POLICIES AND PROCEDURES FOR PROTECTED HEALTH INFORMATION

Version	4.2
Date of Version	2022-10-21
Created by:	Josh Cash & Afolake Fanseu
Approved by:	Josh Cash
Confidential Level:	Confidential

HURON

Change History

Date	Version	Created by	Description of Change
2020-02-05	2.0	A. Fanseu	Clean up of the entire document
2021-02-26	3.0	A. Fanseu P. Hausken	Review and update of the entire document
2022-05-25	4.0	P. Hausken	Review and update of the
2022-10-18	4.1	A. Fanseu	Update of links
2022-10-21	4.2	J. Cash	Update contact information

HURON

Contents

1. Purpose and Target Audience

This document provides "how to" instructions for Huron personnel (Employees, Project Consultants, Officers, Directors, and Independent Contractors) Topics that will be covered are:

- How to encrypt emails.
- How to ensure that data is destroyed at the conclusion of the engagement.

This document applies to all personnel in all practices and corporate departments. Engagement Leadership should review this document with project team members at the beginning of each engagement that involve the processing of PHI[1].

2. Introduction

In an effort to maintain strong management and governance around PHI, the Corporate IT Department has implemented solutions that include policies and procedures for the management, transfer, and storage of PHI documents.

These solutions provide designated online electronic document libraries for you to store and manage your working PHI documents. This is to address:

- Simplifying management of PHI data
- Minimizing the storage of PHI on laptops and peripheral storage devices
- Providing protection of PHI files.

Maintaining the privacy and security of client information is critical to Huron's continued success. For these reasons, all Huron personnel must treat individual identifiable health information carefully and responsibly in accordance with the provisions of HIP AA and other State and Federal requirements.

3. Our Standards and Policies

Huron's Standards and Policies are related to the HIPAA requirements and are governed by our internal HIPAA Compliance Committee. Specific questions related to handling data should be directed to your specific project/engagement Compliance Coordinator, Chief Compliance Officer or the HIPAA Security Officer.

[1] Protected Health information (PHI), under the US Health Insurance Portability and Accountability Act (HIPAA), is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history.

4. Policies – Team Members & Other Personnel

At the beginning of each project, engagement leadership should remind team members of the importance of safeguarding PHI. See the Compliance Methodology for Healthcare Engagements.pdf for further details.

Huron personnel have a responsibility to:

- Comply with the HIPAA Compliance Program, Huron compliance policies regarding HIPAA and PHI and all policies and guidelines contained in this document regarding PHI
- Report any violations of these to the project compliance coordinator immediately
- Comply with all data protection policies
- Ensure that all PHI sent over the Internet is always encrypted before it is sent
- Destroy any PHI that you have (electronic or hard copy) from any previous clients unless you need the PHI to continue to perform work for that client
    - Shred documents when no longer needed – shredders or bins are required at client sites
- Avoid having any PHI on your laptop, cell phone or other portable Huron equipment whenever possible
- Include "PHI" at the beginning of the file name of all documents that contain PHI, and place such documents in a file folder that the name begins with the letters "PHI"
    - Document example: PHI CHI AP File 011110.xls
    - Folder example: PHI Files Jewish St Mary
- Do not use another person's login name or credentials to access client or Huron systems at any time.
- Lock your laptop with username/password when leaving it unattended
    - Hold Windows key and tap the L key.
    - Ctrl, Alt, Del then select Lock Computer
- Obtain privacy screens that limit viewpoint when traveling or working in open work areas
    - Contact IT Support if you need a privacy screen (provide your laptop model)
- Project team members must report lost or stolen technology immediately
    - Personnel must immediately notify IT Support, as required by Huron Electronic Communication and Use of Technology.pdf. Additional procedures may be required after loss/theft disclosure
    - If the equipment was stolen, the employee must also notify the appropriate police agency and provide a copy of the police report to Huron
    - Project team members must also immediately notify their Managing Director

5. Project Compliance Policies

During the life cycle of all our projects/engagements our exposure to PHI may occur. During the negotiations and acceptance of our Business Associate Agreement specific terms and conditions

are negotiated to determine the proper handling (Storage, Transfer, Disposal) of all Client-provided Data. All personnel need to be aware of these terms and conditions and abide by them for each engagement.

Project/engagement Compliance Coordinator or other designated compliance lead should review specific details with the project team on how to document, transfer, store, and dispose of PHI.

6. Project Compliance Coordinators Responsibility

Huron practices may designate an individual on each project/engagement to have the added responsibilities of being the project/engagement Compliance Coordinator to oversee and support personnel's adherence to Huron compliance requirements including HIPAA and PHI policies assigned at each engagement

- While Managing Directors retain ultimate responsibility for adherence to corporate policies by all project team members, they may delegate project compliance coordinator administrative tasks to other engagement leaders as appropriate
- Project compliance coordinators will be manager level or above, have at least six months' time in grade, and have a solid or above performance rating
- Engagement leadership should ensure that a new compliance coordinator is assigned to the project if the current compliance coordinator rolls off the project
- In cases of integrated projects, the integrated services engagement leader will serve as the overall project compliance coordinator and may delegate responsibility for individual practices to respective Managing Directors

Project Compliance Coordinator responsibilities include:

- Verify that that all engagement team members have completed Huron HIPAA Compliance training as well as Project HIPAA and PHI Training
- Conduct project-specific HIPAA and PHI training and document that all personnel receive compliance training
- Inform team members of any unusual requirements contained in the client Business Associate Agreement and remind team members of key privacy and security provisions
- Conduct periodic reviews of team member practices to ensure compliance; provide refresh training or new team member training as needed
- Review any reported or suspected project HIPAA or PHI violations and escalate appropriately to Huron Chief Compliance Officer and as appropriate to Client personnel.

7. PHI Breach Determination and Notification

Under regulations related to HITECH provisions of HIPAA, organizations may be required to notify individuals, the DHHS, and in some cases, the media, if the Covered Entity or a Business Associate (such as Huron) discovers a breach of unsecured PHI.

Notification is required if there is a breach and PHI is "unsecured"; notification is not required if there is a "breach" and PHI is "secured"

- PHI is secured if data is encrypted and encryption keys are kept separate from the data and the media on which the PHI is stored or recorded has been properly destroyed when it is no longer needed
- PHI in paper form is unsecured if removed from secured client facilities. Specific handling and management of non-electronic PHI needs to be documented for each project/engagement.

For Huron project purposes, a breach has occurred if PHI is accessed, used, or disclosed in a way that is not allowed under the HIPAA Privacy Rules or Huron HIPAA policies; and such access, use or disclosure compromises the security or privacy of the PHI

- Project team members who discover, believe, or suspect that PHI has been accessed, used, or disclosed in a way that violates the HIPAA Privacy Rules, must immediately report such information to the project compliance coordinator and MD
- The Managing Director must then immediately report such information to the Corporate Compliance Officer or Huron Legal Department
- The detailed policy on PHI breach determination and notification as well as the Breach Determination and Notification Process Steps can be found here.

8. Requests for Client PHI

Client PHI should only be requested if necessary, for your assigned task. The information that you should request should be for the minimum amount of data required. Data should be de-identified by the client when possible.

There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are two ways to de-identify information; either:

- A formal determination by a qualified statistician; or
- The removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is required, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.

However, any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. To qualify as de- identified data, all PHI must be removed and there must be no way to identify the individual even though all of the identifiers have been removed.

A de-identified data set may include a tracking or unique code or other numbering system, provided that:

- The tracking or unique code is not related to information about the individual; for example, the unique code cannot include the last four digits (in sequence) of the social security number

The re-identification methodology or method of applying the tracking or unique code is not disclosed to the data recipient

9. Unsolicited Receipt of PHI

If you have received inappropriate or misdirected PHI follow these steps:

- Do not open, print, download, forward or retain the unsolicited PHI
- Reply to the sender of the material that a PHI request was not made
  Delete or properly dispose of the PHI and notify the project Compliance Coordinator that this event has occurred

10. PHI (Paper and Electronic) Removal

- Shredders or shredding bins are provided on project sites for the destruction of hard copy PHI documents; Although strongly discouraged, hard copy PHI documents that are taken from client sites for work purposes should be properly shredded and disposed of or returned to the client site for destruction.
- Electronic files and email containing PHI should be deleted from Outlook files and inboxes, file directories on your laptop hard drive (C drive), USB/flash drives, and external hard drives as soon as it is no longer needed for the project.
  - Use Shift-Delete for a permanent removal of email messages.
  - Once the above is completed, you will also need to empty your recycle bin on your desktop
- Do not store PHI outside of your Microsoft OneDrive / work profile
- Do not use your Mobile Device to transfer PHI (i.e., texting) via messaging application
- If accessing PHI files from OWA (Outlook Web App), you will also need to clear your temporary internet files before emptying your recycle bin
  - Click “tools” “settings” and Delete “Temporary Internet files” from your local browser
- Emails containing PHI should never be moved outside the Microsoft Outlook application
- Voicemails containing PHI should be removed from your mobile device immediately
- Non-Huron issued devices must have encryption and password protection per contract/forms signed by subcontractors.

11. Approved Storage Locations for PHI

The following methods are acceptable for PHI storage:

Data storage during the engagement. Unless otherwise specified contractually:

- Electronic documents containing PHI should ideally remain on client servers.
- PHI sent from the client to an engagement team member should be stored securely in the engagement SharePoint PHI Library.
- PHI or other confidential information should never be placed on personal home computers or portable devices.
- Engagement team members should include "phi" in the file name of all documents that contain PHI, and/or place such documents in a file folder that contains the letters "phi". Designating data files in this manner will help ensure that personnel can locate and destroy all PHI when it is no longer required for work on behalf of the client.
- Team members should avoid storing PHI on a Huron-issued computer or laptop. If PHI is stored on a Huron-issued laptop, team members should regularly delete the PHI during the course of the engagement if no longer needed.
- Hard copy PHI must not be taken off-site, must remain secured during the engagement, and placed in locked shredding bins when no longer required.

Beyond permissions based security and SSL encryption technology, SharePoint protected libraries are secured with Microsoft's IRM (Information Rights Management) technology. IRM adds an additional layer of encryption and authentication to each downloaded document, restricting access to only the user that downloaded it. IRM will automatically add this protection to the following document types.

- The 97-2003 file formats for the following Microsoft Office programs: Word, Excel, and PowerPoint
- The Office Open XML Formats for Microsoft Office Word 2007, Microsoft Office Excel 2007, and Microsoft Office PowerPoint 2007
- Microsoft Office InfoPath Forms

Other document types are still allowed in these encrypted libraries but would not have additional IRM protection.

Note: IRM protected document libraries are not intended for large data files such as large data sets for import into database applications; designated file servers should continue to be the primary method for storage of these types of files.

Designated File Servers

For groups that work with large data files (>60 MB), or data files intended for database import, designated file servers will continue to serve as your primary storage solution. Contact your project/engagement compliance coordinator for specific designated file server access procedures.

Mashups Application

For Stockamp Product Services, client PHI is often needed and stored in client support requests. If necessary, to complete a request, storing PHI in a support ticket is acceptable.

Laptops

Encrypted laptops are not recommended and strongly discouraged for storing PHI files. If you use your laptop to download and work with PHI data, once work is complete, files containing PHI should be uploaded back to their primary storage repository, if necessary, and deleted off your laptop and empty your recycle bin.

Small Storage (USB Sticks/Drives/thumb drives) used as storage.

Encrypted thumb drives and external hard drives are also not recommended and strongly discouraged for storing or transferring PHI files. If used, as with laptops, once work is complete, files containing PHI should be uploaded back to their primary storage repository, if necessary, and deleted off of the device.

Huron's laptops have an external drive encryption mechanism that prompts employees to encrypt external drives when connected.

12. Approved Methods for Transferring PHI to Clients

Client Systems

- Utilizing client systems is the preferred method for transmitting client PHI.
- If the engagement team is assigned client email addresses, email messages that contain PHI or include PHI in an attachment should be sent from the **Huron employee's client email address** to client personnel as well as other Huron employees, project consultants or contractors **who also have a client email address.**

Microsoft Teams

- PHI can be shared and exchanged with clients and with other Huron team members within Microsoft Teams
- See the Controls for Sharing PHI in Teams below for detailed requirements

Microsoft Teams Huron to Huron Transmission

Use these controls when using Teams with another Huron employee.

	Files	Messages
Teams Chat	• Do NOT attach files with PHI to a chat. These files are stored in OneDrive, which is not an approved location for PHI. • Employees CAN share *links* to PHI files stored in PHI libraries over chat.	• Chatting PHI (e.g., account numbers) in the body of a chat between internal Huron users is permissible if all parties are authorized and have a business need to view the PHI data.
Teams Channels	• All PHI files should be stored in the PHI library in the SharePoint site associated with the Team. This ensures we are	• Do NOT post PHI in Teams channels messages because these messages

	using Information Rights Management. • Only users that have an approved business need should be granted access to the PHI library. • Teams site owners must ensure that access is immediately removed for users who no longer have a need. Additionally, Teams site owners are required to review access to the PHI library and Team every year.	last until the Team is deleted.

Microsoft Teams Huron-to-External Transmission

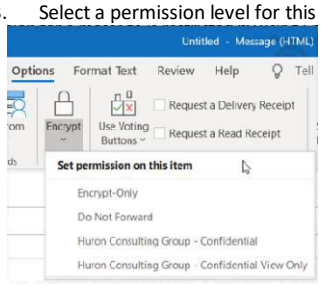
There must be a Business Associate Agreement (BAA) in place with any third party to share PHI. Additionally, these controls must be in place when using Teams to transmit and store PHI.

	Files	**Messages**
Teams Chat	• Same as Huron-to-Huron transmission	• Chatting PHI (e.g., account numbers) is permissible if all parties are authorized and have a business need to view the PHI data.
Teams Channels	• To collaborate with clients, you must set up a separate Team appended with [External] and request guest access to invite external people into that Team. This site must be finalized at the same time as the Huron-only Team. Click on Set up Teams with Guest Access for step by step information. • Files cannot be stored in the PHI library because the security controls would prevent external users from accessing files. Instead, store files in private Teams channels. • PHI files must be stored in a private channel in the external team called "PHI External," and the team owners must ensure only authorized people have access.	• Same as Huron-to-Huron transmission

	• Teams site owners must ensure that access is immediately removed for Huron and non-Huron users who no longer have a need. Teams site owners are required to review access to the Team and private channel each quarter. GRC will also work with Team owners to review access annually. • Guest users are automatically disabled after 60 days of inactivity, but this does not remove the requirement for team owners to remove people who no longer need access. • The " PHI External" channel must be deleted as soon as the engagement or project had been completed.	

Exchange Online Email encryption

- Exchange online enables internal users to securely exchange emails and attachments with clients.
- Exchange online email encryption secures the body of the message as well as any attachments.
- Exchange online has an attachment size limit of **35MB**.
- Outlook/ Outlook web access can be used to send secure emails.
    a. **How to Use Microsoft Email Encryption**
    You can use Email Encryption by including the **[secure]** or **[encrypt]** tags in the **subject line** of your email message.
    Alternatively, you can follow these steps.
        1. Open a new email message
        2. **Options** > **Encrypt**
        3. Select a permission level for this message



Transport Layer Security (TLS) Protocol

- Once set up by Huron IT, the TLS process automatically secures emails between client domains and Huron domains.

- The TLS Protocol should be considered on every engagement as a backup safety mechanism for sending PHI between client and Huron domains.
- Engagement Leadership should work with project sponsors to identify a client IT contact who can work with Huron IT to set up the TLS Protocol.
- Huron IT will provide the client with the 'eTLS request template' to identify the client contact and all applicable email domains.
- **Team members are still required to send PHI via secure messaging systems.** Even with a TLS Protocol in place, if a Huron team member sends PHI without using a secure messaging system, the team member should complete the Privacy Incident Reporting Form.

1. In the event **a Huron team member** transmits PHI in a manner other than one of the approved methods noted above, the team member responsible for that transmission must report the incident to Engagement Leadership immediately and the Privacy Incident Reporting Form must be submitted to the Chief Compliance Officer within twenty-four (24) hours of discovering the transmission.
2. In the event **the client** transmits PHI in a manner other than one of the approved methods noted above, the Huron team member that received the transmission must report the incident to Engagement Leadership immediately and the Privacy Incident Reporting Form must be submitted to the Chief Compliance Officer within twenty-four (24) hours of discovering the transmission.

3. Engagement Leadership should determine whether the engagement contract or BAA requires notification to the client of either event described in bullet point 1. or 2., noted above. If written notification to the client is required, the form Letter to Client of Potential HIPAA Compliance Issue should be used. See Section 4.1, below, for detailed reporting instructions.

13. Transferring Files between Huron personnel

Transferring files containing PHI between Huron team members on Outlook is acceptable (i.e., from a Huron email address to another Huron email address). Outlook has a limitation on the size of a file that may be transmitted of 50MB. If the file is larger than 50MB, Microsoft Teams should be used to transmit the file.

Small removable media including USB devices and CD's, or DVD's is strongly discouraged. Please utilize the above systems resources for transferring large client data sets.

Record Retention Policy for PHI

PHI data is only stored for the minimal duration of your project. As per client engagement protocol any PHI must be properly disposed at the end of the engagement if not sooner. This would include all data on secured storage locations and secured Databases.

PHI (electronic and other forms) and client provided materials are not considered Huron records and are not to be retained in any form at the close of any engagement.

At the end of the engagement, Engagement Leadership should review with team members how PHI and other confidential client information such as PII, Personal Data, or PI should be handled. Unless otherwise specified contractually:

- Electronic media containing PHI must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved. Redaction is specifically excluded as a means of data destruction. Contact IT GRC with any questions.
- The destruction requirement includes PHI or other data located in any file, email, Microsoft Teams site, or on a SharePoint server, unless Engagement Leadership specifically approves and documents the retention of that information as being required to support the continuation of services to the client.

If retention of PHI or other client data is essential to support the client after the end of the engagement, the engagement MD may approve retention of the information for up to six months, when all PHI/PII must be destroyed or returned without exception. This data should be stored so that it is accessible to the minimum possible number of employees.

If the engagement MD believes that Huron may need to access PHI or other client data in the future to respond to client requests, he/she may request retention from the client. PHI obtained to provide continuing service support to a client must be destroyed or returned immediately once it is no longer being used to support the client.

Paper, film, or other hard copy media must be shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed.

14. Current Huron Contacts

Chief Compliance Officer
Josh Cash, Joshcash@hcg.com, 312-212-6029

Chief Privacy Officer **TBD**

HIPAA Security Officer
Afolake Fanseu, afanseu@hcg.com 312-880-3599

Chief Security Officer
David Smiatacz, dsmiatacz@hcg.com, 312-880-3146

Corporate Information Technology (IT) Support
Peter Choi, pchoi@hcg.com, 312-880-5601

Corporate Information Technology (IT) Governance and Compliance
Safeer Hashmi Shashmi@hcg.com

Project/Engagement Compliance Coordinators

For each practice or corporate group contact your operations manager for specific individuals/contacts