POLICY INFORMATION

Document # **200**	Title: **Security Management Process**	Original Effective Date: **9/06/2016**
Safeguard: **Administrative**	Approved by: **Dean Beth E. Foley**	Review Date: **10/20/2017** **10/02/19**

I. POLICY STATEMENT

CEHS will take reasonable and appropriate precautions to prevent, detect, contain, and correct security violations. It is the policy of CEHS to conduct thorough and timely risk assessment of the potential threats and vulnerabilities to the confidentiality, integrity and availability of the Protected Health Information (PHI) and to develop strategies to efficiently and effectively mitigate the risks identified in the assessment process as an integral part of the college's HIPAA information security program.

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

1. **System Identification and Tracking –** The CEHS IT department in conjunction with the HCC is responsible for identifying and maintaining an inventory of the information system(s) managed within HCCs. When a new information system is implemented, all applicable USU policies regarding approval, purchasing and implementation of new information systems will be followed.
2. **Risk Program -** The CEHS Compliance department will establish a program to identify and mitigate risks to PHI.

   Risk Assessments will take place:

   i. Periodically, based upon the USU Compliance Office schedule;
   ii. Whenever a new information system is implemented;

iii. In response to newly-recognized risk(s) that have identified as a result of activity reviews, security incidents, or environmental or operational changes.

3. **Completing the Risk Assessment:**
   The Risk Assessment team can involve some or all of the following individuals:

- CEHS Compliance Officer
- SCCE Compliance Analyst
- SCCE Executive Director
- CEHS Information Technology
- USU Information Security Office
- USU Privacy and/or Security Officer(s)
- Individual HCC Representatives

The Risk Assessment Team will work with each HCC to identify and document where confidential or sensitive data, including PHI, is created, received, maintained, processed or transmitted. Both physical boundaries as well as logical boundaries covering the media containing the confidential or sensitive electronic data, including PHI, regardless of its location should be documented. Any remote workforce removable media and portable computing devices (e.g. laptops, removable media and backup media) should also be taken into account.

The HCCs will gather all information requested by the Risk Assessment Team as well as identify (1) the conditions under which the confidential or sensitive electronic data, including PHI, is created, received, maintained, processed or transmitted by the HCC; and (2) the security controls currently being used to protect the data. An assessment of current security controls shall be performed.

The Risk Assessment Team will identify potential threat sources and vulnerabilities that are applicable to the HCCs and could have a negative impact on their ability to protect PHI. A report listing each threat should be compiled. Some examples of common threat sources are listed in the table below:

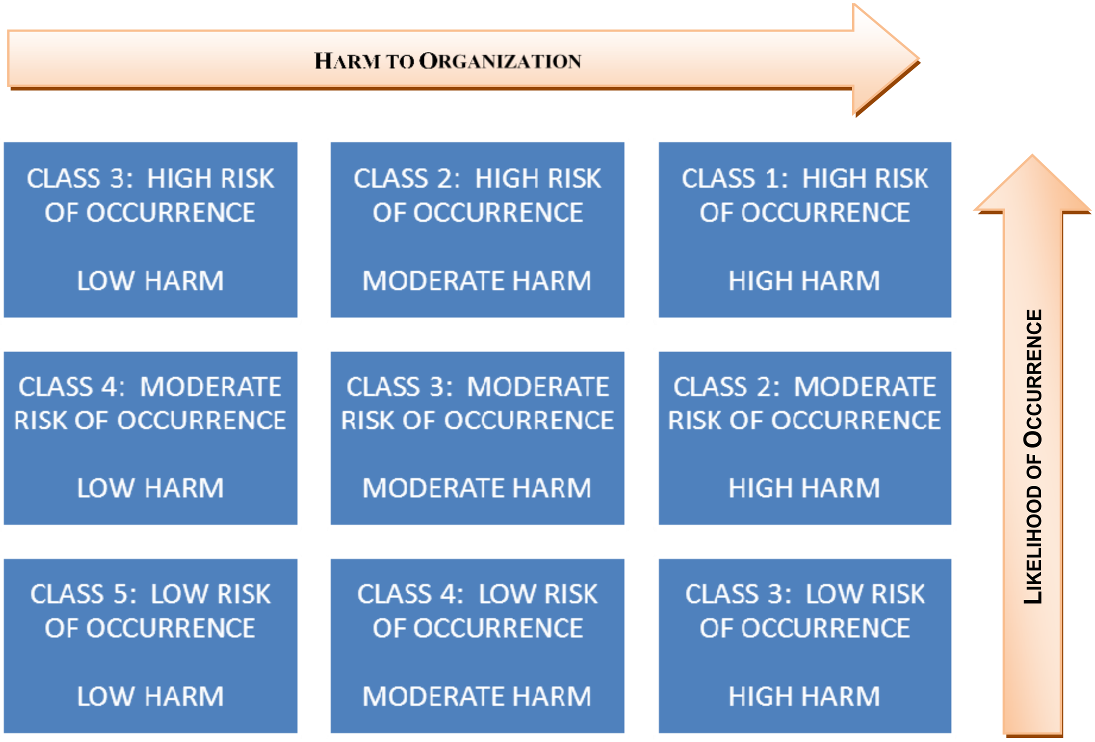
Type	Examples
Natural	Flood, earthquake, tornado, landslide, storms, etc.
Human	Unintentional human acts such as inadvertent data entry or deliberate acts such as unauthorized access to confidential information.
Environmental	Long-term power failure, pollution, chemicals, etc.

The Risk Assessment Team will determine the likelihood and impact of each threat. The system and data sensitivity can be determined based on the level of protection required to maintain the confidential data, including PHI's confidentiality, integrity and availability. The adverse impact of a security event can be described in terms of the loss of any, or a combination of any, of the following three security objectives; integrity, availability and confidentiality. The table below provides a brief description of each security objective and the impact of its not being met.

Security Objective	Impact Description
Loss of Confidentiality	System and data confidentiality refers to the protection of information from unauthorized disclosure. Unauthorized, unanticipated or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the HCC and CEHS.
Loss of Integrity	System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all of these reasons, loss of integrity reduces the assurance of an IT system.
Loss of Availability	If a mission-critical IT system is unavailable to its end users, CEHS's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

The Risk Assessment Team will then determine the risk level by taking into account the information acquired in all of the previous steps. The level of risk should be determined by analyzing the values assigned to the likelihood that a threat could occur, and the impact of the threat occurrence.

The following Risk Management Model can provide help in classifying the level of risk and potential harm to the organization:



CLASS 3: HIGH RISK OF OCCURRENCE LOW HARM	CLASS 2: HIGH RISK OF OCCURRENCE MODERATE HARM	CLASS 1: HIGH RISK OF OCCURRENCE HIGH HARM
CLASS 4: MODERATE RISK OF OCCURRENCE LOW HARM	CLASS 3: MODERATE RISK OF OCCURRENCE MODERATE HARM	CLASS 2: MODERATE RISK OF OCCURRENCE HIGH HARM
CLASS 5: LOW RISK OF OCCURRENCE LOW HARM	CLASS 4: LOW RISK OF OCCURRENCE MODERATE HARM	CLASS 3: LOW RISK OF OCCURRENCE HIGH HARM

Once classified, the following response and timeframes should be used:

CLASS	RISK	RECOMMENDED ACTION
Class 1	High Risk, High Harm	Allocation of resources necessary to accept, avoid, transfer or mitigate the risk within 48 hours.
Class 2	High Risk, Moderate Harm Moderate Risk, High Harm	Allocation of resources necessary to accept, avoid, transfer or mitigate the risk within 30 days.
Class 3	Moderate Risk, Moderate Harm Low Risk, High Harm High Risk, Low Harm	Allocation of resources necessary to accept, avoid, transfer or mitigate the risk within 60 days.
Class 4	Low Risk, Moderate Harm Moderate Risk, Low Harm	Review of the risk in order to determine the appropriate action. Such action may include allocation of resources to accept, avoid, transfer or mitigate the risk. Assumption of this risk should not be considered an option.

Risk Mitigation and Monitoring: The Compliance and IT Departments will recommend and monitor the effectiveness of security measures designed to reduce risks and vulnerabilities to a reasonable and appropriate level. More specifically these measures are designed to reasonably and appropriately:

- Protect the Confidentiality, Integrity, and Availability (CIA) of all PHI that CEHS HCCs create, receives, maintains or transmits.
- Protect against any reasonably anticipated threats or hazards to the CIA of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule.
- Facilitate workforce compliance.

4. **Information System Activity Reviews -** The Compliance Analyst and applicable system administrator will:
    a. Regularly perform Information System Activity Reviews (e.g., audit logs and trails, information system activity records, facility access records) for the purpose of detecting:
        i. Unauthorized access to PHI:
        ii. Unusual patterns of use or activity; and
        iii. Other potential security violations.
    b. Document the findings of the System Activity Review. Documentation shall be retained for at least six years from the date of review; and
    c. Report suspicious finding in accordance with the security incident reporting mechanisms established by CEHS.

5. **Security Incident Detection, Response and Reporting -**
   The Compliance Department will develop, document, and implement procedures to:
    a. Identify possible security incidents;
    b. Respond to suspected or known security incidents;
    c. Mitigate, to the extent practical, harmful effects of known security incidents; and
    d. Document and report security incidents and their outcomes. All documentation relating to potential and verified security incidents will be retained for at least six years from the date of documentation.
6. **Risk Acceptance -** There could be situations where a risk is reviewed and a determination is made that the risk is acceptable for the HCC's environment. When accepting the risk results in (1) an information system, a communications system, or an organizational unit being out of compliance with CEHS policies and procedures and/or standards, and (2) the responsible HCC Director does not intend to come into full compliance within the timeframe prescribed by CEHS policy, the Risk Acceptance form **(Attachment A)** must be prepared and submitted to the CEHS Compliance Department.
7. **Risk Avoidance -** The risk is reviewed and a determination is made that the risk can be removed from the HCC environment by removing the source of the risk. This could include removal of the application, host, platform or other system that contains the identified risk.
8. **Risk Transfer -** The risk is reviewed and a determination is made that the system capability is required but can be transferred to a third party vendor or provider. Although

such a transfer is an acceptable method for managing risk, it does not relieve the facility of compliance with a security policy or procedure.

V. ATTACHMENTS

Attachment A - Risk Acceptance Form

VI. REFERENCES

45 CFR §164.308 (a)(1)

Emma Eccles Jones College of Education and Human Services Utah State University

Attachment A

Risk Acceptance Form

WHEN TO USE THIS FORM: This form must be employed when (1) an information system, a communications system, or an organizational unit is known to be out of compliance with CEHS information security policies and/or standards, and (2) the responsible manager does not intend to come into full compliance within the timeframe prescribed by CEHS policy.

RISK ACCEPTANCE

Regarding policy or procedure number ______________________, dealing with the topic of: ____.

I understand that compliance with CEHS Security Policies and Procedures is expected for all departments, organizational units, and information and communication systems. I have read the above-named policy or procedure and I believe that the control(s) described therein should not be required for the following department, organizational unit, and information or communication system.

I furthermore understand that a control deficiency in one information system can jeopardize other information systems because erroneous data may be inherited, or because a conduit for an intruder to enter CEHS systems may be created. I also understand that non-compliance in this instance may adversely affect the morale or willingness of staff associated with other systems to comply with information security policies and standards. I understand that an exception to Information Security Policies and Standards is appropriate only when it would: (a) adversely affect the accomplishment of CEHS business, and/or (b) cause a major adverse financial impact that would not be offset by the reduced risk occasioned by compliance. I believe that an exception to this policy or standard is warranted because:

____

____

____

I have prepared, or have had a staff member reporting to me prepare, a written assessment of the risks associated with being out of compliance with the above-mentioned policy or procedure. This risk assessment has been reviewed and approved by the designated system owner and the HCC system administrator. I accept responsibility for this decision to be out of compliance with Policies and/or Procedures. Responsibility means that my job performance evaluation, my salary and bonus, and my continued employment status at CEHS can be jeopardized or damaged if a major loss takes place because this out of compliance situation existed. I also understand that this exception will expire one year from the date the above-mentioned approvals are obtained.

________________________________ ________________________________

Signature of responsible manager Date signed

____

Printed name of responsible manager

Procedural Note: If this out of compliance situation is to continue, the brief risk assessment regarding the out of compliance situation must be updated annually, the above-mentioned approvals must be obtained annually, and this form must be signed by the responsible manager annually. Each year the responsible manager must return a signed copy of this form to the Privacy and/or Security Official.