

**HEALTH INFORMATION BREACH**
**POLICIES, PROCEDURES AND GUIDELINES**

Title/Subject: **HIPAA: Breach Response**

Applies to: ☒Information Technology ☒Human Resources ☒Full Time Employees ☒Part Time Employees ☒Contractors

Effective Date of This Revision: September 1st, 2018

Contact for More Information: Security Operations Center

☐Board Policy ☒Administrative Policy ☒Procedure ☒Guideline

---

**BACKGROUND:**

Fantastical Unicorn Staffing Services[1] (FUSS) provides health insurance coverage for more than 500 employees. As an employer with an employee **health plan** for more than 500 employees, FUSS is a **covered entity** that must comply with the Health Insurance Portability and Accountability Act (HIPAA); Code of Federal Regulations (CFR) 45 C.F.R. Part 160, Part 162, and Part 164. As such, FUSS must comply with HIPAA regulations and safeguard the **protected health information** of FUSS employees. In the event of a health information security breach, a **breach report** must be filed. This policy and procedure guidelines describes which circumstances do and do not require the filing of breach report. Actions herein described are to be implemented to minimize or obviate, make unnecessary, the requirement of filing a breach report. If the circumstances require the filing of a breach report, the necessary actions required to file a breach report are enumerated here.

**PURPOSE:**

This policy and procedure guidelines describes under which circumstances a "breach report" is required to be filed and; how to a file a "breach report" with the U.S. Department of Health and Human Services, Office of Civil Rights (OCR). This document does not cover the concommitant reporting required for other information-sharing and analysis organizations (ISAOs) such as notifiying the Federal Bureau of Investigation (FBI) and the Department of Homeland Security (DHS) Assistant Secretary for Preparedness and Response. Reporting to the FBI and DHS is covered in FUSS document SOC-HI-158. Reporting of breaches to local and State police is covered in FUSS document SOC-HI-157. How a breach is identified is covered in FUSS document SOC-CY-485.

A breach report must be completed online on the HHS web site. The fields of the breach reported are listed below and highlighted. The required fields that must be completed are provided below. The director of the Security Operations Center (SOC) must review this document prior to filing a breach report.

**DEFINITIONS:**

The HIPAA Security Rule defines a "**security incident**" as the attempted or successful unauthorized access, use, disclosure, modification, or destructions of information or interference with system operations in an information system.

**Protected Health Information (PHI)** includes all individually-identifiable health information except for employment records, records covered by the Family Educational Rights and Privacy Act (FERPA), or information about individuals deceased more than 50 years. PHI includes any health information that relates to the care or payment for care for an individual. For example, treatment information, billing information, insurance information, contact information, and social security numbers.

---

1 Any relationship to any unicorns fictional or non-fictional, alive or dead, is purely coincidental.

A **business associate** includes any vendor that creates, receives, maintains, or transmits protected health information (PHI) for or on behalf of a HIPAA covered entity. This includes vendors that have access to PHI to provide IT-related services to the covered entity.

The Cybersecurity Information Sharing Act of 2015 (CISA) describes cyber threat indicators as information that is necessary to describe or identify: malicious reconnaissance; methods of defeating a security control or exploitation of a security vulnerability; a security vulnerability; methods of causing a user with legitimate access to defeat of a security control or exploitation of a security vulnerability; malicious cyber command and control; a description of actual or potential harm caused by an incident; any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or any combination thereof.

An **actionable breach** is a breach in which data was actually stolen and/or compromised. Also, actionable breaches include repeated attempts at breahces even though data was stolen. Actionable breaches requires following the procedures described in the procedure section of this document.

An **unactionable breach** is a breach in which data was not stolen or; the data stolen was encrypted. Unactionable breaches do not require reporting or remedial action.

A **DMZ** is a physical gap between data and the internet. For example, a database does not reside on a web server. Rather, the data resides on a separate hard drive that only the web server can access. This way, the data is not directly accessbile from the internet.

A **dump** or **data dump** is the indiscriminate, quick downloading or copying of data, from memory, a region of storage or an entire storage device, simply to copy data and not for processing purposes.

In this document, **keys** refers to **electronic encryption keys** and **physical keys** refers to physical keys made of metal for physical locks to filing cabinets, drawers, door handles and other physical locks.

**Substitute Notice** is an alternate form of notification to an individual whose PHI has been breached or stolen and can not be contacted with the current snail mail address on file. Such individuals may be notified by telephone, email or by a link provided on the **Covered Entity's** web site.

**POLICY:**

**All PHI is encrypted with cryptographically strong encryption.** No encryption algorithm that may be defeated with a brute force attack is permitted. Key size must be a minimum of 1024 bits. The encryption method must use randomness and alternating outputs. The algorithm must comply with the NIST Cryptographic Standards and Guidelines Development Process (NISTIR 7977).

**All PHI is encrypted and maintained in separate drives with DMZs.** No PHI is located on web servers. Data drives with PHI are not directly accessible from the internet.

**All encryption keys are kept in-house.**

**All encryption keys adhere to very strong password procedures.** See User Management Documentation SOC-UM-064, Password Rules section.

**Only operators and system administrators who require keys to PHI, will have keys to PHI databases or drives.**

**No one with a criminal conviction within the past 10 years will have access to keys.**

**Passwords or keys must be written down in 3" x 5" notebooks (password notebook) provided by the SOC and kept in locked filing cabinets or desk draws.** All password notebooks are to be hardcover bound. Wirebound password notebooks are not to be used.

**Pages are not to be ripped out of a password notebook.** Expired passwords are to be crossed off and new passwords written in. If pages are ripped out of a notebook, a potential breach is assumed but, not report needs to be filed. If pages are ripped out of a notebook and concurrently, there was a data dump, then a breach is assumed and report must be filed. In either event, all passwords must be changed. If the identity of the person having ripped the page out is unknown, then, the locks securing the notebook must be changed. Ripping a page out of a password notebook will come with a warning. Three warnings for ripping out a page from the password book is grounds for dismissal.

**Expired notebooks with passwords are to have their pages cross shredded and the remains burned.**

**Passwords may not be copied to personal electronic devices such as cellphones or tablets**. Only authorized personnel will have access to the physical keys to the filing cabinets or desk draws securing notebooks with a record of a key.
**Passwords may not be copied to Post-Its and attached to computer screens.** Doing so, is considered a serious security violation. An initial offense will come with a warning. Three offenses within a year are grounds for dismissal.

**All databases with PHI will be encrypted.**

**All PHI data uploaded to any cloud service, will be encrypted before uploading and; the keys will remain exclusively on FUSS premises.**

**The Security Operations Center (SOC) will monitor all network traffic, cloud activity and attempted accesses to disk drives or data storage devices or services with PHI.** If access to a drive or data source with PHI data is attempted from an unauthorized location or actor, the SOC will flag the attempted access as a "**Possible PHI Breach**" and investigate. After a thorough investigation, breaches will be classified as either actionable or unactionable.

**If PHI has been accessed in an unauthorized manner and the PHI is encrypted and; the keys have not been compromised; then, the breach is unactionable.**

**If PHI has been accessed in an unauthorized manner and the PHI is not encrypted or; the keys have been compromised; then, the breach is unactionable.**

**Each service provider that may potentially have a breach, e.g. a cloud provider or ISP, must supply a physical address for their SOC as well as a designated security agent with the security agent's email.** This information is to be written into any purchasing and/or service agreements with that provider. FUSS must be notified in writing of any changes to the physical address of the SOC, the name of the security agent, the telephone number of the security agent and the email address of the security agent.

**PROCEDURE:**

All employees who suspect that their PHI has been altered without their consent or; have lost their password to access PHI, are required to notify the SOC immediately and describe the circumstances.

If an actionable breach has occurred, which affects fewer than 500 individuals then; only the individuals involved need be notified of the breach.

OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches unless the information was encrypted by the entity at the time of the incident. For FUSS to consider encrypted data theft unactionable, the data must be encrypted with cryptographically strong encryption. In addition, the security of the keys to PHI data may not be compromised. If the SOC determines that neither the encryption nor the keys were compromised, then, a breach report need not be filed.

If the SOC determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach, then, a breach report need not be filed.

If an actionable breach has occurred, which affects all employees or more than 500 individuals, then; a report must be filed with OCR within 60 days of the breach. In addition, all affected individuals and the media must be notified of the breach, unless a law enforcement official has requested a delay in the reporting. Also, a report must be filed electronically on the OCR portal.

Filing a report with the OCR involves logging on to the OCR portal at the following web address: https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true

Have the following information prepared to file the report:

Is this an initial report? Y/N
If this is an addendum report, have the **breach tracking number** from the initial filing of the incident report.

Of the possible options select one of the two following: either "Covered Entity" or "Covered Entity filing because your Business Associate experienced a breach." If a breach occurred on in-house computers and data storage devices, select "Covered Entity." If the breach occurred on a cloud service but, not due to the internal operation of the cloud service, select "Covered Entity." If the breach occurred on the internal operations of a cloud service, select "Covered Entity filing because your Business Associate experienced a breach."

Under no circumstances should a breach be filed as "a Business Associate who experienced a breach, and filing on behalf of a Covered Entity."

*The name of the Covered Entity:* Fantastical Unicorn Staffing Services.
Do not use abbreviations. Write out the company name in full.

*The type of Covered Entity:* Health Plan

*Street Address 1:* 1 Main Street

*Street Address 2:*
Leave Blank. Do not write anything in this space.

*City:* La Laland
*State:* Pennsylvania

*Zip:* 58962

*Covered Entity Point of Contact Information*
The head of the SOC is the point of contact.
Give the first name, last name, email and phone number of the point of contact.
Only a work phone is to be given.

"*If "Are you a Business Associate who experienced a breach, and are filing on behalf of a Covered Entity" was selected*" – This is option should NOT be filled out. There is no such applicable circumstance.

"*If "Are you a Covered Entity filing because your Business Associate experienced a breach" was selected: Covered Entity: Please provide the following information.*" – Only if the breach occurred in conjunction with a cloud provider or an ISP, then this option should be selected.

*Name of Covered Entity*:
Use the name of entity only. Do not use the name of its representative, abbreviations, or acronyms.
*Type of Covered Entity:* Select "Health Plan"

*Street Address 1:* 1 Main Street

Street Address 2: Leave Blank. Do not write anything in this space.

*City:* La Laland
*State*: Pennsylvania

*Zip*: 58962

*Covered Entity Point of Contact Information*
The head of the SOC is the point of contact.
Give the first name, last name, email and phone number of the point of contact.
Only a work phone is to be given.

*Business Associate*
*Name of Business Associate:*
*Street Address Line 1:*
*Street Address Line 2:*
*City*:
*State*:
*ZIP*:
For the name of Business Associate use the full name. Do not use abbreviations or noacronyms.
For the address of the Business Associate, give the address of the SOC designated in the service level agreement with the vendor.

*Business Associate Point of Contact Information*
*First Name:*
*Last Name:*
*Email:*
*Phone Number:*
*Work*
For the name, email and phone number of the Business Associate, give the name of the security agent in the Business Associate's SOC that is designated in the service level agreement with the vendor. Specify that a work phone number is being given. Make sure to include the area code in the phone number.

BREACH Information Screen
*Breach Affecting:*
Select how many individuals were affected by the breach.
Select *500 or More Individuals*
Do not select *Fewer Than 500 Individuals*

*Breach Dates:*

*Breach Start Date:*
*Breach End Date:*
Give the start date.
If the breach is no longer occuring, give the end date of the breach.

*Discovery Dates:*
*Discovery Start Date:*
*Discovery End Date:*
Give the start date when the breach was discovered.
Give the end date, if applicable, for when the breach was discovered.

*Approximate Number of Individuals Affected by the Breach:*
Supply the number of people affected by the breach.
If the entire employee database or billing database was downloaded, then the number of total employees in the database at the time of download, is to be used.

*Type of Breach*
Type of Breach has a drop down of options to select:

Hacking/IT Incident
Improper Disposal
Loss
Theft
Unauthorized Access/Disclosure

Select the appropriate option for the breach.

*Location of Breach:*
Locatin of Breach has a drop down of options to select:

Desktop Computer
Electronic Medical Record
Email
Laptop
Network Server
Other Portable Electronic Device
Paper/Films
Other

Select the appropriate option.

*Type of Protected Health Information Involved in Breach:*
Select the appropriate category (categories):

Clinical
Demographic
Financial
Other

Upon selecting a category for the type of PHI involved in the breach, select the specific kinds of data involved in the breach.

Clinical
- Diagnosis/Conditions
- Lab Results
- Medications
- Other Treatment Information

Demographic
- Address/ZIP
- Date of Birth
- Driver's License
- Name
- SSN
- Other Identifier

Financial
- Claims Information
- Credit Card/Bank Acct #
- Other Financial Information

Other

*Type of Protected Health Information Involved in Breach (Other):*
If *Other* is selected, specify the kind of data that was breached.
There is a 4,000 characters limit to the description.

*Brief Description of the Breach:*
Provide a brief description of the breach.
Include how the breach occurred. How the data was taken. What data was taken. How the theft of data was arrested as soon as the theft of data came to the attention of the IT dept.
There is a 4,000 characters limit to the description.

*Safeguards in Place Prior to Breach:*
None
Privacy Rule Safeguards (Training, Policies and Procedures, etc.)
Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)
Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

Select from the options available. "Security Rule Technical Safeguards" and "Privacy Rule Safeguards" should always be selected. If these options do not apply, select none and immediately notify the Director of Information Technology.

*Notice of Breach and Actions Taken:*
Supply the required information about notices and actions.

Give Individual Notice Start Date:
Give Individual Notice Projected/Expected End Date:

*Was Substitute Notice Required?*
• Yes
o Fewer than 10
o 10 or more
• No

Select "Yes" if substitute notice was required for any one at all.
Select the number of people for whom substitute notice was required. This will be either less than 10 individuals and; 10 or more if 10 more individuals required substitute notice.

*Was Media Notice Required?*
• Yes
o Select State(s) and/or Territories in which media notice was provided
• No

State if media notice was given. Select "**yes**" or "**no**."
If "**yes**" was selected, select the State(s) or Territories in which media notice was given.

*Actions Taken in Response to Breach:*

Adopted encryption technologies
Changed password/strengthened password requirements
Created a new/updated Security Rule Risk Management Plan
Implemented new technical safeguards
Implemented periodic technical and nontechnical evaluations
Improved physical security
Performed a new/updated Security Rule Risk Analysis
Provided business associate with additional training on HIPAA requirements
Provided individuals with free credit monitoring
Revised business associate contracts
Revised policies and procedures
Sanctioned workforce members involved (including termination)
Took steps to mitigate harm
Trained or retrained workforce members
Other

Select the appropriate actions taken.

*Describe Other Actions Taken:*
If remedial actions not listed, were taken and "**other"** was selected, describe for those actions.
There is a 4,000 characters limit to describing other actions.

*Attestation*
Only the director of the Security Operations Center is to sign the attestation. The head of the SOC is totally responsible for the accuracy and truth of all statements made on the breach report.