, Participant notification to the Individual of the disclosure of information about them or Participant request to the party who received such information to return and/or destroy the impermissibly disclosed information.

Policy 1002: Public Breach Notification

Version: 20100225.j *Approved: February 25, 2010*

1002. Breaches of unsecured health information trigger the notification requirement. Notice must be afforded no later than 60 days after the discovery of the breach. A breach is considered to be "discovered" when at least one employee of the Participant (other than the person responsible for the breach) knows, or reasonably should know, about the breach. Notice is required to be provided to media outlets if the information of more than 500 individuals is involved. Notice of all breaches must also be provided to the Secretary of the U.S. Department of Health and Human Services. This notice must be immediate of the breach involves the information of more than 500 individuals. These breach provisions do not expressly preempt any applicable State breach notification laws or regulations.

---

[1] 45 C.F.R. § 164.530(f).