POLICY INFORMATION

Document # **700**	Title: **Privacy & Security Incident Procedures**	Original Effective Date: **8/29/2016**
Safeguard: **Administrative**	Approved by: **Dean Beth E. Foley**	Date Reviewed: **10/13/2017** **9/30/19**

I. POLICY STATEMENT

It is vital to the CEHS community that all incidents that threaten the security or privacy of confidential information are properly identified, contained, investigated and remedied. All incidents, threats, or violations that affect or may affect the confidentiality, integrity, or availability of PHI must be reported. This purpose of this policy is to provide the basis for appropriate response to incidents and a process for documentation, investigation and appropriate reporting. Finally, the policy establishes responsibility and accountability for all steps in the process of addressing privacy and security incidents.

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

CEHS shall immediately respond to incidents to ensure confidentiality is maintained and to mitigate any adverse effects resulting from the incident. Workforce members are required to report all known or suspected privacy and security incidents to the CEHS Compliance Officer.

1. REPORTING PRIVACY AND SECURITY INCIDENTS

   Every workforce member has the responsibility to immediately report suspected or known breaches of the privacy or security of PHI. It is critical that incidents are reported as soon after discovery as possible. HIPAA regulations have strict notification timelines in the event of a breach. The notification requirements are based on initial time of

discovery not based on completion time of investigation. Typically, an investigation will need to be done in order to determine whether or not a breach has occurred. Investigations can take time.

2. RESPONDING TO INCIDENTS

After receipt of the initial report, the CEHS Compliance Officer and/or their designee will collect and review incident information. From there they will classify the incident and analyze the situation. Incident response will be managed based upon the results of the risk assessment.

A. Four-Factor Risk Assessment
   a. What type of PHI was involved, and to what extent?
   b. Who is the unauthorized person or organization?
   c. Did the person or organization acquire or view the PHI?
   d. To what extent has the risk been mitigated?

B. When notified of a serious incident with potential liability under the HIPAA regulations, the Compliance Officer will assemble an Incident Response Team (IRT) based upon the type and location of incident. The IRT could include:
   a. Administrative representation such as Department Head
   b. Representative from the clinic where incident occurred
   c. CEHS Information Technology representative
   d. USU Legal Counsel
   e. USU Privacy and/or Security Officer
   f. Others as needed (for example, Media Relations or USU PD)

The response team shall take the following actions:

   a. Create a timeline of events and conduct additional fact-finding tasks as necessary.
   b. Determine response to incident and assign responsibilities and timeframe for completion.
   c. Determine if any policies and procedures or processes must be changed to mitigate incident recurrence. Assign responsibility for making changes.

If, after examining all parts of the four-factor risk assessment it is determined that the incident meets the criteria of a breach, CEHS HIPAA Policy 202- Breach Notification should be implemented.

3. DOCUMENTATION

The CEHS Compliance Officer and, when applicable, the IRT will document all privacy and security incidents and corrective actions taken. Documentation will be maintained for six (6) years from the date the incident was closed or reported to the HHS. Documentation shall include:

a. Initial Incident Report Form.
b. Incident Risk Assessment and Findings Report.
c. Description of corrective actions taken, if any, or explanation of why corrective actions are not needed.
d. Any mitigation undertaken.
e. If incident is determined to be a breach, all breach notification documentation e.g., individual notices, media notices, notice to the Secretary.

V. ATTACHMENTS

Attachment A- Incident Report Form

VI. REFERENCES

CEHS HIPAA Policy 202- Breach Notification

45 CFR 164.308(a)(6)

45 CFR 164.530

Utah State Board of Regents Policy R345

Attachment A

CEHS Incident Report Form

The purpose of this form is to report information to any known or suspected violation of CEHS's security and privacy standards or the laws and regulations governing CEHS. Although we ask you to provide your name, it is not necessary for you to do so if you wish to make an anonymous report. An anonymous report can be made by completing this form and mailing it to the CEHS Compliance Officer at 6405 Old Main Hill Logan, UT 84322-6405. If you wish to identify yourself in this report, CEHS will make every effort to keep your identity confidential, unless you give CEHS permission to reveal it. Only the Compliance Officer and others designated by them will have access to your report. No disciplinary action or retaliation will be taken against you for making a good faith report of a compliance violation. Please complete this form. Include all factual details of the suspected violation, however big or small, to ensure that the Compliance Officer has all of the information necessary to conduct a thorough investigation. Please attach additional pages as needed. The information that you provide should include names, dates, times, places and a detailed description of the incident that led you to believe that a violation of CEHS's privacy and/or security standards have occurred. Please include a copy or a description of any documents that support your concerns. PLEASE DO NOT SEND ANY PHI VIA UNENCRYPTED EMAIL.

Date of this report:

Name of person making this report (optional):

Contact Information (optional):

Phone: Email:

Description of violation:

If applicable, electronic system(s) potentially affected by violation:

Detailed description of the incident(s) resulting in the violation (include names, dates, times and places):

Name(s) of person(s) involved in the incident and an explanation of their role:

Name(s) of other person(s) having knowledge of the incident:

Department where the incident occurred:

Date(s) of the incident:

Explanation of how you became aware of the suspected violation:

Please attach or describe any documents that support your concern (include a description of the documents, the identity of the persons who wrote the documents, the dates of the documents, and the location of the documents).