

ROCHESTER



RHIO

Regional Health Information Organization

Privacy Policies  
& Procedures

**Rrho Privacy Policies and Procedures**  
**Version 1.0 September 20, 2007**

*The policies as outlined in this document are based on the Connecting For Health Common Framework as developed by the Markle foundation and the Connecting For Health Policy Subcommittee, whose contributors are listed in appendix A. Subsequent review, modifications and additions were conducted and developed by the Greater Rochester Regional Health Information Organization (Rrhio) Privacy Work Group.*

*Version 1.0  
September 20, 2007*

### ***Guiding Principles***

*The following nine principles inform much of the efforts of the Rhio to craft a set of policies to promote consumer control of their own health information while considering the operational needs of a health information exchange to provide value to the greater community.*

#### **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 use must be limited to the amount necessary to accomplish specified purposes. Minimization of use will help reduce privacy violations, which can easily occur when data is collected for one legitimate reason and then reused for different or unauthorized purposes.

**3. Collection Limitation.** Personal health data should be obtained only

by fair and lawful means, and, if applicable, with the knowledge or consent of the pertinent individual or their legal representative. In an electronic networked environment, it is particularly important for individuals to understand how information concerning them is being collected.

**4. Use Limitation.** The use and disclosure of health information should be limited to those purposes specified by the data recipient. Certain exceptions 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 any 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 prevent 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, another tools can 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.

**10. Applicability:** The following Policies apply to all Participants that have registered with and are participating in the Rrhio, the Record Locator Service (RLS), the Virtual Health Record (VHR) and that may provide or make available health information through Rrhio and the VHR.

### **Rrhio Policy 100: Compliance with Law and Policy**

**Scope:** This Policy stipulates compliance with all applicable laws and Rrhio policies, while requiring Participants to establish efforts to comply with Rrhio policies and laws.

#### **Policy:**

1. **Laws.** 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 compliance.

2. **Rrhio Policies.** Each Participant shall, at all times, comply with all applicable Rrhio policies and procedures (“Rrhio Policies”). These Rrhio Policies may be revised and updated from time to time upon reasonable written notice to Participant. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Rrhio Policies.
3. **Participant Policies.** Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and these Rrhio Policies. In the event of a conflict between these Rrhio 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.

**Rrhio Policy 200:**  
**Notice of Privacy Practices**

**Scope:** This Policy relates to the maintenance of privacy notices.

**Policy:**

Each Participant shall develop and maintain a notice of privacy practices (the “Notice”) that complies with applicable law and this Policy.

1. **Content.** The Notice shall meet the content requirements set forth under the HIPAA Privacy Rule and comply with all applicable laws and regulations.
2. **Provision to Individuals.** Each Participant shall have its own policies and procedures governing distribution of the Notice to individuals, which 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: (1) available to the public upon request; (2) posted on all web sites of the Participant and available electronically through such sites; (3) provided to a patient at the date of first service delivery; (4) available at the institution; and (5) posted in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read the Notice.
  - For Participants that are health plans, the Notice shall be: (1) available to the public upon request; (2) provided to new enrollees at the time of

plan enrollment; (3) provided to current plan enrollees within 60 days of a material revision; and (4) 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.

**3. Individual Acknowledgement.**

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

**4. Participant Choice.** Participants may choose to supplement the notice distribution process which is described herein.

**Rrhio Policy 300: Individual Participation and Control of Information in the Community Virtual Health Record (VHR)**

**Scope:** This Policy addresses an individual's choice to participate in Rrhio and Participants efforts to support such decisions.

**Policy:**

1. **Granting Consent.** All individuals must specifically consent to have clinical information about them made available through the VHR.
2. **Effect of Choice.** An individual's choice to have information about him or her made available through the VHR shall be exercised through the Rrhio or Participant as described in the Rochester RHIO patient consent form. If an individual has explicitly chosen not to participate, that individual's clinical results will not be made available through the VHR. Rrhio shall implement appropriate mechanisms to securely prevent access to clinical information about an individual if the individual does not choose to have such information included in the VHR.
3. **Revocation.** An individual, who has chosen to make information concerning him or her available through the VHR, subsequently may be excluded from the VHR only if the individual specifically revokes his or her decision. For patients who have elected not to share their clinical results through the VHR, only first name, last name, gender, date of birth and their consent status will be

displayed if data is entered by a user and an exact match is found.

4. **Reinstatement.** An individual who has chosen not to make their clinical results available through the VHR may be included in the VHR only if they subsequently provide specific consent for such access to be granted.
5. **Documentation.** Each Participant shall document and maintain documentation of all patients' decisions to consent to have information about them included in the VHR using the Rrhio's consistent and standard patient consent form.
6. **Participant's Role.** Participants shall establish reasonable and appropriate processes to enable the exercise of a patient's choice not to have information about him or her included in the VHR. Each Participant retains the authority to decide whether and when to make information available through the VHR consistent with Rrhio policies and the Data Sharing Agreement signed between the Participant and the Rochester RHIO.
7. **Provision of Coverage or Care.** Participants shall provide care or coverage to an individual regardless of the individual's decision to make their information available through the VHR.

8. **Complaint.** All individuals, regardless of their consent status, may file a written complaint to Rrhio at any time. A formal complaint must include a detailed explanation of the individual's concern as well as detailed contact information. Contact information should include: name, address and phone number as well as the individual's preferred method for the Rrhio to contact them. All formal complaints should be sent to:

*Rochester RHIO  
Support Services  
150 State St.  
Rochester, NY 14614*

#### **Rrhio Policy 400: Uses and Disclosures of Health Information**

**Scope:** This Policy addresses issues of use limitation, purpose specification, minimization, accountability and oversight, while integrating general HIPAA frameworks for privacy.

#### **Policy:**

1. **Compliance with Law.** All disclosures of health information through the Rrhio and the use of information obtained from the Rrhio 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.

2. **Purposes.** A Participant may request health information through the RLS or Rrhio only for purposes permitted by applicable law. Each Participant shall provide or request health information through the RLS or Rrhio only to the extent necessary and only for those purposes that are permitted by applicable federal, state, and local laws and regulations and these Policies. In some cases information may not be requested without additional specific patient authorization e.g. Fundraising, Marketing, Research. 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 Rrhio.
3. **Rrhio Policies.** Uses and disclosures of and requests for health information via the Rrhio shall comply with all Rrhio Policies, including, but not

limited to, the Rrhio Policy on Minimum Necessary and the Rrhio Policy on Information Subject to Special Protection.

4. **Participant Policies.** 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 documentation that shall be obtained, if any, prior to making such disclosures.
5. **Accounting of Disclosures.** An individual has the right to request an accounting of disclosures as defined by the HIPAA privacy rule. Each Participant is responsible for ensuring its compliance with such requirement 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 HIPAA Privacy Rule's accounting of disclosures requirement.
6. **Audit Logs.** The Rrhio shall maintain an audit log documenting which Participants posted and accessed the information about an individual through the VHR and when such information was posted and accessed. Rrhio will provide an audit reporting mechanism for participants, detailing access requests for information

exchange facilitated by the Rrhio's RLS services. Participants and Rrhio shall consider and work towards implementing a system wherein, upon request, patients have a means of seeing who has posted and who has accessed information about them through the VHR and when such information was accessed.

**7. Access.** Rrhio should have a formal process through which clinical information in the VHR can be requested by a patient or other authorized personal representative on a patient's behalf. Participants and Rrhio shall consider and work towards providing patients direct access to the information contained in the VHR that is about them.

**Rrhio Policy 500: Information Subject to Special Protection**

**Scope and Applicability:** This Policy facilitates individualized privacy protections by requiring Participants to heed any special protections of certain information set forth under applicable law.

**Policy:**

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

information through the Rrhio. Each Participant is responsible for complying with such laws and regulations.

**Rrhio Policy 600: Minimum Necessary**

**Scope and Applicability:** This Policy incorporates the HIPAA privacy rule requirements that entities may disclose only the amount of information reasonably necessary to achieve a particular purpose.

**Policy:**

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

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

**Rrhio Policy 700: Workforce, Agents, and Contractors**

**Scope and Applicability:** This Policy helps guarantee the legitimate use of health data, the proper implementation of Participant's privacy practices and the prompt identification of and undertaking of remedial action for privacy violations.

**Policy:**

1. **Access to System.** Each Participant shall allow access to the Rrhio with unique log on IDs only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the Rrhio and/or release or obtain information through Rrhio. No workforce member, agent, or contractor shall be granted access to Rrhio without first having been trained on these Policies and signed the representation described below.
2. **Authentication.** Each Participant shall follow uniform minimum authentication requirements as per the Rrhio Data Sharing Agreement for verifying and authenticating those within their institutions who shall have access to, as well as other Participants who request access to, information through the Rrhio and/or the RLS.
3. **Training.** Training shall include, at a minimum, a web based training tool provided by Rrhio with a review of applicable Policies. Each Participant shall develop and implement a training program for its workforce members, agents, and contractors who will have access to the Rrhio to ensure compliance with these Policies. Each trained workforce member, agent, and contractor shall complete a representation that he or she received, read, and understands these Policies and has completed appropriate training.
4. **Discipline for Non-Compliance.** Each Participant shall implement procedures to discipline and hold workforce members, agents, and contractors accountable for ensuring that they do not use, disclose, or request health information except as permitted by these Policies and that they comply with, but are not limited to these Policies. Such discipline measures may include, but not be limited to, verbal or written warnings, demotion, or termination and provide for retraining where appropriate. The gRrhio reserves the right to terminate individual user access

based on non-compliance with stated policies.

5. **Reporting of Non-Compliance.** Each Participant shall have a mechanism for reporting any noncompliance with these policies, and shall encourage, all workforce members, agents, and contractors to report any noncompliance with these Policies to the Participant. 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. Participants should notify Rhio regarding instances of significant non-compliance that lead to disciplinary action.

#### **Rhio Policy 800: Amendment Of Data**

**Scope and Applicability:** This policy integrates the rights granted by HIPAA Privacy Rule of individuals to request access of an amendment for health information about them under certain circumstances.

**Policy:**

The Participant shall make reasonable efforts to inform other Participants that accessed or received such information through the Rhio if the recipient institution may have relied on or could foreseeably rely on the information to the detriment of the individual. The Rhio does not have the ability

to make amendments but can assist participants in determining who may have reviewed the results through the HIE.

#### **Rhio Policy 900: Requests For Restrictions**

**Scope and Applicability:** This policy requires 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 to Rhio.

**Policy:**

If a Participant agrees to implement an individual's request for restrictions, as permitted under the HIPAA Privacy Rule, such Participant shall ensure that it complies with the restrictions when releasing information through the Rhio.

#### **Rhio Policy 1000: Mitigation**

**Scope and Applicability:** This Policy applies to all institutions that have registered with and are participating in the Rhio and that may provide, make available, or request health information through the Rhio.

**Policy:**

Participants and the Rhio shall collaborate to mitigate and take appropriate remedial action, to the extent practicable, of any known harmful effect that is known to the institution of a use or disclosure of health information through the Rhio in violation of applicable laws and/or regulations and/or these 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.

# Glossary

**MPI.....Master Patient Index:** A way to identify patients.

**HIE.....Health Information Exchange:** A system to exchange health care information between institutions and health care providers.

**Participant.....**A healthcare provider or institution, participating in and bound by the terms of the RHIO data sharing agreement.

**RLS.....Record Locator Service:** A system to find clinical results for a given patient across institutions.

**VHR.....Virtual Health Record:** A summarized view of patient health care information as it has been provided across institutions. These clinical results are made available only as Participants make them available to the HIE.

# Appendix A

## Acknowledgements

### Greater Rochester Regional Health Information Organization Privacy Work Group

**Patricia A. Beato**, RHIT, CHP  
*Privacy Officer*, University of Rochester Medical Center

**Ted Kremer**, MPH  
*Executive Director*, Greater Rochester Regional Health information Organization

**Lisa M. Santelli**, Esq.  
*Legal Counsel*, Excellus

**Aileen Shinaman**, Esq.  
*Attorney*, University of Rochester Medical Center

**Toni Teumer**, RHIA, CHP  
*Privacy Officer*, Unity Health Systems

**Cindy Bileschi**, RN, BSN  
Director for Regulatory Affairs, Rochester General Hospital, Privacy Officer, Via Health

### The Markle Foundation Connecting for Health Policy Subcommittee

**William Braithwaite**, MD, eHealth  
Initiative, (Co-Chair)

**Mark Frisse**, MD, MBA, MSc, Vanderbilt  
Center for Better Health, (Co-Chair)

**Laura Adams**, Rhode Island Quality  
Institute

**Phyllis Borzi**, JD, George Washington  
University Medical Center

**Susan Christensen\***, JD, Agency for  
Healthcare Research and Quality,  
United States Department of Health and  
Human Services

**Art Davidson**, MD, MSHP, Denver

Public Health

**Mary Jo Deering\***, PhD, National Cancer  
Institute/National Institutes of Health,  
United States Department of Health and  
Human Services

**Jim Dempsey**, JD, Center for Democracy  
and Technology

**Hank Fanberg**, Christus Health

**Linda Fischetti\***, RN, MS, Veterans Health  
Administration

**Seth Foldy**, MD, City of Milwaukee  
Health Department

**Janlori Goldman**, JD, Columbia College of Physicians and Surgeons

**Ken Goodman**, PhD, University of Miami

**John Halamka**, MD, CareGroup Healthcare System

**Joseph Heyman**, MD, American Medical Association

**Gerry Hinkley**, JD, Davis, Wright, Tremaine LLP

**Charles Jaffe**, MD, PhD, Intel Corporation

**Jim Keese**, Eastman Kodak Company

**Linda Kloss**, RHIA, CAE, American Health Information Management Association

**Gil Kuperman**, MD, PhD, New York-Presbyterian Hospital

**Ned McCulloch**, JD, IBM Corporation

**Patrick McMahon**, Microsoft Corporation

**Omid Moghadam**, Intel Corporation

**Joyce Niland**, PhD, City of Hope National Medical Center

**Louise Novotny**, Communication Workers of America

**Michele O'Connor**, MPA, RHIA, MPI Services Initiate

**Victoria Prescott**, JD, Regenstrief Institute for Healthcare

**Marc A. Rodwin**, JD, PhD, Suffolk University Law School

**Kristen B. Rosati**, JD, Coppersmith Gordon Schermer Owens & Nelson PLC

**Sara Rosenbaum**, JD, George Washington University Medical Center

**David A. Ross**, ScD, Public Health Informatics Institute

**Clay Shirky**, New York University (Chair, Technical Subcommittee)

**Don Simborg**, MD, American Medical Informatics Association

**Michael Skinner**, Santa Barbara Care Data Exchange

**Joel Slackman**, BlueCross/BlueShield Association

**Peter P. Swire**, JD, Moritz College of Law, Ohio State University

**Paul Tang**, MD, Palo Alto Medical Foundation

**Micky Tripathi**, Massachusetts eHealth Collaborative

**Cynthia Wark\***, CAPT, United States Public Health Service Commissioned Corps, Centers for Medicare and Medicaid Services, United States Department of Health and Human Services

**John C. Wiesendanger**, MHS, West Virginia Medical Institute/Quality Insights of Delaware/Quality Insights of Pennsylvania

**Marcy Wilder**, JD, Hogan & Hartson LLP

**Scott Williams**, MD, MPH, HealthInsight

**Robert B. Williams**, MD, MIS, Deloitte

**Joy Wilson**, National Conference of State Legislatures

**Rochelle Woolley**, RxHub

**Amy Zimmerman-Levitan**, MPH, Rhode Island State Department of Health