Policy Revisions Log

Date	Section #	Amended	Requested by:	Approved by:
11/17/11	9.1.3.4	Added section to require password changes should Hoag implemented such a policy	Dr. Margarita Pereyda	Kieran Murphy
11/17/11	4.4	Removed restriction for a user to query their own information	Dr. Francis Rhie	Kieran Murphy & Michelle Kikuchi
12/5/11	4.4	Added the following language, "unless the provider has a clinical relationship with the person and has a need-to-know in accordance with HIPAA."	Drs. Bart Barrett & Dennis Jordanides	Kieran Murphy

Hoag Memorial Hospital Presbyterian

Hoag-Enabled Health Information Exchange Privacy Policy

1.0 Purpose

1.1 This Hoag-Enabled Health Information Exchange ("HIE") policy on patient privacy considers patients' rights and expectations while balancing the need for health care providers to have information that enables them to make informed decisions and ultimately provide better quality health care services.

1.2 In order to maintain an appropriate level of security and to protect patient data from unauthorized access and disclosure, this policy defines the access controls and parameters necessary to achieve this protection and to ensure reliable operation of the HIE.

2.0 Definitions

2.1 "Health information" means any individually identifiable information, in electronic or physical form regarding a patient's medical history, mental or physical condition, or treatment.

2.2 "Individually identifiable" means that the information includes an element or elements relating to an individual such that, when taken alone or in combination with other publicly available information, it becomes sufficient to allow identification of the individual.

2.3 "Access Controls" means the system-level security that grants or denies authorization to view personal health information in the HIE.

2.4 "Auditing" means the logging and monitoring of all system activity, including: User log-in identification; User name; User organization; date and time; patient account that was accessed; and type of records viewed by User.

2.5 "Health Care Provider" means a health professional licensed in California with the authority to order or prescribe clinical tests and diagnostics, including physicians as defined by Title 18, Section 1861(r) of the Social Security Act, and clinical medical professionals who are licensed to diagnose and treat patients under the supervision of such licensed professionals.

2.6 "Data Sending Organizations" means those health care facilities that make clinical data (e.g. lab results) available to health care providers/clinicians through the HIE

2.7 "Users" means those who enroll in the HIE to receive clinical results and reports. HIE Users are clinicians and their designated staff, who must agree to maintain the privacy and security of the information they obtain from the HIE. HIE Users receive clinical results and reports and, when available, may also query the HIE for clinical history.

2.8 "User Roles" means the rules defined by the HIE and assigned to Users, which establish the parameters on an individuals' level of access to personal health information through the HIE.

2.9 "User Authentication" means the system's verification process to ensure the User is properly identified and/or credentialed to gain authorized access to the HIE application.

2.10 "Query" means a system search for clinical information about a patient by an authorized User who has an established relationship with that patient conducted via the HIE on a need-to-know basis.

2.11 "Expanded Query Access" means the ability of a User to temporarily extend their access rights under defined parameters, allowing the User to view more broadly clinical information available through the HIE on a need-to-know basis for a limited, expressly defined period of time.

2.12 "Need-to-Know" means the basic standard or threshold of justification required of a User in order for that User to view patient information in the HIE. In order to safeguard patient/consumer privacy, the HIE Users shall receive access only to the minimum functions and privileges required for performing their jobs.

3.0 Policy

3.1 This policy is applicable to all Users and member organizations of the HIE. All Users of the HIE, both senders and receivers of data, have signed the appropriate legal agreements to ensure the privacy and security of data in the HIE, in compliance with state and federal law.

3.2 This policy does not supersede or replace any Health Insurance Portability and Accountability Act (HIPAA) requirements or state-required privacy and security policies in use by individual HIE Users and member organizations.

3.3 Patient/consumer privacy is of critical importance. California law (i) authorizes the state to assess fines and penalties against health facilities and individuals for privacy breaches of patient health information, and (ii) requires health facilities to report privacy breaches to the California Department of Public Health ("CDPH") and to the affected patient(s) within five (5) days from the date the breach was discovered.

4.0 Restrictions on the Use and Disclosure of Individually Identifiable Health Information

4.1 Disclosure of Individually Identifiable Health Information. Patient information in the HIE shall not be sold or disclosed to any third party for any commercial or unauthorized activity.

4.2 Query Access. Only Users enrolled in the HIE who have an established relationship with a patient will have access to that patient's information available through the HIE. Emergency care personnel will have access to the HIE whereby they can access patient records in emergency care situations on a need-to-know basis.

4.3 Expanded Query Access. Users may expand their access to patient information by requesting to establish a relationship with a patient in the HIE. Users are required to log a reason for the relationship and set a defined time period for access, not to exceed six (6) months.

4.4 Special Restrictions. HIE Users shall not access health information in the HIE on an immediate family member, relative, friend and/or co-worker, unless the provider has a clinical relationship with the person and has a need-to-know in accordance with HIPAA.

4.5 Audit Reporting. Patients/consumers are provided the means and opportunity to request an audit report that identifies the HIE User(s) who have accessed the patient/consumer's personal individually identifiable health information through the HIE. Audit reports will

not contain any personal health information. Specific procedures shall be established to respond to requests for audit reports.

4.6 Compliance with Law. Users who violate patient privacy are subject to consequences ranging from immediate termination of access to the HIE up to and including legal action in accordance with this HIE Privacy Policy and with all applicable federal and state laws and regulations.

5.0 Patient/Consumer Notification

5.1 Data Sending Organizations shall implement appropriate procedures to inform their patients (1) that they use the HIE to exchange their patients' information with other HIE Users, and (2) of their patients' right to opt out from having medical information about them made available for query by authorized Users of the HIE. Options for obtaining patients' acknowledgement of their rights to be excluded from the HIE may include, among other things: 1) an update to the organization's Notice of Privacy Practices in combination with patient's acknowledgment of having received notice of such filed in the patient's chart; 2) a signed form specifically notifying the patient of the exchange of their medical data in the HIE and attesting to the patient's consent to such; or 3) electronic consent (i.e., patient checks a box that acknowledges consent for data exchange) via the organization's patient web portal.

5.2 Hoag shall make available to Users tools necessary to respond to patient inquiries about the HIE (e.g., brochures, answers to frequently asked questions, talking points, and forms for opting out).

6.0 Patient/Consumer Opt Out

6.1 Patients/consumers may decide not to participate in the HIE or "opt out" by submitting an Opt-Out Request Form.

6.2 If a patient ops out, that patient's personally identifiable health information will not be available to Users (including emergency personnel) upon a query or expanded query of patient data in the HIE.

6.3 Patients/consumers who have opted out may choose to participate in the HIE again at any time by submitting a Cancellation of Opt-Out Form.

6.4 The HIE will implement specific procedures to process opt-out requests, as well as requests to cancel a previous opt-out.

6.5 The HIE shall respond to a patient's request to opt out, and to cancel a previous opt-out request, in a timely manner and according to the procedures that are established.

7.0 Amendment of Data

7.1 Responsible Party: Once patient data has been provided to the HIE, any change to that data based upon patient/consumer request to amend such data can only be made by the Data Sending Organization that originally contributed the data to the HIE. The HIE does not have the authority or access to amend individually identifiable health information.

8.0 Breach Notification

8.1 Applicable Law: Unauthorized access is defined as "the inappropriate review or viewing of patient medical information without a direct need for diagnosis, treatment, or other lawful use as permitted by the Confidentiality of Medical Information Act ("CMIA") (Part 2.6 (commencing with Section 56) of Division 1 of the California Civil Code) or by other statutes or regulations governing the lawful access, use, or disclosure of medical information."

8.1.1 If a User (or a business associate of User under HIPAA) discovers that a privacy breach of patient medical information has occurred, the privacy breach must be reported immediately to the Director of Health Information Exchange at Hoag Memorial Hospital Presbyterian.

8.1.2 Upon receipt of any such report, the Director of HIE shall, in conjunction with other necessary and appropriate parties, investigate the incident and follow-up appropriately (e.g., notifying the patient and CDPH).

9.0 Access Controls

9.1 Access rights and parameters are granted to HIE Users based on the following factors:

9.1.1 User Authentication. Any User accessing the HIE must be authenticated. The level of authentication will correspond appropriately to the designated access rights.

9.1.2 User roles and job responsibilities. The health care provider enrolled in the HIE is responsible for assigning User roles to those who work in the provider's organization. Users should be granted access to information on a need-to-know basis; that is, Users should only receive access to the minimum functions and privileges required for performing their jobs.

9.1.3 Unique User identification. Each User is assigned a unique identifier that ensures individual accountability and enables tracking.

9.1.3.1 The User is held responsible for all actions conducted under his/her log-in credentials.

9.1.3.2 Under no circumstances should a User's log-in credentials be shared.

9.1.3.3 If a password is suspected of being disclosed to an unauthorized party, it must be promptly changed.

9.1.3.4 All users will be required and prompted to change their passwords at a time interval defined by the Hoag-enabled HIE and consistent with HIPAA.

9.1.3.5 At the time a User is no longer associated with or employed by a member organization, the member organization is required to immediately terminate the User's access to the HIE.

9.1.3.6 The HIE will routinely audit User accounts for activity and disable those that have been inactive for 180 or more days.

10.0 Audit Controls

10.1 The HIE logs and monitors all system activity and Expanded Query Access, including: User log-in identification; User name; User organization; date and time; patient account that was accessed; the reason the User utilized expanded query; time period for which access was established; and the type of records viewed by User.

10.2 The HIE shall monitor/audit access to individually identifiable health information on a regular and scheduled basis to ensure appropriate use of the system. Procedures shall be established to define this process.

10.3 Access to the HIE for Users determined to be a risk to security will be suspended, terminated and/or flagged for enhanced security review commensurate with the potential risk.

10.4 Patients/consumers are provided the means and opportunity to request an audit report of who has accessed their health information through the HIE, including utilization of expanded query. Audit reports do not contain personal health information. The HIE shall establish specific procedures to respond to patient requests for audit reports in a timely manner.

10.5 As part of the HIE User security audit, staff identify Users that potentially "misused" the HIE by accessing individually identifiable health information without meeting the need-to-know standard.

10.6 Follow-up/Legal Action. Upon a determination than an authorized User has not complied with this Privacy Policy, the User's access authority may be suspended, limited or revoked if doing so is necessary for the privacy of individuals or the security of the HIE.

11.0 Penalties for Inappropriately Accessing Personally Identifiable Health Information

11.1 California law gives the California Department of Public Health the authority to assess fines on health care entities and individuals who misuse, or fail to protect from misuse, patient health information.

11.2 Individual(s) responsible for a breach, including inappropriate review or viewing of patient information without a direct need for diagnosis, treatment, or other lawful use will be subject to fines and penalties.

11.3 Health care entities are subject to fines and penalties for administrative violations resulting in a breach, including failing to protect patient information from inappropriate access and use.

11.4 Patients have a private right of action to seek damages as a result of privacy/security incidents.