**The College of St. Scholastica**

**HIM 6545 CORPORATE COMPLIANCE IN HEALTHCARE**

**HIPAA Contingency Planning**

**Purpose:** This assignment is intended to provide you with an understanding of the HIPAA Requirements for a Contingency Plan for a Covered Entity of Business Associate. It also will provide you with the opportunity to learn and understand the HIPAA Audit Protocol published by the Department of Health and Human Services.

**Activity:** Review a current HIPAA Contingency Plan, evaluate the requirements under the HIPAA Security Rule and the HIPAA Audit Protocol for the Contingency Plan, and update the Contingency Plan to meet the requirements of the HIPAA Regulations and the HIPAA Audit Protocol. This will also become part of your final project for the course.

**Instructions:**

1. Review the following
   1. Chapter 11, Pages 322 – 325 in the Oachs & Watters Book (2016)
   2. HIPAA Security Regulations - 164.308(a)(7) (164.308(a)(7)(ii)(A) to 164.308(a)(7)(ii)(E)) - <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf> (page 65)
   3. HIPAA Security Series – Administrative Safeguards, Contingency Plan – pages 19 – 22 <https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf>
   4. HIPAA Audit Protocol for 16.308(a)(7) - <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/protocol/index.html?language=es>
2. As identified in the Final Project Use Case, you are the new Compliance Officer at Grace University Hospital and have been given the responsibility to ensure that the current HIPAA Contingency Plan (attached below) meets the requirements specified in the HIPAA Security Rule as well as the HIPAA Audit Protocol that was published in 2016 by the Department of Health and Human Services.
3. Below is the current HIPAA Contingency Plan that your organization has established. It was last updated on 1/10/2014.
4. Since then, your organization has added 2 new systems that store protected health information
   1. Dictation System – Dictaphone – stored on Local Server #1, Backed up daily to unencrypted tape that is stored in the main office in a safe
   2. Electronic Collections Database – cloud based system, Backed up by vendor daily to a secure off-site solution
5. For this assignment you will:
   1. Review the current HIPAA Contingency Plan below to evaluate if any components are missing based on the HIPAA Security Rule and the HIPAA Audit Protocol
   2. Review the current status of the backup processes for the organization
   3. Develop an updated HIPAA Contingency Plan to meet the requirements of the HIPAA Security Regulations and the HIPAA Audit Protocol
   4. Evaluate current Contingency Plan Processes to determine if any changes need to be made
   5. Ensure that the two new systems that store and maintain protected health information are added to the contingency plan as appropriate
6. Deliverables for this assignment:
   1. An updated HIPAA Contingency Plan (this will become part of your final assignment)
   2. A Summary Document of what was missing from the current HIPAA Contingency Plan (i.e. define exactly what you changed, added, or updated). Attach this as a separate document in an outline format. Specifically list out the missing pieces to the contingency plan in an outline format including where your source of the information was from (HIPAA Audit Protocol, HIPAA Security Series, or HIPAA Security Regulations)
      1. Example: Contingency Plan is missing the individual responsible for the Contingency Plan – HIPAA Audit Protocol
   3. Finally, identify specific recommendations that you would make to the contingency plan process that would enhance the process to better protect and preserve the confidentiality, integrity, and accessibility of the protected health information and how would that enhance security.
      1. Example: Off-site backup solutions for Local Server #1 and Local Server #2. This would allow for better physical security of the backups in case of a local disaster at this Organization.

Information about Your Organization’s data:

Your organization currently has an electronic health record, a lab information system, a radiology information system, a dictation system, and a collections database. The organization is currently running 2 local servers that maintain most of the system that creates, stores, transmits, and maintains protected health information. In addition, protected health information is being stored on a file server located on Local Server #2 as well as being transmitted through e-mail, which is locally hosted on Local Server #1. Please see below for more details:

* Electronic Health Record – stored on Local Server #1, Backed up daily onto an unencrypted hard drive (entire server – Local Server #1) that is stored in the office of the IT Manager. Monthly a backup is made and brought to a safety deposit box at the local bank (Electronic Health Record Only).
* Lab Information System – Stored on Local Server #1, Backed up daily onto an unencrypted hard drive (entire server – Local Server #1) that is stored in the office of the IT Manager
* Radiology Information System – Stored on Local Server #2, , Backed up daily onto an unencrypted hard drive (entire server – Local Server #2) that is stored in the office of the IT Manager in a locked safe
* File Server –Stored on Local Server #2, Backed up daily onto an unencrypted hard drive (entire server – Local Server #2) that is stored in the office of the IT Manager in a locked safe
* Dictation System – Dictaphone – stored on Local Server #1, Backed up daily to unencrypted tape that is stored in the office of the IT Manager in a locked safe
* Electronic Collections Database – cloud based system, Backed up by vendor daily to a secure off-site solution

|  |  |
| --- | --- |
| Your Organization | HIPAA Policy  Contingency Plan |
| Effective Date: April 20, 2005 | Reviewed/Updated Date: January 10, 2011 |
| Policy Owner: HIPAA Security Officer |  |

**Policy:**

In the event that the systems that This Organization uses for managing day to day operations pertaining specifically to protected health information become unavailable, a plan of action to continue with the day to day operations of the organization are defined. The contingency plan for This Organization system will focus on data backup, disaster recovery, emergency mode operation plan, and testing and revision.

**Data Back Up Plan:**

1. The systems that use, store, and maintain ePHI for This Organization mostly stored on local servers.
2. The Organization has two local servers that house the majority of the systems:
   1. Local Server 1
   2. Local Server 2
3. Local Server #1 and Local Server #2 are both backed up daily and stored on unencrypted hard drives in the IT Manager’s office within a locked safe.
4. One a monthly basis, a backup of the electronic health record databased is completed to an unencrypted flash drive that is stored in a safety deposit box at the local bank
5. The IT Manager is responsible for all successful backups to the systems and local servers.
6. If there is a concern with the backup process, the IT Manager will work directly with the HIPAA Security Officer.

**Data Recovery Plan:**

1. In the event of data loss, the IT Manager and HIPAA Security Officer will work together for data restoration
2. Data restoration will occur from the most recent back up of the failed server
3. Once the device (server) is back up and function, the IT Manager and HIPAA Security will work together to restore the systems and data to the server.
4. The Electronic Health Record will always be the first system to be restored as it is the most valuable to the organization.
5. Once the Electronic Health Record is restored, an analysis of the integrity of the data and information will be taken based on the printed schedule from the previous day.
6. After the validation of the information from the Electronic Health Record, the remainder of the systems will be restored in the following order:
7. After each system is restored, there will be a process of validation of the information prior to moving on to restoring the next system
8. Data restoration will take approximately 5 – 10 hours.
9. A log will be kept of the entire data restoration process, including an issues that came up in the process.

**Emergency Mode Operation Plan:**

1. In the event that an unplanned downtime occurs, the HIPAA Security Officer becomes the lead contact for the emergency mode operations and physical contingency plan.
2. If the event of an event where This Organization’s systems are not available, communication will be given by leadership at each location within the facility.
3. Documentation of patient’s visit will be done on paper and kept within the temporary records in each area of the clinic.
4. The Leadership in the Clinic area will be responsible for ensuring documentation is being successfully completed on paper and stored appropriately.
5. This Organization will continue to monitor and evaluate the current downtime and give estimates expected down time internally to workforce members.
6. If it is determine that there is any type of risks to patients due to the emergency, This Organization reserves the right to cancel patient appointments.

**Testing and Revision Plan:**

1. This Organization will regular test the recovery plan to assure that it is appropriate and meets business expectations
2. After testing of the contingency plan, if revisions are needed, This Organization will promptly make the changes
3. If changes are made, proper training and updating awareness to the workforce will be conducted.
4. This Organization will maintain documentation of testing and revisions to the contingency plan for 6 years.

**HIM 6545 CORPORATE COMPLIANCE IN HEALTHCARE**

**HIPAA Contingency Planning – Grading Rubric**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Purpose**: This assignment is intended to provide you with an understanding of the HIPAA Requirements for a Contingency Plan for a Covered Entity of Business Associate. It also will provide you with the opportunity to learn and under the HIPAA Audit Protocol published by the Department of Health and Human Services. | | | | | | | |
| **Grading Rubric Possible** | | | | | | | |
| **Criteria** | **0** | **1** | **2** | **3** | **4** | **5** | **Points**  **60** |
| *Evaluation of Contingency Plan*   * Summary of missing components of the HIPAA Contingency Plan * Identification of the Source of Information * Critical Evaluation Skills of Regulations and HIPAA Audit Protocol * Minimum of 10 Missing Components of the HIPAA Contingency Plan | No logistical requirements present | 1 requirement present | 2 requirements present | 3 requirements present | 4 requirements present | ALL (5) requirements present | Points x 3 |
| *Creation of a Contingency Plan*   * Addition of missing information to the HIPAA Contingency Plan * Updating the systems to include the 2 new systems * Adding the missing sections of the HIPAA Contingency Plan * Ensuring that the HIPAA Contingency Plan meets expectation of the HIPAA Security Rule * Ensuring that the HIPAA Contingency Plan meets expectation of the HIPAA Audit Protocol | No content requirements are addressed | Content requirements are vaguely addressed | 2 content requirement is sufficiently addressed | 3 content requirements are sufficiently addressed | 4 content requirements are sufficiently addressed | ALL areas of content are thoroughly addressed | Points x 4 |
| *Recommendation for Enhancements to the Contingency Plan*   * A minimum of 6 recommendations to the Contingency Plan * Explanation on the reason for the enhancement * Explanation on how the enhancement will impact the security and protection of the patient data * Critical Evaluation Skills of requirements of protection of patient information | No content requirements are addressed | Content requirements are vaguely addressed | 1 content requirement is sufficiently addressed | 2 content requirements are sufficiently addressed | 3 content requirements are sufficiently addressed | ALL areas of content are thoroughly addressed | Points x 2 |
| *Organization & Comprehension*   * Logical sentence structure * Good transitions between topics * Information synthesized from all sources * Thorough comprehension * Writing clarity (including proper grammar / spelling, APA style) | Shows no comprehension of assignment; disorganized; lack of synthesized information from chosen sources | Only 1 area of organization and comprehension are sufficiently met | 2 areas of organization and comprehension are sufficiently met | 3 areas of organization and comprehension are sufficiently met | 4 areas of organization and comprehension are sufficiently met | ALL areas of organization and comprehension are sufficiently met |  |
|  |  |  |  |  |  | **Total** |  |