POLICY INFORMATION

Document # **101**	Title: **Security of Confidential & Sensitive Electronic Data & Information; Including PHI**	Print Date: **5/18/2016**
Revision # **1.0**	Prepared by: **J. Black**	Date Prepared: **1/15/2016**
Standard: **HIPAA**	Approved by: **Dean Beth E. Foley** DocuSigned by: beth foley 7AB6B86710B5491...	Date Approved: 8/7/2016

I. INTRODUCTION

It is the objective of CEHS to establish, document and implement policies and procedures to ensure the security of confidential or sensitive electronic data and information, including electronic Protected Health Information (ePHI) that is created, received, maintained or transmitted in CEHS's environment.

To establish formal Security Policies and Procedures that address the full range of security issues including but not limited to the following safeguards and documentation requirements required by the HIPAA Security Standards, 45 CFR § 164.302, *et seq.:*

1. Administrative Safeguards
2. Physical Safeguards
3. Technical Safeguards

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. POLICY STATEMENT

It is the policy of CEHS to establish a series of formal Information Security Policies and Procedures (the "Security Policies") that will address the following:

1. Ensure the confidentiality, integrity, and availability of electronic data, including ePHI, that is created, received, maintained, or transmitted within CEHS;
2. Protect against all reasonably anticipated threats or hazards to the security or integrity of such data, including ePHI;

3. Protect against any reasonably anticipated uses or disclosures of such data, including ePHI that is not permitted or required; and
4. Ensure compliance with the Security Policies by all members of the workforce.

V. PROCEDURES TO IMPLEMENT

To achieve the objectives of this policy, CEHS will establish and document security standards and implementation specifications to ensure the creation and maintenance of a security framework as defined in Security Policies.

1. CEHS will use appropriate security measures that allow the healthcare components to reasonably implement the HIPAA Security Standards and Implementation Specifications.
2. CEHS will allow for flexibility of approach by evaluating the following factors for establishing security measures:

    a. The size, complexity, and capabilities of each healthcare component.

    b. The healthcare component's technical infrastructure, hardware, and software security capabilities.
    c. The total cost of security measures.
    d. The probability and criticality of potential risks to confidential or sensitive electronic data, including ePHI.

3. Scalability: In order to maintain a flexible, scalable and technology neutral approach to the Security Rule, no single method is identified for addressing security safeguards. Scalability is another concept that was created as part of the Security Rule to tailor the process to the size and complexity of one's practice. When considering what steps must be taken to comply with the Security Rule, an HCC should take the following aspects of the HCC into account to determine to what degree one must comply:

    - Size
    - Complexity
    - Capabilities
    - Technological Infrastructure
    - Cost to Comply
    - Potential Security Risk

    Implementation Specifications:

    a. "Implementation Specifications" are the steps to be taken to achieve the Security Standard. They may be either Required or Addressable.
    b. If an implementation specification is Required, it is so stated in the policy or procedure and must by implemented. If an implementation specification is addressable, the word "Addressable" appears in the policy or procedure.
    c. If a Security Standard includes Required implementation specifications, CEHS will implement the specification. When a Security Standard includes Addressable implementation specifications, CEHS will assess whether the implementation

specification is a reasonable and the appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting CEHS's confidential or sensitive electronic data, including protected health information; and

i. Document why it would not be reasonable and appropriate to implement the specification; and
ii. Implement an equivalent alternative measure that is reasonable and appropriate.

4. Exceptions:

Exceptions to any security policy or procedure must be documented using the Security Policy Exception Form. (See Attachment 101 A- Security Policy Exception Form). Exceptions should be rare and will not be granted unless it is for an "Addressable" implementation specification.
The following procedure defines the process for the review and approval of exceptions security policies, standards, guidelines and procedures:

A Clinic Director seeking an exception must assess the risks that non-compliance causes CEHS resources and business processes. If the manager believes the risk is reasonable, then the manager prepares a written request describing the risk analysis and request for an exception. NOTE: The only reasons that justify an exception are when compliance adversely affects business objectives or when the cost to comply offsets the risk of non-compliance.

The risk analysis should include:

a. Identification of the threats and vulnerabilities, how likely each is to occur, and the potential costs of an occurrence.
b. The cost to comply.
c. Request for Security Exception Form.

Submit the request for exception to the HIPAA Privacy Officer. The PO may recommend that other areas such as the Data Steward's(s), IT personnel and or the Information Security Office review certain requests and decisions. The PO will gather any necessary background information and approve or deny the request.

The requesting manager will be notified of the decision to approve or deny. All requests for exception will be retained by the Privacy Officer and are valid for a one-year period. Annually, any approved exception will need to be reviewed by the requesting manager who must determine whether the conditions that justified the original exceptions are still in effect. If the conditions have substantially changed, a new request for exception must be submitted. Where little has changed, the review process may be shortened as recommended by the Privacy and/or Security Officer.

5. Maintenance

All security measures adopted by CEHS and implemented to comply with the Security Standards and implementation specifications must by reviewed and modified as needed

to continue provision of reasonable and appropriate protection of confidential or sensitive data, including ePHI.

VI. STATE LAW PRE-EMPTION

The CEHS Security policies have been prepared for the purpose of satisfying the Security regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996 and does not take into account any state law requirements. Section 160.203 of the HIPAA regulations provides that the Federal Security regulations generally pre-empt contrary state law requirements. However, there are certain identified situations in which state laws are not preempted, including, without limitation, situation in which a state law related to the security of health information is more stringent that the corresponding Federal Security requirement. In such case, the more stringent state laws continue to apply in that state. Utah State Laws in regards to health information are under code R380 and can be found at: http://www.rules.utah.gov/publicat/code/r380/r380-250.htm

VII. ATTACHMENTS

101 A Security Policy Exception Form

VIII. REFERENCES

45 CFR §164.306

HIPAA Privacy Policy 100

101 Attachment A

Security Policy Exception Form

Location (Building/Room #):	
HCC Name:	
HCC Clinic Director:	
Date Initiated:	
Description of Exception:	
Risk Assessment – Indicate below the system(s) and application(s) affected and the impact to CEHS, the health care components and CEHS's system(s) for failure to comply with the CEHS Policy and Procedures. (NOTE: The impacts should be described in financial terms, where possible. Include subjective impacts if they are significant. In the risk assessment, include any compensating controls in place to mitigate the risk of non-compliance. Additionally, indicate the cost to implement the policy, if possible.)	
Operational History (For Installed Applications or Systems)	

Has any non-compliance resulted in significant operational control problems during the past year?	YES	NO
Has any operational control problems resulted in loss of financial data or assets?		
Have there been any audit recommendations or citations within the last year?		
Provide detail(s) if any of the above responses are "YES"		

List all of the known available options that would result in CEHS Policy or Standard compliance:

Requestor Signature: _____ **Print Name:** _____ Date: _____		
Explanation (Include what is approved or denied):		
Review Date: _____	**Approved**: (CEHS PO) _____	**Denied:** (CEHS PO) _____