Policies and Procedures for Electronic Protected Health Information (ePHI) and Personally Identifiable Information (PII)

Effective Date: April 10, 2012 Prepared by: Joe Raschke (IT)

Table of Contents

Purpose and Target Audience

This document discusses the policies of Huron and provide "how to" instructions for Huron personnel (Employees, Project Consultants, Officers, Directors and Independent Contractors) e.g., how to encrypt emails, and 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. Specific practices including Healthcare, Higher Education, and Legal Consulting should review this document at the beginning of each engagement that potentially can involve accessing, processing, or storage of ePHI or PII. These policies are written to communicate the technical guidelines and procedures of how to use Corporate IT Systems.

Introduction

In an effort to maintain strong management and governance around PHI and PII, the Corporate IT Department, with the guidance of the Corporate Compliance Committee and several practices and corporate departments, has implemented solutions that include policies and procedures for the management, transfer, and storage of ePHI and PII documents.

These solution provide designated online electronic document libraries for you to store and manage your working ePHI and PII documents and address:

- Simplifying management of ePHI and PII data
- Minimizing the storage of ePHI and PII on laptops, peripheral storage devices, tape libraries, and other mobile media
- Providing protection of ePHI and PII 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 heath information carefully and responsibly in accordance with the provisions of HIPAA, HITECH, and other State and Federal requirements.

Huron's Policies address the US Federal HIPAA and HITECH requirements. Specific questions related to handling data should be directed to our Chief Compliance Officer and your specific project/engagement Compliance Coordinator.

Policies
The Policies section below provides required processes while handling information related to identifying, handling, management and reporting ePHI and PII.

Procedures
The Procedures section below provides step by step instructions on utilizing the Technology tools that are available to you to implement the Policies. The procedures additionally can be accessed on our corporate iNet under various IT web pages.

Training
Periodic and ongoing compliance training is required for all personnel. The training related to handling ePHI and PII includes sessions on HIPAA Privacy and Security, HIPAA Updates and HITECH, Huron's Code of Business Conduct and Ethics, and Data Security Overview. Additional training is required for each engagement. Technical assistance with training is available by calling IT Support at 312-583-8776 or on the iNet Academy.

Policies – Team Member & Other Personnel

All Huron personnel assigned to each project/engagement are required to attend and document attendance at periodic HIPAA and protected health information project training.

Huron personnel have a responsibility to:

- Comply with the HIPAA Compliance Program, Huron compliance policies regarding HIPAA, PHI, PII as well as report any violations of these to the project compliance coordinator immediately
- Comply with all data protection policies
- Encrypt any mobile device that contains confidential data
- Ensure that all PHI sent over the Internet is always encrypted before it is sent
- Destroy any PHI or PII that you have (electronic or hard copy) from any previous clients unless you need the PHI or PII to continue to perform work for that client
- Avoid storing any PHI on your laptop, Blackberry, mobile phone, or other portable Huron equipment whenever possible – for current or previous clients
- Include "PHI" at the beginning of the file name of all documents that contain PHI, and place such documents in a file folder that's name begins with the letters "PHI"
  Document example: PHI CHI AP File 011110.xls
  Folder example: PHI Files Jewish St Mary
- Never use another person's logon name or credentials to access client or Huron systems at any time
- Use physical cable locks to lock down laptops at Huron offices and client sites
- Physically carry your Laptop with you at all times if you cannot securely tether your laptop with a cable lock to a secured desk or trunk of your vehicle
- 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 immediately following training if you need a privacy screen (provide your laptop model)
- Shred documents when no longer needed – shredders or bins are required at client sites
- Project team members must report lost or stolen technology immediately
  - Personnel must immediately notify IT Support, as required by Huron Use of Technical Resources policy. 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

All Company Policies are located on iNet at:
https://intranet.huronconsultinggroup.com/hr/policies/Pages/home.aspx

Project Compliance Policies

During the life cycle of all of our projects/engagements our exposure to PHI, PII, or ePHI 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 understand and abide by these terms and conditions for each engagement.

Please contact your project/engagement Compliance Coordinator or other designated compliance lead for specific details on how to document, transfer, store, and dispose of PHI and PII.

PHI or PII 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 to organizations outside of Huron **is required** if there is a breach and **PHI is "unsecured";** notification is not required if there is a breach and PHI is "secured"

- 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, which will determine what reporting requirements are applicable.
- The detailed policy on PHI breach determination and notification as well as the Breach Determination and Notification Process Steps are available on iNet at: https://intranet.huronconsultinggroup.com/hr/policies/Pages/home.aspx

Requests for Client PHI

Client PHI should only be requested if necessary for your assigned task. When requesting or sending PHI to a client you need to verify in written or verbal communications the expected protocol for the handling of the client PHI prior to transmission, including protocols for the request, transmission, handling, storage, and disposal of the PHI.

The information that you should request should be for the minimum amount of data required and that the data be de-identified data by the client whenever 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 apply the tracking or unique code is not disclosed to the data recipient

Unsolicited Receipt of PHI

If you have received inappropriate or misdirected PHI please follow these steps as required under Huron's HIPAA Compliance program; 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. Do not open or retain the unsolicited PHI.

PHI (Paper and Electronic) Removal

- Shredders or shredding bins are provided on project sites for the destruction of hard copy PHI documents; 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 personal 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
- Storage of ePHI on Blackberrys/Smart Phones is strongly discouraged. Do not store ePHI on your BlackBerry/Smart Phone
- Transfer of ePHI from BlackBerrys/Smart Phones is also strongly discouraged. DO not use your BlackBerry/Smart Phone to transfer ePHI
- 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 and voicemails containing PHI should be removed from Blackberry immediately
- Corporate IT Support or your PDA/Smartphone provider can provide instructions on how to set your device so deletions from your device will not also be deleted from Outlook when synching
- Non-Huron issued devices must have encryption and password protection per contract/forms signed by subcontractors
- The engagement MD may authorize retention of the PHI for a limited time period of up to 90 days. If PHI data needs to be retained after that time period, contact the Huron HIPAA Compliance Officer for approval

Approved Storage Locations for PHI

The following methods are acceptable for PHI storage:

Client Provided Solutions

The preferred method for PHI data storage including designated File Servers, Hard Drives, and Email is for the client to provide a storage solution for the project team. If this is not available, SharePoint IRM libraries should be your next selection.

SharePoint IRM Protected Document

SharePoint IRM protected document libraries will be created for each project or team in need of PHI storage. These libraries are restricted to Huron employees only and are suitable for PHI files <60 MB in size. IRM protected document libraries should be considered your first choice for PHI data storage if client provided storage is not available. Permissions to these libraries are controlled by Huron IT with approval by the project or team's Compliance Coordinator.

Beyond permissions based security and SSL encryption technology, SharePoint IRM 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 Huron Healthcare 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 & Periphery Devices
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, PII, or any confidential 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.

BlackBerrys and Smart phones should never contain PHI data. If PHI is received on such device it should be removed immediately.

Encrypt small storage devices and removable media with Huron approved tools encryption software tools – BitLocker and Credant.

Instructions on encrypting removable media are located on the iNet:
https://intranet.huronconsultinggroup.com/employee/technology/Pages/home.aspx

All other storage methods are deemed unacceptable unless otherwise approved by the Huron CIO

Blackberry and Smart Phones
Do not store PHI to your company issued Blackberry or smart phone. These devices are encrypted automatically and verified, but it is a best practice to not store any PHI on those devices.

CD and DVD Media
Do not store PHI on removable media unless you have verified that those devices are fully encrypted and comply with company it policies and procedures.

Approved Transfer Methods for ePHI

The following are deemed as acceptable methods for PHI transfer, meaning sending PHI from one person or system to another. Utilizing client systems – is the preferred method, data is not transferred, remains on the clients system. You need to confirm with your project Compliance Coordinator on the client approved solutions. These solutions should also be used for transferring data between disparate Huron employees, project consultants and independent contractors. Additionally before transmitting any PHI you need to verify both the sending and receiving parties and the expected data. If there is any discrepancy in the receipt of the data the data should be treated as an unsolicited receipt of PHI.

Secure Messenger

The Secure Messenger application is used to send encrypted emails and large file attachments to external/non-Huron parties/email addresses. This is a preferred solution since both the message and attachments are encrypted and address books can be self-maintained.

1. To login to the secure mailbox go to
   https://messenger.huronconsultinggroup.com
2. Enter your email address and Windows password to login
3. Compose email, etc.
4. The first time a recipient receives an encrypted email from a Huron user, they will be required to register and setup an account so they can view and reply to encrypted emails
5. The encrypted emails are stored on a Huron server
6. After the recipient registers, they will be able to view the email via a secure encrypted tunnel between the Huron server and their desktop
7. The recipient will not be able to forward encrypted emails to anyone except to a Huron email address
8. Messages are automatically deleted from the server after 60 days

For more details see the Secure Messenger Document located at:
https://intranet.huronconsultinggroup.com/employee/technology/Pages/home.aspx

Accellion Secure File (Secure Transfer Solution)

The Secure File transfer application allows for high speed transfer for larger data set. Up to 20 GB of data can be effectively and safely transferred between Huron and our clients. Attachments are encrypted and meet with our compliance Policies. Message subjects and the email text are not encrypted. If PHI transfer is only embedded in attachments this solution provides for the best performance and the address book can be self-managed. Files are automatically deleted after 30 days

For detailed instruction review the Accellion document located on the iNet.
https://intranet.huronconsultinggroup.com/employee/technology/Pages/home.aspx

PGP Encryption

PGP Encryption requires a special installation of software on individual laptops. Please contact Huron Support for licensing and installation specific instructions. 312-583-8776. Documentation is available on the iNet. https://intranet.huronconsultinggroup.com/employee/technology/Pages/home.aspx

Encrypted Email

Huron's Email system has encryption protocols enabled for a high level of secured transmission between our email system and most of our clients, though we do not rely on this as being sufficient. Additionally you can force the complete message to be encrypted by typing [encrypt] in the subject line.

To encrypt an email using Outlook, OWA, or Blackberry type **[encrypt]** in the subject line
Make sure there is a space before or after **[encrypt]** for the subject line
The **[encrypt]** text will be stripped from the email during processing

Directing a Huron Employee to a Storage Location
Please contact your project Compliance Coordinator for specific file server location

Transferring Files Between Huron Personnel

Encrypted Media, CDs, DVDs, Hard drives, USB devices as a transfer method
Small removable media including USB devices and CD's or DVD's is strongly discouraged. Please utilize the above systems resources such as Secure File transfer for transferring large client data sets.

- Mashups tickets
- Voicemail
  Do not use voice mail to transfer confidential information.
- Fax, Following Proper Protocol
  Do not use Fax to transfer confidential information

All other methods are deemed unacceptable unless otherwise approved by the Huron CIO.

Encrypted Media, CDs, DVDs, Hard drives, USB devices as a transfer Protected health information (PHI)
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.

For more information regarding PHI and our Compliance Department please follow the link below:
https://intranet.huronconsultinggroup.com/company/corpgroups/legal/complianceprograms/Pages/compliancedocuments.aspx?program=Compliance-HIPAA

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
For details related to Huron's Record Retention Policy for ePHI please refer to the corporate Legal department's web page:
https://intranet.huronconsultinggroup.com/company/practices/lc/servicelines/rim/Pages/home.aspx

Current Huron Contacts

Chief Compliance Officer
Ken Jones, kjones@huronconsultinggroup.com, 503-303-1141

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

Corporate Information Technology (IT) Support
Mike Abraham, SupIT@huronconsultinggroup.com, 312-583-8776

Corporate Information Technology (IT) Governance, Risk and Compliance
Joe Raschke, jraschke@huronconsultinggroup.com, 312-880-3519

Project/Engagement Compliance Coordinators
For each practice or corporate group contact your operations manager for specific individuals/contacts