POLICY INFORMATION

Document # **1000**	Title: **Contingency Plan**	Print Date: **10/24/2016**
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: 11/8/2016

I. POLICY STATEMENT

In order to safeguard EPHI, CEHS and the Health Care Component (HCC) must make efforts to plan for operational continuity in the event of an emergency or disaster.

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 (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

Through a combination of preventative and recovery controls and processes, CEHS disaster and emergency response procedures will seek to reduce to an acceptable level the risk to the confidentiality, integrity and availability of EPHI by developing a Contingency Plan. The Contingency Plan shall include:

- Disaster Recovery Plan
- A Data Back Up Plan
- Emergency Mode Operation Plan
- Testing and Revision Procedure
- Applications and Data Criticality Analysis

1. **Disaster Recovery Plan (Required):** CEHS Security Officer or his/her designated official shall establish, document and implement procedures to restore any loss, corruption, or damage of data due to an emergency or disaster on all systems that contain EPHI. The disaster recovery plan should include:
    a. The conditions under which the plan may be activated.
    b. HCC workforce member roles and responsibilities in executing the Disaster Recovery Plan.

c. Recommended procedures that contain the actions to be taken to restore EPHI, and to return EPHI to normal operations, within a defined time frame.
d. Documented order in which EPHI will be restored and the EPHI systems will be returned to operation.
e. Documented reporting and notification procedures to the CEHS Security and/or Privacy Officer(s), the HCC IT system administrator and other designated workforce members.
f. In the event of a disaster or other emergency, documented procedures for permitting appropriate specified workforce members physical access to the HCC facilities, and to any backup media on which EPHI is stored whether it is onsite or offsite, in order to carry out the recovery plan.
g. Documented procedures that specify how and when the plan will be tested and maintained.

2. **Data Backup Plan (Required):** Each HCC will take reasonable and appropriate steps to back up and store EPHI stored on EPHI Systems and to create exact and retrievable copies of EPHI. Each HCC will create and implement a documented and detailed plan for creating and maintaining backup data from all electronic media associated with EPHI that:
    a. Defines who is responsible for taking reasonable steps to ensure the backup of EPHI.
    b. Defines a backup schedule.
    c. Specifies the EPHI systems that are to be backed up.
    d. Defines where backup media is to be stored and CEHS workforce members who may access the stored backup media.
    e. Defines restoration procedures to restore EPHI from backup media to the appropriate EPHI systems.

    Each HCC will implement a backup procedure that will:
    a. Generate up-to-date copies of EPHI that can be recovered in the event that EPHI systems are damaged by or during a disaster or other emergency.
    b. Complete periodic testing of its restoration procedures for EPHI systems to confirm the effectiveness of those procedures and that the EPHI can be restored in the time set forth in the HCC's Disaster Recovery Plan.
    c. Document the retention period for backup media that contain backup copies of EPHI.
    d. Store backup copies of EPHI.
    e. Provide access to authorized workforce members to the backup copies.

3. **Emergency Mode Operation Plan (Required):** Each HCC will implement a documented and detailed Emergency Mode Operation Plan designed to allow the continuation of critical operations processes, while permitting necessary access to and use of EPHI, during and immediately following an emergency or disaster. The Emergency Mode Operation Plan will:

a. Define and categorize reasonably foreseeable emergencies that could have an impact on the confidentiality, integrity, and availability of EPHI systems.
b. Include a procedure for the HCC to follow during and immediately following an emergency that outlines how the HCC will maintain security processes and controls to ensure the confidentiality, integrity and availability of EPHI.
c. Include a procedure authorizing CEHS workforce members to enter the HCC and any off-site location where backup storage media are stored to maintain the security process and controls that protect the confidentiality, integrity, and availability of EPHI while the HCC is functioning in emergency mode.
d. Identify and document processes and controls that protect the confidentiality, integrity, and availability of EPHI while CEHS is functioning in emergency mode.

4. **Testing and Revision (Addressable):** The HCC in conjunction with the system administrator will take reasonable and appropriate steps to perform testing of its Contingency Plan and making necessary revisions on a periodic basis.

5. **Applications and Data Criticality Analysis (Addressable):** The HCC in conjunction with the system administrator will assess the relative criticality of specific applications and data in support of other contingency plan components.

V. ATTACHMENTS

N/A

VI. REFERENCES

45 CFR §164.308 (a)(7)(i)

45 CFR §164.308 (a)(7)(ii)(A)

45 CFR §164.308(a)(7)(ii)(B)

45 CFR §164.308(a)(7)(ii)(C)

45 CFR §164.308(a)(7)(ii)(D)

45 CFR §164.308(a)(7)(ii)(E)