REFERENCE ID NUMBER: 001	POLICY TYPE: IT INFORMATION SECURITY MANAGEMENT
OWNER: CHAD PETERSON	
EFFECTIVE DATE: 2/26/16	DOCUMENT NAME:
REVISION DATE: 7/28/16	**ACCESS CONTROL POLICY**

ACCESS CONTROL POLICY

PURPOSE

To protect an Individual's health information from unauthorized use, the Koble-MN HIO shall verify the identity of Participants and their Authorized Users before access to Koble-MN HIO is granted. Health information available through Koble-MN HIO shall be accessed only by Authorized Users who have been granted access rights.

SCOPE

This policy applies to all Koble-MN HIO participants and workforce; participants, employees / users, temporary staff, contracted staff, and credentialed provider staff.

AUTHENTICATION

Authentication is the process of verifying that an Authorized User who is seeking to access information through the Koble-MN HIO is the individual who the Authorized User claims to be.

PARTICIPANT AUTHENTICATION

The Koble-MN HIO CEO, or designee, and each Participant shall execute a written and signed Koble-MN HIO Participation Agreement prior to the Network access.

The Koble-MN HIO shall review, evaluate and act upon requests submitted by organizations that want to become a Koble-MN HIO Participant.

- Each Koble-MN HIO Participant must demonstrate that it is a legitimate business by completing an application and provide the requested information. The Koble-MN HIO participant must assure that its agents and workforce access ePHI for only valid business reasons and that it participates in the types of health care transactions required of a Covered Entity or its Business Associate.
- The Koble-MN HIO CEO, or designee, in collaboration with the Koble-MN HIO participant shall determine whether the entities meet technical and operational requirements and pass the readiness assessment.
- Koble-MN HIO Participant identity shall be authenticated and unique user names and passwords shall be assigned by Koble-MN HIO to Authorized Users identified by Participant.
- Each Koble-MN HIO Participant shall designate its responsible contact person (e.g., department manager) who shall be responsible on behalf of the Participant for compliance with Koble-MN HIO policies and to receive notice on behalf of the Participant. Access rights shall be properly authorized and documented by the participant contact and access rights will be periodically audited to ensure compliance.
- Koble-MN HIO Participants shall, within five (5) working days, notify Koble-MN HIO if there is a material change in status such as a change in ownership or change in job assignment. If the Participant ceases to engage in health care transactions, it shall notify Koble-MN HIO at least 30 days before the change.
- Participants shall notify Koble-MN HIO within twenty-four hours, of termination of an Authorized User's employment or affiliation with the Participant.
- Only information technology staff at Koble-MN HIO or system administrators are permitted to create or change access control settings.

REFERENCE ID NUMBER: 001	POLICY TYPE: IT INFORMATION SECURITY MANAGEMENT
OWNER: CHAD PETERSON	DOCUMENT NAME: **ACCESS CONTROL POLICY**
EFFECTIVE DATE: 2/26/16	
REVISION DATE: 7/28/16	

AUTHORIZED USERS

Koble-MN HIO Participants shall designate the Authorized Users within their organizations who will be authorized to access information through the Koble-MN HIO. Participants shall develop and implement policies to assure proper identification of each Authorized User.

- Authorized Users shall be required to execute a user agreement prior to network access.
- Authorized Users must maintain a current relationship with a Participant to access the Koble-MN HIO.

Access to health information shall be based on the Authorized User’s job function and relationship to the patient. Categories of Authorized Users shall be established, at a minimum, as the following:

1. Practitioner with access to clinical information and “Break the Glass” authority.
2. Practitioner with access to clinical information but no “Break the Glass” authority.
3. Non-practitioner with access to clinical information.
4. Non-practitioner with access to non-clinical information.

Koble-MN HIO Administrative Authorized Users shall be based on the job functions. Categories of Koble-MN HIO Administrative Authorized Users shall be established, at a minimum, as the following:

1. Administrative Authorized User with access to non-clinical information.
2. Administrative Authorized User with access to clinical information to resolve technical issues or input advance directives received from third parties.
3. Administrative Authorized user with access to clinical information for audit purposes.

PASSWORDS

Each Authorized User shall be assigned a unique user name and an initial password that is required to be changed at the next use by Koble-MN HIO.

Passwords shall meet the strong password guidelines set forth in this Koble-MN HIO Access Control Policy.

1. Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing the last 5 passwords.
2. Password must be a minimum of eight characters and contain a combination of upper case letters, lower case letters, and special characters.
3. Password should not be a word found in the dictionary (English or foreign).
4. The password should not be a name, initials, birthdays or phone numbers associated with authorized user.

Authorized Users are prohibited from sharing their user names and passwords with others and from using the user names and passwords of others.

Koble-MN HIO shall encrypt user authentication data stored in the Network.

FAILED ACCESS ATTEMPTS

REFERENCE ID NUMBER: 001	POLICY TYPE: IT INFORMATION SECURITY MANAGEMENT
OWNER: CHAD PETERSON	DOCUMENT NAME: **ACCESS CONTROL POLICY**
EFFECTIVE DATE: 2/26/16	
REVISION DATE: 7/28/16	

The Koble-MN HIO shall enforce a limit of consecutive failed access attempts by an Authorized User. Upon the 5th failed attempt, Koble-MN HIO shall disable the Authorized User's access to the KOBLE-MN HIO. The Authorized User may reestablish access using appropriate identification and authentication procedures established by the Participant.

PERIODS OF INACTIVITY

The Koble-MN HIO will have an automatic log-off and will terminate an electronic session after 30 minutes of inactivity. A Participant may establish a shorter automatic log-off and termination period for an electronic session on its network or for any device or class of devices used by its Authorized Users to access the Participant's network.

TRAINING

Participants shall provide training for all of its Authorized Users consistent with the Participant's and Koble-MN HIO policies including privacy and security requirements.

PARTICIPANT POLICIES/REMOTE ACCESS

Each Koble-MN HIO Participant shall establish and enforce policies and procedures regarding Authorized User access to Patient Data (including Remote Access), the conditions that must be met and documentation that must be obtained prior to allowing an Authorized User access to Patient Data.

Policies shall include procedures for taking disciplinary actions for its Authorized Users or members of its workforce in the event of a breach or non-compliance with the policies.

The Koble-MN HIO Participant may suspend, limit, or revoke the access authority of an Authorized User on its own initiative upon a determination that the Authorized User has not complied with the Participant's policies or the Koble-MN HIO policies. The Koble-MN HIO Participant shall inform the Koble-MN office immediately, and in any case within twenty-four hours, of any revocation or suspension.

KOBLE-MN AUTHENTICATION

Koble-MN HIO shall authenticate users accessing the Koble-MN HIO with each attempt the user accesses the Network.

References: 45 C.F.R. §164.308 (3) (i), 45 C.F.R. §164.308 (3) (i), 45 C.F.R. §164.312(d), 45 C.F.R. §164.312(a) (1-2).

REFERENCE ID NUMBER: 001	POLICY TYPE: IT INFORMATION SECURITY MANAGEMENT
OWNER: CHAD PETERSON	DOCUMENT NAME: **ACCESS CONTROL POLICY**
EFFECTIVE DATE: 2/26/16	
REVISION DATE: 7/28/16	

REVISION HISTORY

DATE	DESCRIPTION OF REVISION	AUTHOR	APPROVAL DATE	APPROVED BY NAME & TITLE
7/26/16	Full review of Policy-See Advisory Committee Notes dated 7/28/16	Laurie Peters	7/28/16	Koble-MN Advisory Group

INTENTIONALLY LEFT BLANK