POLICY INFORMATION

Document # **700**	Title: **Security Incident Procedures**	Print Date: **8/29/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Safeguard: **Administrative**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B86710B5491...	Date Approved: 9/7/2016

I. POLICY STATEMENT

All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of PHI must be reported. This policy establishes a security incident process for all covered components.

II. DEFINITIONS

See HIPAA Privacy Policy 100

III. AUTHORITY AND RESPONSIBILITIES

CEHS has component units that are listed as a hybrid entity in accordance with USU's HIPAA Hybrid Covered Entity Declaration. Only the Health Care Component/HCC (i.e., covered functions) of CEHS must comply with this policy. All references in this policy to "CEHS" shall be construed to refer only to the health care component of CEHS.

IV. PROCEDURES TO IMPLEMENT

Workforce members are required to report all known or suspected security incidents to the CEHS Security and/or Privacy Officer(s). A security response team will be formed based on the type and location of incident. The security response team could include:

a. Department Head
b. CEHS Security Officer
c. CEHS Privacy Officer
d. ISO Security Officer
e. Others as needed (for example, Media Relations or USU PD)

1. REPORTING SECURITY INCIDENTS - Any member of the CEHS community who suspects the occurrence of a security incident must report all incidents through the following channels:
    a. All suspected high severity events as defined in section 2 below, including those involving possible breaches of PHI, must be reported directly to the CEHS Security and/or Privacy Officer(s) as quickly as possible by phone (preferred), email, or in person.

b. All other suspected incidents must also be reported to the CEHS Security and/or Privacy Officer(s). These incidents may be first reported to departmental IT support personnel, the components clinic privacy Officer, or to the clinic director who can then contact the CEHS Security and/or Privacy Officer(s).

2. RESPONDING TO SECURITY INCIDENTS - Incident response will be managed based on the level of severity of the incident. The level of severity is a measure of its impact on or threat to the operation or integrity of CEHS and its information. The severity level determines the priority for handling the incident, who manages the incident, and the timing and extent of the response. Four levels of severity will be used to guide the incident response:
    a. **High -** The severity of a security incident will be considered "high" if any of the following conditions exist:
        i. Threatens to have a significant adverse impact on a large number of systems and/or people (for example, all of CEHS is affected).
        ii. Poses a potential large financial risk or legal liability to CEHS.
        iii. Threatens PHI (for example, the compromise of a server that contains patient records).
        iv. Adversely impacts a system or service critical to the operation of a major portion of CEHS (for example, email, internet service, Point & Click).
        v. Incident has a high probability of propagating to other systems causing significant damage or interruption of those systems.
    b. Medium - The severity of an incident is considered to be "medium" if any of the following conditions exist:
        i. Adversely impacts a moderate number of systems and/or people, such as an individual department or clinic.
        ii. Adversely impacts a non-critical system or service.
        iii. Disrupts a building or department network.
        iv. Incident has a moderate probability of propagating to other systems and causing moderate damage or interruption.
    c. Low - Low severity incidents have the following characteristics:
        i. Adversely impacts a very small number of systems or individuals.
        ii. Will disrupt a very small number of network devices or segments.
    d. Not Applicable - This is used for events reported as a suspected security incident but upon investigation of the activity, no evidence of a security incident is found.

The following table summarizes the handling of security incidents based on incident severity:

Incident Severity	**Characteristics** (one or more condition present determines the severity)	**Response Time**	**Incident Manager**	**Who to notify**	**Post-incident Report Required**
High	Significant adverse impact on a large number of systems and/or people Potential large financial risk or legal liability to CEHS Threatens PHI or other confidential data Adversely impacts a critical system or service High probability of propagating to other systems and causing disruption of those systems	Immediate	CEHS Security Officer	CEHS Security Officer CEHS Privacy Officer HCC Director IT administrator for affected device	Yes
Medium	Adversely impacts a moderate number of systems and/or people Adversely impacts a non-critical system or service Disrupts a building or departmental network Moderate risk of propagating to other systems and causing disruption to those systems	Within 4 hours	CEHS Security Officer	CEHS Security Officer CEHS Privacy Officer HCC Director IT administrator for affected device	Potentially- To be determined by CEHS Security and/or Privacy Officer
Low	Adversely impacts a very small number of	By next business	Technical support for	CEHS Security	No

Incident Severity	**Characteristics** **(one or more condition present determines the severity)**	**Response Time**	**Incident Manager**	**Who to notify**	**Post-incident Report Required**
	non-critical individual systems, services or people Disrupts a very small number of network devices Little risk of propagation and further disruption	day	affected device	Officer CEHS Privacy Officer	
Not Applicable - used for suspicious activities which upon investigation are determined not to be a security incident.					

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR 164.308(a)(6)

Utah State Board of Regents Policy R345