REFERENCE ID NUMBER: 012	POLICY TYPE: IT INFORMATION SECURITY MANAGEMENT
OWNER: CHAD PETERSON	
EFFECTIVE DATE: 2/26/16	DOCUMENT NAME:
REVISION DATE: 7/28/16	**SECURITY INCIDENT MANAGEMENT**

SECURITY INCIDENT MANAGEMENT

PURPOSE

Provides guidelines to Koble-MN HIO Participants for the identification and reporting of information security incidents.

SCOPE

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

ROLES & RESPONSIBILITIES

It is the primary responsibility of Koble-MN HIO participants and workforce to identify and respond to suspected or known security incidents in order to limit risk to exposure and mitigate harmful effects of such incidents.

Koble-MN HIO will provide incident management training to all management staff on how to identify and report security incidents and how to continuously and proactively monitor for security incidents.

VIOLATION of this policy may result in disciplinary action up to and including termination of employment for Koble-MN HIO employees and temporary or contract staff.

REFER TO *BREACH MANAGEMENT AND NOTIFICATION POLICY* FOR SPECIFIC REPORTING REQUIREMENTS

DEFINITION OF SECURITY INCIDENT

For purposes of this policy, security "incident" means the act of violating an explicit or implied security policy, which includes unwanted disruption or denial of service, the unauthorized access to a system or its data; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent.

Incidents include the loss of data through theft or device misplacement, loss or misplacement of hardcopy documents, and misrouting of mail, all of which may have the potential to put the data at risk of unauthorized access, use, disclosure, modification or destruction.

While certain adverse events, (e.g. floods, fires, electrical outages, excessive heat, etc.) can cause system crashes, they are not considered incidents.

SEVERITY OF AN INCIDENT

When determining the scope of a security incident the following criteria will be considered:

- Scope of the impact
- Critical nature of the system or service that is affected
- Sensitivity and type of information accessed

- Likelihood that the negative impact will affect other systems or services or spread?

Response will be guided by the level of severity of the incident.

Level of Severity will be rated as – HIGH, MEDIUM, LOW AND NOT APPLICABLE

GUIDELINES FOR SECURITY INCIDENT RESPONSE:

HIGH SEVERITY INCIDENT: *SIGNIFICANT ADVERSE IMPACT ON A LARGE NUMBER OF INDIVIDUALS OR SYSTEMS, PRESENTS A LARGE FINANCIAL RISK OR LEGAL LIABILITY OR THREATENS CONFIDENTIAL DATA OR A CRITICAL SYSTEM OR SERVICE.*

RESPONSE: Requires immediate and focused attention by the Koble-MN HIO CEO, notification of legal and all department managers, incident response report and formal / extensive notification.

MEDIUM SEVERITY INCIDENT: *DISRUPTS A BUILDING OR DEPARTMENT NETWORK, IMPACTS A MODERATE NUMBER OF INDIVIDUALS OR SYSTEMS OR IMPACTS A NON-CRITICAL SERVICE OR SYSTEM.*

RESPONSE: Requires a quick response by personnel in the affected unit or department who have primary administrative responsibility within 4 hours of the incident, notification of CEO, legal, affected department manager and an incident response report if requested by Koble-MN HIO CEO.

LOW SEVERITY INCIDENT: *IMPACTS VERY SMALL NUMBER OF INDIVIDUALS, SERVICES, NETWORKS OR BUSINESS SEGMENTS WITH NO RISK OF PROPAGATION AND LITTLE DISRUPTION.*

RESPONSE: Response by the next business day, notify Koble-MN HIO CEO and affected department manager, no incident report required unless the CEO requests it for the purposes of tracking patterns or trends.

NOT APPLICABLE: *USED FOR ANY SUSPECTED SECURITY INCIDENTS THAT ARE UNDER INVESTIGATION.*

REPORTING PROCEDURES

Koble-MN HIO participant or workforce member will immediately notify the Koble-MN HIO Help Desk (at (844) 335-6253, option 4) of any reportable security incident.

A ticket will be opened and notification of the appropriate resources will begin as stated above.

Each incident will be documented as per the Koble-MN HIO BREACH MANAGEMENT AND NOTIFICATOIN POLICY and the record of that incident retained for at least one year or until the security incident is resolved.

Koble-MN HIO will report security breaches affecting individuals within 60 days of the breach via email or postal service mail and HHS will be notified of any security breach that reaches the harm thresholds outlined in the HIPAA Security Rule.

KOBLE-MN HIO REPORTING OF SECURITY INCIDENTS TO PARTICIPANTS

Koble-MN HIO will report to a Participant any successful impermissible access, use, disclosure, modification, or destruction of Participant's electronic PHI or interference with system operations in an information system containing Participant's electronic PHI of which KOBLE-MN HIO becomes aware, within five (5) business days of Koble-MN HIO's learning of the event.

When feasible, Koble-MN HIO will also report to a Participant the aggregate number of unsuccessful attempts of impermissible access, use, disclosure, modification, or destruction of electronic PHI or interfere with system operations in an information system containing electronic PHI of which Koble-MN HIO becomes aware, provided that these reports will be provided only as frequently as the parties mutually agree.

RECOGNITION OF UNSUCCESSFUL ATTEMPTS – PROACTIVE MONITORING PROCEDURE

Koble-MN HIO recognizes the number of unsuccessful attempts to the network, that is, remote access attempts without authorization.

- The number of unauthorized remote access attempts have a demonstrable effect on incident handling capability.
- Therefore, an "unsuccessful security event" is defined as one that does not result in unauthorized access, use, disclosure, modification, or destruction of electronic PHI or does not result in interference with an information system.
- No further notice of any such unsuccessful security event will be required.

References: 45 C.F.R. § 164.312 (c) (1-2), 45 C.F.R. § 164.312 (d), 45 C.F.R. § 164.312 (a) (1-2), 45 C.F.R. § 164.308 (3) (i), 45 C.F.R. § 164.308 (4) (i)

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 Committee

INTENTIONALLY LEFT BLANK