

Governor's Office of Electronic Health Information Policies

INTRODUCTION

The following policies apply to the access, use and disclosure of protected health information by Participants of the Kentucky Health Information Exchange (KHIE). These are the initial policies adopted by the Governor's Office of Electronic Health Information (GOEHI) according to the following language found in the initial Participation Agreement adopted and signed by the pilot participants in the KHIE on or about April 1, 2010.

GOEHI will establish policies and standards (respectively, "Policies and Standards") that are consistent with the Agreement and will govern GOEHI's and Participant's use of the Exchange. It is the intention of the Parties that the development of the Policies and Standards will be through the KHIE Coordinating Council and its committees. The six initial pilot Participants will be allowed to participate as members of such committees. GOEHI will make these Policies and Standards available to Participant through the website of the Cabinet for Health and Family Services. These Policies and Standards will govern the use, submission, transfer, access, privacy and security of Data. These Policies and Standards, however, shall not alter the relative rights and obligations of the Parties under the Agreement.

The KHIE Coordinating Council was established by Administrative Order CHFS 2010-02 dated February 23, 2010. There are 23 members of the Coordinating Council and additional members serving on the six Coordinating Council Committees. The Council and Committees represent a broad range of stakeholder interests that include health care providers, Regional Health Information Organizations (RHIOs), health plans, patient or consumer organizations, health information technology vendors, public health agencies, universities and colleges, clinical researchers and other users of health information technology, including health practice managers and care coordinators.

According to the Participation Agreement, GOEHI may change or amend the Policies in a manner consistent with the Participation Agreement. The Participant shall be given notice of any proposed and final changes and

GOVERNOR'S OFFICE OF ELECTRONIC HEALTH INFORMATION

Participants shall be given an opportunity to comment on such proposed and final changes. Any change to a policy is effective thirty days after the change unless an earlier effective date is required to address a legal requirement, a concern relating to privacy or security of Data, or an emergency. GOEHI may also postpone the effective date of a policy, if additional implementation time is needed.

GOEHI believes the nine principles defined in “The Architecture for Privacy in a Networked Health Information Environment”¹ are essential for protecting privacy and developing a comprehensive privacy-protective architecture in a networked environment. The principles are as follows:

1. Openness and Transparency
There should be a broad and universal practice of transparency in the way data is handled. Individuals should be able to establish what information exists about them in the data and in databases.
2. Purpose Specification and Minimization
Data should never be collected without the subject of the data knowing why it is being collected and how it will be used. Data should only be used for the purpose for which it was collected.
3. Collection Limitation
The collection of data should be obtained by lawful and fair means and with the knowledge and consent of persons.
4. Use Limitation
A minimization requirement would strictly limit whether data collected for one purpose could be reused in another context. Such use should not be permissible without the explicit consent of individuals.
5. Individual Participation and Control
Consistent with the scope of individual rights in HIPAA, an individual has a vital stake in, and needs to be, a participant in determining how his or her information is used. Individuals should be seen as key participants in the process of information collection and dissemination, and not as mere subjects or passive spectators.

¹ ©2006, Markle Foundation

This work was originally published as part of The **Connecting for Health** Common Framework: Resources for Implementing Private and Secure Health Information Exchange and is made available subject to the terms of a license (License) which may be viewed in its entirety at: <http://www.connectingforhealth.org/license.html>. You may make copies of this work; however, by copying or exercising any other rights to the work, you accept and agree to be bound by the terms of the License. All copies of this work must reproduce this copyright information and notice.

GOVERNOR'S OFFICE OF ELECTRONIC HEALTH INFORMATION

6. Data Integrity and Quality

Mechanisms need to be developed to address data corruption and for establishing accountability among those who maintain records. Individuals should have clear avenues to view all information that has been collected about them and to ensure that the information is accurate, complete and timely.

7. Security Safeguards and Controls

Reasonable security safeguards must be built against loss, unauthorized access, destruction, use, modification, or disclosure of personal information. In addition, all data collectors and disseminators should be mandated to immediately disclose any security breach through a direct communication to those consumers affected.

8. Accountability and Oversight

There must be mechanisms to ensure that the responsibility for privacy and privacy violations is identifiable and that remedial action can be taken.

9. Remedies

There should be legal and financial means to remedy any privacy or security breaches.²

These principles guide the GOEHI policies to the extent HIPAA, HITECH, state and federal laws allow. In some instances, current technology will not allow full implementation of the principles; however, these principles guide the policies.

The following terms are used in the policies:

Definitions

American Recovery and Reinvestment Act means the appropriations bill signed into law on February 17, 2009.

Authorized User means an individual authorized by a Participant under a GOEHI Participation Agreement to use the Kentucky Health Information Exchange to access or provide Data for a Permitted Use.

²These principles are based upon the Organization for Economic Co-operation and Development's (OECD) Guidelines for the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1.00.html#guidelines The mission of OECD is to promote policies that will improve the economic and social well-being of people around the world.

GOVERNOR'S OFFICE OF ELECTRONIC HEALTH INFORMATION

Business Associate shall have the definition assigned to Business Associate under HIPAA by 45 C.F.R. § 160.103.

Cabinet for Health and Family Services or CHFS means the program cabinet of the Commonwealth of Kentucky established by K.R.S. § 12.250.

Covered Entity shall have the definition assigned to Covered Entity under HIPAA by 45 C.F.R. § 160.103.

Data means patient health information provided to KHIE by a Participant.

Exchange means the Kentucky Health Information Exchange (KHIE), the health information exchange provided by GOEHI. The Exchange provides connection options for the capability to exchange key clinical information among Participants.

GOEHI means the Governor's Office of Electronic Health Information, an office created by Governor Steve Beshear by Executive Order 2009-770, eff. 8-14-09. The order provided that the Governor's Office of Electronic Health Information be created and be a part of the Cabinet for Health and Family Services in order to assist with electronic health technology, to improve patient care, reduce medical errors and make more efficient use of health care dollars by reducing redundant services. The Executive Order is found as a note to K.R.S. § 11.065.

Help Desk means the service provided to Participants by KHIE to assist with questions concerning the functions and operation of the exchange.

HITECH means the Health Information Technology for Economic and Clinical Health Act, enacted as part of the American Recovery and Reinvestment Act of 2009.

HIPAA means the Health Insurance Portability and Accountability Act of 1996.

IP address means internet protocol address.

KHIE Community Virtual Health Record means the web-based portal that allows an Authorized User to see a consolidated, tabular view of a patient's health information.

National Institute of Standards and Technology means the non-regulatory federal agency within the U.S. Department of Commerce.



GOVERNOR'S OFFICE OF ELECTRONIC HEALTH INFORMATION

Operations shall have the definition assigned to Health Care Operations under HIPAA as limited by 45 C.F.R. §164.506(c)(iv).

Participant means a Health Care Provider, as defined in 45 C.F.R. § 160.103, who is also a Covered Entity as defined by HIPAA, or the Kentucky Department for Medicaid Services or the Kentucky State Laboratory, Division of Laboratory Services. The Participant must have entered into a GOEHI Participation Agreement and have not terminated the Participation Agreement.

Participation Agreement means the agreement between the Governor's Office of Electronic Health Information and Participants to contribute Data to the Kentucky Health Information Exchange.

Payment shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA regulations.

Permitted Use is defined in relationship to the use made by the type of Participant. Currently there are three types of participants providing data; health care providers, the Department of Medicaid Services and the Kentucky State Laboratory, Division of Laboratory Services. Permitted Use is defined as follows:

- (a) By Health Care Providers:
 - (i) For Treatment, Payment and/or Operations such that patient authorization is not required under HIPAA; and
 - (ii) To facilitate the implementation of "meaningful use" criteria as required under the American Recovery and Reinvestment Act of 2009 and its related federal regulations, as permitted by HIPAA; and
- (b) By the Department for Medicaid Services:
 - (i) For Treatment and Payment for Medicaid patients and/or Operations such that patient authorization is not required under HIPAA, limited to functions related to case management, care coordination, and quality improvement activities; and

GOVERNOR'S OFFICE OF ELECTRONIC HEALTH INFORMATION

- (ii) To facilitate the implementation of “meaningful use” criteria as required under the American Recovery and Reinvestment Act of 2009 and its related federal regulations, as permitted by HIPAA.

- (c) By the Kentucky State Laboratory, Division of Laboratory Services:
 - (i) For Treatment and Payment for patients and/or Operations such that patient authorization is not required under HIPAA, limited to functions related to case management, care coordination, and quality improvement activities for the Kentucky newborn screening program as authorized in KRS 214.155 and cited as the James William Lazzaro and Madison Leigh Heflin Newborn Screening Act; and

 - (ii) To facilitate the implementation of “meaningful use” criteria as required under the American Recovery and Reinvestment Act of 2009 and its related federal regulations, as permitted by HIPAA.

Privacy Rule means those provisions of 45 C.F.R. Part 160 and Subparts A and E of 45 C.F.R. Part 164 of the HIPAA regulations that regulate the privacy of individually identifiable health information.

Protected Health Information shall have the definition assigned to Protected Health Information in 45 C.F.R. § 160.103 of the HIPAA regulations.

Security Rule means those provisions of 45 C.F.R. Part 160 and Subparts A and C of Part 164 of the HIPAA regulations that regulate the security of individually identifiable health information.

Treatment shall have the meaning set forth at 45 C.F.R. § 164.501 of the HIPAA regulations.