Holyoke Medical Center

HMC HealthConnect

Health Information Exchange Policies and Standards

1. Purpose of the Health Information Exchange Policies and Standards

These Health Information Exchange (HMC HealthConnect) Policies and Standards define the policies for clinical data exchange via Holyoke Medical Center's (HMC) HealthConnect. The policies establish operating rules for HMC, as the provider of HMC HealthConnect services, and for HMC HealthConnect Participants, as users of HMC HealthConnect. The policies also provide the foundation for development of Implementation Guides which will define the specific requirements for exchanging clinical data via HealthConnect.

1.1. Guiding Principles

The following principles guide the development of all policies for community clinical data exchange.

- *Policies Based on Guiding Principles.* Policies are developed collaboratively based on adherence to underlying principles.
- *Openness and Transparency.* Policies are available for review by all stakeholders: patients, Health Care Providers and Suppliers. Stakeholders are welcome to comment on and propose changes to policies, procedures, and technologies.
- *Patients' Rights.* Patients are provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their health information.
- *Patient Access and Participation.* Patients may request and receive information about access to their own data, to the extent possible with available technologies. Participant should allow Patients to di*spute the accuracy or integrity of* their health information, request to have erroneous information corrected, or have a note made of the disputed data, if correction is not made.
- *Data Collection and Use Limitation.* Health data are collected, exchanged, and used only for the agreed upon and stated purpose. The purpose itself is narrowly suited to the need.
- *Privacy and Security Policy Compliance.* Policies comply with Federal laws and regulations, including HIPAA, and with other applicable laws governing electronic healthcare data exchange.
- *Coordinated Decentralization.* Policies are designed to allow local control and management by Participants to the extent practical, in order to allow flexibility and minimize centralized resources and costs.
- *Broad Adoptability.* Policies are designed for ease of use by Participants and for cost effectiveness, in order to facilitate broad adoption and to facilitate participation by organizations with varying access to resources. To the extent practical, policies are designed to permit reasonable adoption time frames by Participants.

- *Anticipation of Change.* To the extent practical, policies are designed to anticipate and prepare for potential changes in federal and state requirements and standards.

The following principles guide the adoption and use of technology policies.

- *Open Standards.* All policies adhere to accepted national and industry standards where available, are based on open standards, are not dependent on proprietary technologies, and are vendor-neutral to facilitate widespread adoption. Connectivity among Participants' systems is based on the public Internet.
- *Hybrid Data Architecture.* Policies are designed to promote a combination of a federated and centralized approach to give local control of data and local accessibility whenever possible.
- *Flexibility and Agility.* Following architectural best practices, policies for application software design are biased toward loosely coupled and coarse grained services and reusability without compromising performance.
- *No Rip and Replace.* Policies are designed to protect current technology investments of Participants to the extent possible through adoption of open standards.
- *Multiple Implementation Models.* Policies are designed to support multiple network architectures, varying from Participant and vendor-hosted connectivity, to centrally hosted services

1.2. Applicability and Scope

The policies in this document apply to the exchange of clinical data and the organizations, business processes, computer applications, and technology involved in the exchange of clinical data via HMC HealthConnect. Clinical data is understood to include data directly related to care provided to individuals and data used to manage the exchange of this data.

The policies in this document do not apply to the exchange of financial and administrative data between Participants or to HMC in its role as operator and facilitator of administrative and financial healthcare data exchange.

The following are more specific definitions of scope and applicability.

1.2.1. Organizations and Location

The organizations to which policies apply are:

- HMC, which is located in Holyoke, Massachusetts. Compliance by employees, agents, contractors, and other persons affiliated with HMC is the responsibility of HMC.

- HMC HealthConnect Participants. Participants include all organizations actively exchanging clinical data via HMC HealthConnect. These organizations may include payer, provider, quality, government, and other organizations. Participants are located mainly in Western Massachusetts. Participants may be located outside of Western Massachusetts as HMC grows the HMC HealthConnect. Compliance by employees, agents, contractors, and other persons affiliated with a Participant (sometimes called Authorized Users) is the responsibility of the Participant.

1.2.2. Data

Data to which the policies apply are:

- All clinical data transmitted in electronic form from one Participant to another using HealthConnect services.

- All clinical data stored by HMC in support of the transmission of data from one Participant to another.

1.2.3. Business Processes

Business processes to which the policies apply are:

- All business processes used by a Participant to send or receive data via HealthConnect.
- All business processes used by HMC to provide clinical data exchange services and infrastructure.

1.2.4. Applications and Technology

The computer applications and technology solutions to which the policies apply are:

- Applications and technology solutions owned and operated by a Participant or on behalf of a Participant which are used to send or receive data via HealthConnect.
- All applications and technology solutions owned or operated by HMC or on behalf of HMC are used to provide clinical data exchange services.

1.3. Effective Date

The policies outlined in this document are effective upon approval by HMC and may be changed at any time by HMC.

1.4. Responsibilities

The following are the policy-related responsibilities of Participants in the community clinical data exchange.

1.4.1. HMC

HMC is accountable for the operation of HMC HealthConnect, which may be carried out by HMC employees, agents, vendors, and subcontractors.

HMC responsibilities are to:

- Maintain the HMC HealthConnect Policies and Standards.
- Make the policies and standards available to requestors upon request.
- Work with Participants to identify new policies and policy changes required to operate HMC HealthConnect.
- Manage development of Participation Agreements with Participants and related changes as needed to align with current policies.
- Manage developments of Participation Agreements with other external partners and related changes as needed to align them with current policies.
- Provide consultative assistance to Participants in interpreting and implementing policies.
- Oversee compliance with the policies by HMC HealthConnect Participants.

1.4.2. Participants

Each Participant is accountable for the execution of its responsibilities, which may be carried out by the Participant organization itself and by its employees, agents, vendors, subcontractors, and affiliates.

Participant responsibilities are to:

- Work with HMC to identify new policies and policy changes required to operate HMC HealthConnect.
- Provide consultative assistance to HMC in the development of new policies and policy changes.
- Manage compliance with the policies as regards use of clinical data exchange services provided by HMC.

1.4.3. External Partners

Each external partner is accountable for the execution of its responsibilities, which may be carried out by the partner organization itself and by its employees, agents, vendors, subcontractor, and affiliates. External partner responsibilities are to comply with the provisions of participation agreements executed with HMC.

2. Policies for Clinical Data Exchange

2.1. Federal , State, and Local Laws

2.1.1. HMC

HMC shall comply with all federal, state, and local laws, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as they pertain to healthcare data exchanged via HMC HealthConnect.

2.1.2. Participant

Participants shall comply with all federal, state, and local laws, including HIPAA, as they pertain to healthcare data exchanged via HMC HealthConnect.

2.2. Participation Agreements

2.2.1. HMC

HMC shall execute a Participation Agreement in a form determined by HMC from time to time with each Participant and External Partners prior to beginning live exchange of data. Such a participation agreement shall establish the mutual responsibilities of HMC and the Participant or External Partner for compliance with the policies in this document and shall be amended as needed.

Any Participation Agreement that contains provisions that are not consistent with the policies in this document shall require approval by HMC.

HMC shall have the right to conduct without notice at any time an audit of the Participant's or External Partner's compliance with the privacy and other provisions of the Participation Agreement.

HMC shall have the right to schedule with the Participant or External Partner an audit of compliance with other provisions of the Participation Agreement.

2.2.2. Participant

Each Participant shall execute a Participation Agreement with HMC in a form determined by HMC from time to time prior to beginning live exchange of data. Such a Participation Agreement shall establish the mutual responsibilities of HMC and the Participant for compliance with the policies in this document and shall be amended as needed.

2.3. Termination and Suspension of Participation

2.3.1. HMC

HMC shall terminate or suspend a Participant's participation in HealthConnect only as directed by the Participant or for cause.

HMC shall promptly investigate any incident or report of non-compliance with a Participation Agreement by a Participant. Upon completing a preliminary investigation and determining that there is a reasonable likelihood that a Participant's acts or omissions would cause harm to another Participant, or to a Patient whose data is exchanged through the network, HMC shall summarily suspend the Participant's participation in the HealthConnect. HMC shall provide notice of suspension to all other Participants, and HMC shall provide to the suspended Participant a written summary of the reasons for the suspension.

If desired by the Participant and if approved by HMC, HMC shall work with the Participant to correct the situation that caused the suspension. Upon resolution of the situation, HMC shall reinstate participation and shall notify other Participants of the reinstatement.

2.3.2. Participant

A Participant may terminate its participation in HMC HealthConnect, with or without cause, by giving HMC written notice. HMC shall execute such instructions by terminating the Participant's ability to access HealthConnect services without any further action by the Participant, and HMC shall provide notice of such termination to the remaining Participants

2.4. Release/Disclosure of Patient Information

Holyoke Medical Center's Privacy Policy describes how medical information about patients may be used and disclosed. The policy also states how patients can get access to their health information. The HMC Privacy Policy can be found at www.holyokehealth.com.

2.4.1. Disclosure of Sensitive Patient Information

Some federal, state, and local laws may impose requirements and restrictions on disclosure of certain types of medical information and may require certain types of patient consent for such disclosures. For example, Massachusetts law imposes restrictions on sharing patient information held by certain health plans related to HIV/AIDS status, genetic testing, confidential communications with mental health professionals, treatment of substance abuse (alcohol or drug), venereal disease(s), abortion, mammography or family planning services ("sensitive information").

Responsibility for obtaining approval for or restricting the transmission of sensitive information shall reside with the Participant providing the information to HMC HealthConnect ("Sending Participant").

2.4.1.1. Participant

If sensitive information is restricted by the Sending Participant, one of the following conditions shall apply:

- The Sending Participant shall obtain appropriate patient authorization, if required, prior to transmitting sensitive information and shall transmit such information only if such authorization has been obtained. In this case, responsibility for restricting information on a patient-by-patient basis resides with the Sending Participant, and the Sending Participant shall inform HMC in writing that it appropriately restricts transmission of sensitive information.

- The Sending Participant shall remove sensitive information from a transmission or shall engage another party to remove such information. In this case, the Sending Participant shall inform HMC in writing that such data is removed from transmissions

2.5. Breach Notification Policy

Both HMC and the Participants will work to ensure that patient health information remains safe and protected. However, in the event that patient health information is misused or the privacy and security of the information is compromised, the following policies outline the responsibilities of HMC and the Participants

2.5.1. HMC

In the event that HMC becomes aware of any actual or suspected breach either through notification by a Participant or otherwise, HMC shall:

- Notify any Participants whose data is affected by the breach.
- Investigate (or require the applicable Participant to investigate) expediently and without unreasonable delay the scope and magnitude of such actual or suspected breach, and identify the root cause of the breach.
- Mitigate (or require the applicable Participant to mitigate) to the extent practicable, any harmful effect of such breach that is known to HMC or the Participant. HMC's mitigation efforts shall correspond with and be dependent upon its internal risk analyses.
- Notify (or require the applicable Participant to notify) the Patient and any applicable regulatory agencies as required by federal, state and local laws and regulations, except if a law enforcement agency determines that such notification impedes a criminal investigation.

2.5.2. Participant

Each Participant shall maintain and uphold individual policies for the notice of misuse or breach of policies. In addition, the Participant shall also adhere to the following:

- Appropriately train its personnel and inform them of sanctions and other action that will result from any breach of confidentiality.
- Report any breaches and/or security incidents to the particular Participant or External Partner whose data was improperly used. Notification shall be made in writing and in the most expedient time possible and without unreasonable delay.
- Report to HMC any actual or suspected breach of confidentiality. Notification shall be made in writing in the most expedient time possible and without unreasonable delay.

- Notify the patient whose health information was disclosed in breach of policy.

2.6. Access to HMC HealthConnect Policies and Standards

2.6.1. HMC

HMC shall provide Participants with access to its data exchange policies upon request.

2.6.2. Participant

Participant shall provide access to its data exchange policies upon request.

2.7. Authentication and Authorization of System Users

Access to Patient data must be carefully controlled, given its sensitive and private nature. Data in electronic form are vulnerable to copying, tampering, and other misuse. HMC and its Participants must ensure that only system users who have been authenticated as being persons authorized to access a Patient's health information for a specific permitted purpose are allowed access to that information.

HMC network security is based on the principle of 'transitive trust'. That is, each node in a network data exchange must trust the immediate preceding node, and so on. Therefore, clear definition of the affiliation of individual User to a Participant organization is critical. A User who accesses data via the HealthConnect is assumed to have been registered as an authorized User by a Participant Organization.

In conducting clinical data exchange via the HealthConnect, Participant organizations are the primary network destinations for addressing messages. Messages to and from individual Users will be routed via the Participant organization with which the User is affiliated. This policy is consistent with the need for individual Users to be invariably authenticated by a Participant system before access to PHI is granted.

2.7.1. HMC

HMC shall establish 'Roles' for all Users, which define categories of Users of HMC services. These categories are based on the types of Patient data that these users need to access to perform their job functions, and the permitted purposes for such access. The permitted purposes are based on each User's job function and relationship with the Patient. HMC Roles are used as community standard classifications, to enable Sending and Receiving Participants to establish access control rules that are meaningful to each other. Participants may continue to use local roles for controlling access to clinical information communicated via the HealthConnect, as long as there is a clear mapping between local and HMC roles.

Example: Industry standards for healthcare stakeholder Roles are evolving. Initial data exchange programs have adopted simple structures, such as classifying users into two categories (Roles): *clinical* and *administrative*. HMC will initially favor simple, broad Role definitions to facilitate adoption by Participants and will refine these definitions over time.

2.7.2. Participant

Each Participant shall adhere to the following practices:

- Authenticate all system Users before the User is given access to any HMC resource containing Patient data.
- Assign each system User with access to HMC services to a specific Role as defined by HMC.
- Mutually communicate and authenticate credentials. In any data exchange, the Sending Participant shall communicate its credentials, and the receiving Participant shall use such credentials to authenticate that the Sending Participant is a HMC Participant in good standing.
- Verify that the user accessing received Patient data has a Role that is permitted to access the type of data being requested from the Sending Participant.

  Example: One User may be affiliated with multiple Participant organizations. Access privileges are governed by the Role of the User in the Participant organization to which the clinical message is addressed. A User may be the Primary Care Physician of a Patient in one clinic, authorized to view the full longitudinal health record in a message addressed to that clinic. The same User may play a specialist Role in another Participant organization, where messages are filtered to display only data needed for permitted purpose.

- Maintain policies and procedures that govern Users' ability to access information on or through the Participant's system and through HMC services ('Participant Access Policy').
- Impose appropriate sanctions for work force members who violate security policies or make improper use of PHI, including revocation of a User's authorization to access the network as may be appropriate under the circumstances.
- Provide its Participant Access Policies to any other Participant upon reasonable request.

2.8. Auditing Access to Patient Information

As Patient data are shared across the HealthConnect, the ability to monitor and audit how Users access information is essential to ensure that all Participants involved in data exchange are complying with access control policies. In addition, publicly announced audit and logging practices foster trust among stakeholders that Patient data are used only in appropriate ways by HMC and Participants.

2.8.1. HMC

HMC shall adhere to the following practices:

- Maintain logs of all messages that pass through its systems, and make them available to Participants upon reasonable request.
- Make logs pertaining to a network interaction available to Participants who were party to the interaction.
- Monitor, and retain capability to audit, data sharing operations across the network.
- Audit a specific Participant's activities related to the data sharing network when HMC has reasonable cause to believe that the Participant may be in material breach of policy or is otherwise compromising the security or stability of the network. Such audits may include requests for documents and information from a Participant concerning its activities in connection with the network, and access to all audit logs maintained by the Participant.

2.8.2. Participant

Participants shall adhere to the following practices:

- Maintain logs of all messages transmitted using the HealthConnect services, in conformance with specifications published by HMC.
- Fully cooperate with any monitoring or auditing activities by providing information requested by other Participants who have participated in data exchange with them, or by HMC in the process of ensuring secure and reliable operation of the network.
- Conduct periodic reviews, not less than once in a calendar year, of Participant's internal security controls, for example, logs, access reports, and incident tracking, and make results of the review available to HMC.

2.9. Use of Data Exchange Standards

Achieving data interoperability across Participants' systems requires the implementation of common data exchange standards by the systems involved. Traditionally, the healthcare sector has focused on data interface standards to support integration across clinical systems within a provider enterprise. Extension of these standards to inter-enterprise data movement requires the specification of coherent standards across the network from low level transport to common clinical and terminology and reference codes.

Concurrent with the HMC policy development and implementation of clinical data exchange, there are Federal initiatives under way to specify standards for secure and reliable healthcare data exchange between disparate healthcare entities over the Internet. The policies outlined below will evolve to conform to national and regional standards as they are institutionalized.

2.9.1. HMC

HMC shall adhere to the following practices:

- Adopt data element, message and network protocol standards (referred to as 'data exchange standards') that shall be used by HMC and Participants too securely and reliably exchange health information. Data exchange standards shall conform to open industry standards and be technology neutral so as to pose the lowest practical barrier to entry for Participants without sacrificing data security and privacy. Data exchange standards shall conform with the National Health Information Network (NHIN) and the Integrating the Healthcare Enterprise (IHE) frameworks, set of standards, services and policies as a benchmark to address the disparity of information systems across the various locations within the community.

- Develop, maintain, and publish Implementation Guides that set forth the data exchange standards. HMC Implementation Guides:
    - Shall be developed through a community process into which all interested Participants shall have input and shall have the right to propose alternatives.
    - Shall be adapted and revised as needed to accommodate new use cases for community data exchange and to accommodate industry developments and changes.
    - Shall be designed to allow Participants to progressively adapt to new and changed data exchange standards. For example, an "earlier" version of a standard shall be supported for an agreed-upon time period to allow Participants to adapt to a current version.
    - Shall be designed to support the incremental growth of data granularity across HMC HealthConnect.

2.9.2. Participant

Participants shall adhere to the following practices:

- Comply with HMC Implementation Guides rigorously to support efficient interoperability across the network. Compliance shall include filling all mandatory data elements, and making best efforts to fill optional data elements, preclude unconventional interpretations of data exchange standards not supported by the Implementation Guide.

- Support the growth of interoperability across Participants' systems by making best efforts to progress from unstructured data exchange to structured data exchange.

- Make best efforts to adopt revised standards expeditiously so as to enable the community to keep up with technological development and industry best practices.

- Maintain internal data and messaging formats and ensure that internal system changes do not adversely impact compliance with HMC data exchange standards.

2.10. Security

Besides security mechanisms, supported through data exchange standards, used to ensure than only Authorized Users access HMC resources, the community must consistently implement additional safeguards to protect the confidentiality and integrity of its information assets.

HMC security policies are designed to meet minimum legal requirements and may be augmented by Participants based on best practices agreed to by the community.

2.10.1. HMC

HMC shall adhere to the following practices:

- Maintain a secure environment for all its systems that handle Patient data and any centralized data repositories containing Patient or Participant data. Implement and enforce appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data.

- Ensure that in the operation of directories and registries such as Patient registries and Provider registries are secure to ensure no incidental disclosure of data occurs during the process of searching for patient or provider matches in the directories. Such controls shall be appropriate to the type of data searched.

- Avoid the use of proprietary encryption algorithms, unless reviewed by qualified experts outside of the vendor in question and approved by Federal guidelines.

2.10.2. Participant

Participants shall adhere to the following practices:

- Maintain a secure environment for HMC-related infrastructure, services, and data to support the secure and reliable operation and continued development of the HealthConnect. Participants shall implement and enforce appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of all data accessed through the HealthConnect services.
- Employ security controls that meet applicable industry or federal standards so that the information and data being transmitted shall not introduce any viruses, worms, unauthorized cookies, Trojans, malicious software, or "malware". In the absence of applicable industry standards, each Participant shall use all commercially reasonable efforts to comply with the requirements of this policy.
- Collaborate with HMC to develop security policies and to amend, repeal or replace provisions as necessary to support the secure operation and continued development of the network.

2.11. Operational Responsibilities

System service levels and procedural controls are essential to support the reliable exchange of clinical data, and the incorporation of data sharing into critical clinical and operational workflows at Participant organizations.

2.11.1. HMC

HMC shall adhere to the following practices:

- Develop 'service levels' for support of operational processes and problems that may arise during exchange of health data between Participants. These service levels shall include obligations on the part of HMC as well as expectations of the Participants involved in HMC HealthConnect, to maintain a minimum level of network performance and continuity of operation.

- For each use case, identify network or operational risks that could affect patient safety or quality of care, and define ground rules for each participant involved to mitigate each risk. These rules shall govern the Participants' and HMC's responsibilities during the course of normal operations and in the event of problems.

- Size and configure systems integral to the operation of the network to enable agreed-upon levels of performance. The performance level shall be determined based on what is essential for the efficient and effective implementation of the use case across the Participant organizations.

2.11.2. Participant

Participants shall adhere to the following practices:

- Fulfill all assigned responsibilities as initiators, responders or receivers of clinical data from other Participants.

  In general, for all use cases, the Receiving Participant shall acknowledge receipt of a clinical message and its appropriate disposition to the Sending Participant. Any exception in handling clinical information at the Receiving Participant shall be communicated to the Sending Participant, which shall take appropriate steps to mitigate the impact of the exception.

- Commit to minimum service levels for their systems so as to enable the efficient and effective clinical data exchange across the HMC network.

  Example: Edge systems may be used to route messages as well as to cache data used for clinical messaging. The availability of these systems is essential to the reliable functioning of the HMC network and should be assigned appropriate priority by Participant organizations.

3. Definitions

Affiliated Practitioner: An affiliated practitioner refers to:

(a) A Practitioner employed by or under contract to a Provider Organization to render health care services to the Provider Organization's patients.

(b) A Practitioner on a Provider Organization's formal medical staff.

(c) A Practitioner providing services to a Provider Organization's patients pursuant to a cross-coverage or on-call arrangement.

Audit Log: An electronic record of the access of information via the HealthConnect, such as, for example, queries made by Authorized Users, type of information accessed, information flows between the HealthConnect and Participants, and date and time markers for those activities.

Authorized User: An individual who has been authorized by a Participant or by HMC to access patient information in accordance with HMC policies and procedures.

Breach: Any unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of Protected Health Information or Demographic Information. An Incidental Disclosure by HMC or a Participant is not a Breach.

Clinical Data: Clinical Data includes healthcare data directly related to care provided to individuals and data used to manage HMC HealthConnect of clinical data.

Participant Agreement: A written, signed agreement between HMC and a Participant or between HMC and an External Partner which sets forth the terms and conditions governing the operation of the HealthConnect and the rights and responsibilities of HMC and the Participant or External Partner with respect to clinical data exchange.

External Partner: An organization that is not a HealthConnect Participant but engages in clinical data exchange with the HealthConnect, provides clinical data services to HMC, or receives clinical data services from HMC. Examples may include local, regional and federal public health authorities and remote provider organizations that exchange patient referrals and clinical summaries with HealthConnect Participants via the HealthConnect.

Health Information Exchange (HMC HealthConnect): An organization or group of organizations which develops and manages a set of contractual conventions and terms, arranges for the means of electronic exchange of information, and develops and maintains HMC HealthConnect standards.

Implementation Guide: A document intended for use by technical persons which defines standards, guidelines, and other rules for transmission of clinical data via the HealthConnect.

Participant: A Provider Organization, Payer Organization, or Other Organization that has directly entered into a Participant Agreement with HMC, accesses Protected Health Information via the HealthConnect, and actively participates in HMC HealthConnect of electronic healthcare data via the HealthConnect.

Policy: A formal statement or plan that defines an organization's general beliefs, goals, and acceptable procedures for a specified subject area.

Protected Health Information (PHI): Individually identifiable health information (e.g., any oral or recorded information relating to the past, present or future physical or mental health of an individual; the provision of health care to the individual; or the payment for health care) of the type that is protected under the HIPAA Privacy Rule.

Provider Organization: An entity such as a hospital, nursing home, home health agency or professional corporation legally authorized to provide health care services.