# HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 ("HIPAA") COMPLIANCE PROGRAM

| | |
|---|---|
| Version: | V7.0 |
| Date of version: | October 2023 |
| Created by: | Compliance |
| Approved by: | Josh Cash, Chief Compliance Officer |
| Policy Owner: | Compliance |
| Confidentiality level: | Confidential |

## Table of Contents

## 1. INTRODUCTION AND PURPOSE

The Huron Consulting Group Inc. ("Huron") HIPAA Compliance Program addresses issues concerning the privacy and security of health information mandated in the Health Insurance Portability and Accountability Act of 1996, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH") (collectively defined as "HIPAA"). Huron's HIPAA Compliance Program (the "Program"), is an acknowledgment that an integral part of Huron's business involves accessing and using health information belonging to its clients. Further, the Program recognizes that an individual's identifiable information is subject to state and federal protections and is a matter of great sensitivity for Huron's clients as well as Huron employees.

Therefore, **maintaining the privacy and security of client information is critical to Huron's continued success.** For these reasons, all officers, directors, employees, agents, and independent contractors of Huron ("Huron personnel") must treat individually identifiable health information, referred to as "protected health information" under HIPAA, carefully and responsibly in accordance with the provisions of HIPAA, its implementing regulations and other State and Federal requirements.

Here are some key points to help in understanding the purpose and requirements of HIPAA.

- HIPAA provides certain standards for creating, storing, managing, transmitting, and disclosing Protected Health Information (PHI) designed to protect the confidentiality and security of the PHI. HIPAA applies directly to a Covered Entity ("CE"), (defined as a health plan, a health care clearinghouse, or a health care provider), and a business associate that creates, receives, maintains, or transits protected health information.
- PHI includes not only information that is electronically transmitted or stored (known as ePHI), but also PHI in all media, including electronic, written, and oral.
- Huron has implemented procedures designed to ensure that Huron will require clients to represent that they will obtain patient permission, as may be required, to allow Huron to receive and use PHI for Huron's payment and health care operations uses and disclosures. Huron will also ensure that appropriate Business Associate Agreements are executed. Huron employees working with Covered Entities are required to assist Huron in honoring the commitments that Huron makes in its Business Associate Agreements.
- HIPAA restricts how PHI can be used and/or disclosed to others. Huron may use and disclose PHI only in accordance with the provisions of a Business Associate Agreement ("BAA") and applicable law. Among other requirements, Business Associates are required to:
    - Restrict its uses and disclosures of PHI to those outlined in the BAA or as required by law,
    - Use or disclose only the minimum amount of PHI necessary to accomplish the intended purpose, and only as permitted or required by the applicable BAA,
    - Implement safeguards to prevent unauthorized uses and disclosures of PHI,
    - Report violations of the BAA to the Covered Entity,
    - Report breaches of PHI, or security incidents, to the Covered Entity,
    - Ensure that its agents and subcontractors who have access to the Covered Entity's PHI agree to the same conditions and restrictions that apply to the Business Associate,
    - Return or destroy all PHI received from the Covered Entity or created or received by the Business Associate on behalf of the Covered Entity and keep no copies.
    - The BAA must permit the Covered Entity to terminate the engagement contract if the Business Associate materially violates the contract.

The goals of the Huron HIPAA Compliance Program are 1) to provide guidance on the requirements of HIPAA so that Huron can maintain compliance with the Act and its BAAs, 2) to provide affected staff with the education and resources necessary to make the appropriate decisions regarding legal, professional and ethical obligations related to their role as consultants to health care providers and others involved in the health care industry, and 3) to monitor, audit and provide corrective mechanisms to ensure those obligations are met.

## 2. PROGRAM ADMINISTRATION

### HIPAA Compliance Committee and Officers

The HIPAA Compliance Officer, who is designated by Huron's Chief Compliance Officer, is currently Josh Cash. The Chief Compliance Officer designates Huron's HIPAA Security Officer, currently Afolake Olakanye. They are jointly responsible for the development, organization, and maintenance of the HIPAA Compliance Program. The HIPAA Compliance Officer serves as the Chair of the HIPAA Advisory Committee.

*Responsibilities of the Officers*

HIPAA Compliance Officer Responsibilities: Provides oversight compliance of Company practice groups and corporate departments to ensure that the Company is acting in compliance with HIPAA rules and regulations. Responsibilities include oversight and cooperation with the HIPAA Privacy Officer, HIPAA Security Officer, and IT to ensure that client PHI is processed in compliance with Company policies, HIPAA, and Huron's Business Associate Agreements (BAAs) when accessed, transmitted, or stored. The HIPAA Compliance Officer is also the main contact for incidents and breaches.

HIPAA Privacy Officer Responsibilities: The Privacy Officer is responsible for developing and implementing HIPAA-compliant company privacy policies and procedures, and along with the HIPAA Compliance Officer, provides training and acts as an official contact person for notices, complaints, and the provision of information. The HIPAA Privacy Officer works closely with the HIPAA Compliance Officer, HIPAA Security Officer, and IT to oversee compliance, policymaking, training, and incident response.

HIPAA Security Officer Responsibilities: The Security Officer is responsible for reviewing and modifying IT policies/procedures related to security based on identified risks to Huron's Information systems that contain PHI. The Security Officer is also responsible for oversight of compliance with HIPAA security rule under HIPAA Compliance officer. Responsibilities include working with IT director to identify areas of risks and provide recommendations to systems that contain PHI. The security officer will also provide guidance on acquisition of new systems/software/vendors that will contain or process PHI for compliance with the HIPAA Security rule. In conjunction with the IT director and GRC manager, the Security Officer will investigate and provide insight into incidents involving PHI. Other responsibilities include; overseeing and monitoring the security of ePHI, identifying and evaluating threats to the confidentiality and integrity of ePHI, responding to actual or suspected breaches in the confidentiality or integrity of ePHI, monitoring applicable rule changes or best practice around implementation of HIPAA security rule requirements, providing recommendations on remediation of audits involving healthcare and identifying areas of high risks in applications/systems that process ePHI.

The HIPAA Compliance, Privacy, and Security Officers along with key personnel on the IT-GRC team meets as needed to formulate, review, revise, and monitor implementation of HIPAA policies to meet Huron's obligations as a business associate of its clients.

The Huron Board of Directors, as the governing body, shall provide adequate resources and authority for the administration of this Program.

### Monitoring, Audits, and Investigations

The HIPAA Privacy and Security Officers shall monitor HIPAA Compliance Program implementation, periodically evaluate the effectiveness of the HIPAA Compliance Program, and shall conduct risk assessments of practice areas which may use or disclose PHI on behalf of Huron clients. In order to assess Huron employees' awareness, understanding, and observance of the HIPAA Compliance Program; to determine how individuals are identifying, tracking, and reporting HIPAA compliance issues; and to identify any existing or

new Huron risk areas, at least one operational engagement audit shall be conducted annually at the direction of the HIPAA Compliance Officer.

The HIPAA Compliance Officer is responsible to investigate all reports of actual or potential Program violations in accordance with HIPAA and the applicable BAA(s).

**Disciplinary Actions**
Personnel found to have violated the HIPAA Compliance Program will be disciplined in an appropriate, measured and consistent fashion. Violations (including the failure to report the misconduct of other personnel) may result in disciplinary actions, including possible immediate termination. Depending on the severity of the violation, the HIPAA Compliance Officer, the Corporate Vice President of Human Resources and other appropriate Corporate and Practice leadership may determine the specific disciplinary action.

The following categories define the significance and impact of the incident to help guide corrective action and remediation:

**HIPAA Compliance Program Violation Categories**
Huron has established the following categories to define the different levels of HIPAA compliance program violations:

1. **Unintentional HIPAA Compliance Program Violation**: Unintentional violation that may have been caused by carelessness or lack of knowledge. Examples include transmitting unencrypted PHI to an authorized recipient; leaving laptop unattended on a client site.

2. **Failure to Follow HIPAA Compliance Program – No PHI disclosure**: Failure to follow HIPAA Compliance Program policy without legitimate reason but does not involve disclosure of PHI. Examples: using another person's log-on name or credentials to access client or Huron systems; sharing log-on name or credentials with other personnel.

3. **Failure to follow HIPAA Compliance Program – PHI disclosure**: Failure to follow HIPAA Compliance Program policy that results in unauthorized access or disclosure of PHI. Examples: transmitting unencrypted ePHI to unauthorized recipient; losing documents containing PHI that were taken off-site; failing to prevent access to PHI on laptop due to removal of Huron-installed security tools.

4. **Deliberate HIPAA Compliance Program Violation**: Examples: disclosure of PHI to unauthorized recipient for malice or personal gain; willful violation of any state or federal statute; failure to report conduct by Huron personnel or client personnel that the employee knew was a violation of law; willfully providing materially false information to Huron, its attorneys, a government agency or other person in connection with any matter related to Huron or the provision of any Huron service; taking or attempting to take any retaliatory action against any person for making any compliance report or raising any compliance issue in good faith.

**HIPAA Compliance Program Violation Disciplinary Actions**
Possible sanctions for violations of the HIPAA Compliance Program shall include, but are not limited to:

a. Verbal warning
b. Written reprimand in employee's personnel file
c. Retraining on HIPAA Compliance Program policies
d. Retraining on Huron Global Information Security Policy
e. Reduction of bonus
f. Final warning

g. Suspension
h. Termination

Sanctions may be reduced based on mitigating factors or increased based on aggravating factors. The following factors will be considered in determining the appropriate sanction:

a. Repeat violations
b. Harm to the client
c. Volume of people or data affected
d. Reputational harm to Huron
e. Financial exposure to Huron, such as breach notifications, external counsel fees, penalties
f. Willful nature of the violation

## 3. GENERAL RESPONSIBILITIES OF HURON PERSONNEL

**Performance Expectations**

All Huron personnel who are engaged in activities for which the HIPAA Compliance Program is applicable are required to review these policies and procedures carefully, including the HIPAA Compliance Program Implementation Procedures. As a condition of employment or affiliation with Huron, these personnel are required to follow these policies and procedures. Adherence to the Huron HIPAA Compliance Program, including the HIPAA Compliance Program Implementation Procedures, will be included in the performance evaluation process and considered when making promotion or other performance decisions.

**Communication and Reporting**

All senior level personnel will reinforce by publication and action that all affected personnel are expected to follow the Huron HIPAA Compliance Program. Senior level personnel shall take an active role in the training and implementation of the HIPAA Compliance Program.

All personnel are encouraged to ask any questions, report any suspected infractions, or speak on any matter of concern without fear of retribution and are encouraged to utilize the current chain of command in their department with these issues where appropriate. Personnel are required to complete, within twenty-four (24) hours of identifying an issue, the Privacy Incident Reporting Form in order to report any violations of law, suspected breaches of PHI, suspected security incidents involving PHI, as well as any actual or suspected Huron HIPAA Compliance Program violations for which they are responsible or become aware.

Infractions or suspected infractions of the HIPAA Compliance Program may also be reported in accordance with the provisions of the Code of Business Conduct and Ethics, directly to the HIPAA Compliance Officer, any member of the Legal Department, or any member of Huron senior management. Personnel may also report suspected ethical, legal, or policy violations anonymously and confidentially using the Huron Helpline (1-800-690-8135).

Communications received by any Huron personnel from government agencies or Huron clients on any of the matters addressed in this Compliance Program shall be forwarded to the Huron HIPAA Compliance Officer immediately for discussion with the HIPAA Privacy and Security Officers, as appropriate.

**Training and Education of Huron Personnel and Contractors**

The Huron Human Resources Department will ensure and document that personnel whose responsibilities include handling PHI and who are engaged in activities for which the HIPAA Compliance Program is applicable receive training on HIPAA policies and procedures before that person is allowed access to information systems that contain PHI and at least annually thereafter. With regard to any new BAAs or amendments thereto, or material changes in the relevant law, including HIPAA and HITECH, training will be provided within a reasonable time after such material changes becomes effective. Educational efforts will be coordinated through the HIPAA Compliance Officer and include training provided by line management.

## 4. HIPAA PRIVACY REQUIREMENTS- CORPORATE

**Changes to Privacy Policies and Procedures**

Huron will promptly revise its HIPAA Compliance Program to reflect any changes in law. Huron may also revise its HIPAA Compliance Program for any other appropriate reason as may be determined by Huron. Huron will ensure that any changes to its HIPAA Compliance Program are appropriately documented in accordance with HIPAA. Huron will document and retain documentation of its compliance with its HIPAA Compliance Program for 6 years from the date of a document's creation or the last date a document was in effect, whichever is later.

**Business Associate Agreement**

Huron will not accept PHI from a Covered Entity unless a Business Associate Agreement that meets the requirements of HIPAA has been entered into with the Covered Entity. This policy applies whenever PHI is disclosed by a Covered Entity to Huron, including the period before and after an engagement begins.

Before Huron discloses a client's PHI to an agent or subcontractor, Huron will sign a contract with the agent or subcontractor that requires that the agent or subcontractor follow, at the minimum, the same restrictions that Huron has agreed to follow in the Business Associate contract entered into with the client. There will be no exceptions to this requirement.

**Use and Disclosure of PHI**

Huron will use and disclose a client's PHI only as permitted by its Business Associate contract, as permitted or required by law, and in accordance with these policies and procedures. Huron will limit its uses, disclosures, or requests for PHI, to the extent practicable, to the minimum necessary to accomplish the intended purpose of such use, disclosure, or request. Huron personnel who support, view, and/or retain client PHI will have access to a copy of the applicable BAA. If Huron personnel become aware of or suspect that there has been a use or disclosure of PHI in violation of Huron's Business Associate contract or these policies and procedures, such personnel will immediately report the violation to the HIPAA Compliance Officer in accordance with Huron's reporting mechanisms for HIPAA compliance issues.

**Return or Destruction of PHI**

Where feasible, at the termination of a project, Huron will return or will destroy PHI received from a Covered Entity or created or received on behalf of such an entity. PHI contained in reports or other files from a project will be deleted from laptops at the end of an engagement, including back-up copies from a client's system on laptops. Paper copies containing PHI will be shredded with Huron's or clients' shred vendor, unless such information can be retained pursuant to the BAA.

Documentation of deliverables retained after termination of a project should not contain PHI. Reports developed for post-engagement clients may be retained for training or marketing purposes only if they are de-identified in accordance with the HIPAA de-identification provisions at 45 C.F.R. §§ 164.514(a)-(c).

Where Huron has determined that it is infeasible for Huron to return or destroy PHI obtained from an engagement, Huron will agree to extend the protections found in the applicable BAA to cover this information.

**Requests for Information**

Requests for access to information by the Secretary of Health and Human Services (HHS), for access, amendment, or accounting purposes by individuals, or by the Covered Entity should be directed to the Huron Privacy Officer, who will respond to such request in accordance with the applicable BAA and Sections 164.524, 164.526, and 164.528 of the HIPAA Privacy Rule.

## 5. PRIVACY RESPONSIBILITIES OF HURON PERSONNEL

Huron will implement reasonable administrative, physical and technical safeguards to protect its clients' PHI from any intentional or unintentional uses or disclosures in violation of its BAA and limit any incidental disclosures of PHI. Huron personnel will take appropriate safeguards to protect PHI including, but not limited to, the following: a) when on-site at a client's place of business, where possible, lock all rooms containing PHI whenever at least one Huron representative is not present, b) use access controls and

password safeguards in accordance with Huron policy, c) dispose of documents containing PHI that are no longer needed by shredding or placing them in Huron's or clients' shredding bins, d) use an approved fax transmittal sheet when transmitting PHI or other confidential information by electronic facsimile, e) use care to avoid unauthorized persons from overhearing discussions that relate to PHI, f) use care not to place computers containing PHI in places where the information may be reviewed by unauthorized individuals, g) follow Huron's HIPAA Compliance Program requirements regarding e-mailing PHI and use of access controls, h) do not take original documents belonging to a client off-site, i) take other paper and/or electronic documents off-site if personnel need to work on them or when traveling, only if reasonable precautions as described in Huron's data security policies are taken to prevent loss or unauthorized access of the materials, and j) place files that contain PHI on one's laptop or other portable electronic device only in accordance with Huron security policies.

## 6. HIPAA SECURITY REQUIREMENTS- CORPORATE

Huron is responsible to ensure the confidentiality, integrity, and availability of its information systems containing electronic PHI by implementing appropriate and reasonable policies, procedures, and controls to prevent, detect, contain, and correct security violations. Huron will develop and maintain written policies and procedures for the routine and non-routine receipt, manipulation, storage, dissemination, transmission and/or disposal of electronic protected health information. The HIPAA Security Rule is a component of Huron's Security Policies, which are applicable to all Huron personnel.

The Managing Director of Information Technology ("IT") is responsible for the administration of Huron's security policies, procedures, and controls that reasonably and appropriately mitigate identified risks to Huron's information systems that contain PHI. Such policies and procedures which relate to HIPAA will be modified by the HIPAA Security Officer, after consultation with the HIPAA Privacy Officer, as needed to continue the provision of reasonable and appropriate protections of electronic PHI, and as appropriate in light of new technology, business requirement changes, risk analyses, and other changes in rules, regulations, or other company policies.

### Internal Audits

In consultation with the HIPAA Compliance and Privacy Officers, IT will perform log checks that will include review of logins to the network, file accesses at the file level, and potential security incidents and breaches when there is a suspicious activity. Logs are sent to a system and tools are in place to provide alerts. Any unusual or irregular activity will be promptly investigated. IT will report incidents of unauthorized use or activity to the Huron HIPAA Security Officer.

### Security Configuration

IT will periodically test the security features of its systems to ensure they are adequate. The process may include hands-on functional testing, penetration testing and/or network assessments. The Privacy and Security Officers will be informed of the results of this testing. IT will also perform virus checks on a regular basis to include: install and maintain up-to-date virus scanning software on all computer systems, respond to all virus incidents, make best efforts to destroy or contain any virus encountered or anticipated, and document any virus encountered.

IT will maintain effective backup procedures for information systems that contain PHI to ensure the confidentiality, integrity, and availability of Huron's data network and information operating systems. IT will develop and implement formal, documented instructions for reporting security breaches and security incidents involving PHI.

## 7. SECURITY RESPONSIBILITIES OF HURON PERSONNEL

### Equipment Security

Huron personnel may receive standard issue, encrypted, computers and mobile devices in connection with the services they are called upon to provide. Huron personnel must adhere to Huron's data security policies (located on iNet) and take all reasonable steps to protect these laptops, mobile devices, Huron computer

systems, data, software and documentation from misuse, loss, theft, unauthorized access and environmental hazards.

**Restrictions on E-mailing PHI**
Because the Internet is an inherently insecure medium, Huron personnel will discourage clients from e-mailing PHI outside the client's network to Huron unless encryption is used, and Huron personnel will not themselves e-mail such information on an open, unsecured network without encryption. Huron personnel are responsible for appropriately protecting PHI from unauthorized access, modification, destruction, and disclosure. (See IT policies on Huron's iNet regarding use of tools to send encrypted data files.)

**Credential Protection**
Huron personnel must not use another person's log-on name or credentials to access client or Huron systems. Huron personnel must take reasonable precautions in handling their passwords to prevent unauthorized access to files containing PHI.

**Access Management**
Managers and supervisors must notify the Human Resources and IT departments promptly when personnel leave Huron or transfer departments in order to ensure that the corresponding access changes are made. Terminations must be reported in conjunction with the termination date. IT and Human Resources will take the steps necessary to timely end other aspects of that person's access, which may involve changing combination locks, removal from access lists, return of keys, token or cards, and termination or deletion of an individual's access privileges to information, services, and resources.

## 8. CORPORATE IT REQUIREMENTS: MEDIA AND ACCESS CONTROLS

**Hardware Controls and Safeguards**
The installation and assignment of hardware and software, within Huron's computer system, that contains or will contain PHI, will be controlled and subject to approval by Huron IT Department. Significant software modifications to the security attributes of proprietary Huron software will be made only after consultation with the Privacy Officer and the Security Officer.

IT will maintain records of ownership and assignment of laptops, and ensure that only authorized individuals have login credentials to access them. IT will implement reasonable physical safeguards in accordance with the Security Rule to protect PHI in Huron's possession and the Huron hardware on which it resides from being stolen or accessed by unauthorized persons.

**Access Controls**
Access control and/or passwords will be used to protect the security, integrity, and confidentiality of all Huron and client data in Huron's possession. Access control is centrally managed by Huron Information Technology (IT) and is based on the personnel member's class, need for access and level of responsibility.

IT will employ user-based access (access based on user name and password) and at least one of the following two types of access control: a) context-based access (access based on the context of the transaction such as time of day or location of the user), or b) role-based access (each user is assigned a role and assigned needed privileges).

IT will be responsible for granting and controlling access on all company-owned computer systems, and will process all system deletions, changes and modifications to user rights. A log will be maintained that tracks access rights given to PHI. All external personnel performing maintenance activities on Huron's computer system will be appropriately supervised by authorized and knowledgeable persons.

IT will utilize entity authentication or a mechanism to verify that entities or persons are who they claim to be before they are given access to client information. This entails using unique user identification, defined as a unique name and number assigned to each user and a password system. All system users will be given access only to such client data they need to perform a function.

IT will configure systems, whenever possible, to prompt users for password changes on a regular basis and require passwords that conform to the standards set forth herein.

IT will employ Technical Security Mechanisms to guard against unauthorized access to data transmitted over a communications network and intrusion to its system through external communication points. Towards this end, it will use access controls, which is defined as the protection of sensitive communications over open or private networks so that it cannot be easily intercepted and interpreted by parties other than the intended recipient and, if using an open network such as the Internet, encryption.

**Safeguards to Protect Data**
Reasonable safeguards will be taken to protect data in transit sent from a client to Huron from unauthorized access.

Frequently, analysis or configuration work using client data containing PHI may be required. When possible this work should be done on client networks or servers without moving the data outside of client firewalls. If the transfer of data containing PHI is required, it must be done using an approved secure encrypted medium in accordance with Huron's data security and ePHI policies. Placing ePHI on any unsecured medium, such as a removable disk or drive, is prohibited, unless specifically authorized by the HIPAA Compliance Officer in writing, in advance, and, if used, the storage device must be encrypted in accordance with Huron policies.

In accordance with the applicable National Institute of Standards and Technology ("NIST") standards specified under HIPAA, IT will use SSL or similar encryption technology to secure Internet communications containing PHI. IT will use an encryption application on all Huron-issued mobile devices, including laptops and outboard devices, so that if a laptop or device is stolen, the data will be encrypted and accessible only by using a username and password.

**Intrusion Protection**
Huron's network will be protected from outside intrusion with firewalls. Regular security patches and upgrades will be applied, if deemed necessary.

Huron will not install its software on a client's system so that it is accessible from external networks such as the Internet unless a client has put in place baseline security measures to prevent such access from being an entry point for unauthorized users to the client's computer system. These baseline measures include firewalls, encryption and entity authentication.

## 9. HITECH: PHI BREACH DETERMINATION AND NOTIFICATION PROCESS

A breach may have occurred if unsecured PHI is accessed, used or disclosed in a way that is not allowed under the HIPAA Privacy Rules; and such access, use or disclosure compromises the security or privacy of the PHI by posing a significant risk of financial, reputational, or other harm to the potentially affected individual, as may be determined by the Huron Legal Department.

If the Covered Entity or a Business Associate discovers a breach of unsecured PHI, organizations may be required to notify affected individuals, federal and state government agencies, and in some cases, the media. Notification is required if there is a breach and PHI is "unsecured" as defined in the Glossary of Terms to this Policy. Conversely, notification is not required if there is a breach and PHI is "secured".

**Huron Personnel Reporting Requirements**
Huron personnel who discover, believe, or suspect that any violation has occurred of Huron's HIPAA Compliance Program or any engagement BAA requirement must immediately report such information to the Huron HIPAA Compliance Officer or Huron Legal Department, in accordance with the Huron HIPAA Compliance Program.

The PHI Breach and Security Incident Determination and Notification Process is provided as an appendix in this Policy.The HIPAA Compliance Officer, with the support of Huron's Legal Department, is responsible for implementing this process.

## 10. Glossary of Terms

**Breach**

A Breach is the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI. The following are exceptions to the definition of a "breach":

1. any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of Huron or its Business Associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule;
2. any inadvertent disclosure of PHI from a person authorized to access PHI at Huron or its Business Associate to another person authorized to access PHI at Huron or its Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; and
3. any disclosure of PHI where Huron or its Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

**Business Associate**

A Business Associate is an entity that provides services to a Covered Entity that involve the use or disclosure of PHI, or performs a service or function for or on behalf of a Covered Entity that involves the use or disclosure of PHI.

**Designated Record Set**

A Designated Record Set is a group of records that includes PHI and is maintained, collected, used, or disseminated by or for the Covered Entity that is (1) the medical records and billing records about individuals maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems and any other information maintained by or for a health plan; or (3) used, in whole or in part, to make decisions about individuals.

| | |
|---|---|
| **DHHS** | DHHS is the Department of Health and Human Services, which is the federal agency charged with administering HIPAA. |
| **Discovery of the Breach of Unsecured PHI** | A Breach of Unsecured PHI shall be treated as discovered by Huron or its Business Associate as of the first day on which such Breach is known to Huron or its Business Associate or – by exercising reasonable diligence – would have been known to Huron or its Business Associate, respectively. Huron or its Business Associate shall be deemed to have knowledge of a Breach if such Breach is known or – by exercising reasonable diligence – would have been known to any person, other than the person committing the Breach, who is a workforce member or agent of Huron or its Business Associate, respectively. |
| **Health Oversight Agency** | A federal or state governmental agency authorized by law to oversee public or private health care systems or programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant. |
| **HIPAA** | HIPAA is the Health Insurance Portability and Accountability Act of 1996. |
| **HIPAA Privacy Rule** | The HIPAA Privacy Rules are the HIPAA regulations issued by DHHS at 45 C.F.R. §§ 160 and 164, Subparts A and E. |
| **HIPAA Security Rule** | The HIPAA Security Rules are the HIPAA regulations issued by DHHS at 45 C.F.R. Parts 160 and 164, Subparts A and C. |
| **HITECH** | HITECH is the Health Information Technology for Economic and Clinical Health Act of 2009. |
| **Law Enforcement Official** | A federal or state governmental employee authorized to investigate a potential violation or law and enforce federal and/or state law |
| **Limited Data Set** | A Limited Data Set is a set of PHI that excludes the following direct identifiers of the individuals or of the relatives, employers, or household members of the individual to whom the PHI relates: name, street address, telephone and facsimile numbers, email addresses, social security numbers, medical records numbers, health plan beneficiary numbers, any account numbers, certificate or license numbers, vehicle identifiers (including license plate numbers), device identifiers and serial numbers, web universal resource locators ("URLs") and internal protocol ("IP") address numbers, biometric identifiers (including finger and voice prints), and full face photographic images and any comparable images. |

**Protected Health Information or PHI**

Protected Health Information or PHI is individually identifiable health information, including demographic information collected from an individual that: 1) is created or received by Huron from or on behalf of a health care provider, health plan, employer, or health care clearinghouse; and 2) relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual and that identifies the individual or reasonably could be used to identifythe individual.

**Unsecured Protected Health Information or Unsecured PHI**

PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under HITECH on the U.S. Department of Health and Human Services ("HHS") website.

# APPENDIX

## 11. HITECH: PHI BREACH DETERMINATION AND NOTIFICATION PROCESS

Under recently enacted regulations related to HITECH amendments to HIPAA, Covered Entities are required to notify individuals, the DHHS, and in some cases, the media, if the Covered Entity or a Business Associate discovers a Breach of Unsecured PHI. Moreover, Business Associates are required to notify Covered Entities of Security Incidents, a term that includes Breaches of Unsecured PHI but is much broader. Specifically, even if an incident is not a Breach of Unsecured PHI, it may be a Security Incident. Under the HIPAA Security Rules, Covered Entities and Business Associates must identify and respond to suspected or known Security Incidents; mitigate, to the extent practicable, harmful effects of Security Incidents that are known to the Covered Entity or Business Associate; and document Security Incidents and their outcomes.

This Addendum to Huron's HIPAA Compliance Program describes Huron's process for reviewing data incidents involving PHI as potential Breaches of Unsecured PHI or potential Security Incidents, determining whether the incident is reportable as a Breach of Unsecured PHI or a Security Incident, and providing notification and reporting of the incident when required by law on Huron's contractual obligations to its customers.

### A. Unsecured PHI

Under HIPAA, notification is required if there is a Breach, as defined below, and PHI is "Unsecured." Conversely, notification under HIPAA is not required if there is a Breach and PHI is "secured", or if the incident itself does not meet HIPAA's definition for the term Breach. PHI is secured if it meets the following standards:

- Electronic data at rest, which includes data that resides in databases, file systems, flash drives, memory, and any other structured storage method:
  Encryption consistent with National Institute of Standards and Technology ("NIST") Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
- Electronic data in motion, which includes, for example, data that is moving through a network, including wireless transmission, whether by e-mail or structured electronic interchange: a.
  Encryption in compliance, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TL Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, or others which are Federal Information Processing Standards (FIPS) 140-2 validated. In addition, encryption keys should be kept on a separate device from the data that they encrypt or decrypt.
- Data disposed, which includes discarded paper records or recycled electronic media: The media on which the PHI is stored or recorded has been destroyed in one of the following ways:
  1. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.
  2. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publication 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

### B. Huron Personnel Reporting Requirements

Generally, a Breach has occurred if PHI is accessed, acquired, used or disclosed in a way that is not allowed under the HIPAA Privacy Rules; and such access, acquisition, use or disclosure compromises the security or privacy of the PHI. Huron personnel who discover, believe, or suspect that PHI has been accessed, acquired, used or disclosed in a way that violates the HIPAA Privacy Rule, must immediately report such information using the Privacy Incident Reporting Form. In the event of doubt, potential

incidents should be reported to the Huron HIPAA Compliance Officer or Huron Legal Department for review, contact the HIPAA Compliance Officer.

Huron personnel who are determined to have failed to adhere to the policies and procedures regarding reporting of Breach of Unsecured PHI will be subject to the disciplinary policies of Huron.

Any report of a potential breach of Unsecured PHI from a Subcontractor Business Associate shall be handled on a case-by-case basis in accordance with the applicable Subcontractor Business Associate Agreement and other relevant agreements.

### C. Breach and Security Incident Determination and Notification Process Steps

The Huron Legal Department will determine whether a Breach of Unsecured PHI has occurred. In summary, the process steps to make this determination involve addressing these questions:

1. Has Unsecured PHI been acquired, accessed, used or disclosed in violation of the HIPAA Privacy Rule?
    a. The HIPAA Compliance Officer, in consultation with others in the Legal Department, as appropriate, will investigate the report to determine whether there has been an acquisition, access, use or disclosure of Unsecured PHI by Huron personnel or that of its Business Associates that violates the HIPAA Privacy Rule, and if necessary, report and remediate any Breach in accordance with this "PHI Breach Determination and Notification Process".
    b. The HIPAA Compliance Officer, in consultation with others in the Legal Department, as appropriate, will review the applicable Business Associate Agreements at issue and determine whether there are any contractual provisions relevant to its analysis, including Breach notification reporting periods and "security incident" reporting periods. All investigations must be conducted without undue delay and in accordance with any notification periods set forth in the applicable Business Associate Agreements. If the applicable Business Associate Agreements fail to specify notification periods, then Huron must complete its investigation and, if it is determined a Breach of Unsecured PHI has occurred, report such Breaches of Unsecured PHI without undue delay and in no event later than 60 calendar days following the Discovery of the Breach of Unsecured PHI, with the exception of law enforcement delays that satisfy the requirements under 45 C.F.R. § 164.412 or as otherwise required by applicable state law
2. Does the impermissible acquisition, access, use or disclosure fall under an exception to the definition of Breach?
    a. If the HIPAA Compliance Officer, in consultation with others in the Legal Department, as appropriate, determines that there has been access to or an acquisition, use or disclosure of Unsecured PHI in violation of the HIPAA Privacy Rule, the Legal Department will then determine whether the potential breach falls under any applicable exceptions to the definition of Breach. These exceptions are as follows:
        i. Any unintentional acquisition, access, or use of PHI by Huron personnel or its Business Associate, if done in good faith and within the scope of authority, and which does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule
        ii. Any inadvertent disclosure from a person authorized to access the PHI at Huron or its Business Associate to another person authorized to access the PHI at the same entity, and the PHI is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule
        iii. Any disclosure where Huron or its Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

b. If the HIPAA Compliance Officer, in consultation with others in the Legal Department, as appropriate, determines that a potential Breach of Unsecured PHI does not constitute an impermissible use or disclosure under the HIPAA Privacy Rule or falls under an exception to the definition of Breach, then a reportable Breach did not occur and Huron should refer to Section 5 of this Process.

3. If no exceptions to the definition of breach apply, does the impermissible acquisition, access, use or disclosure result in more than a low probability that the privacy or security of the Unsecured PHI has been compromised? If yes, go to Section 4. If no, go to Section 5.

   a. If the Legal Department determines that there was a use or disclosure of Unsecured PHI in violation of the HIPAA Privacy Rule and no exception to the definition of "breach" is applicable; the Legal Department will determine, and document, whether the impermissible use or disclosure of Unsecured PHI compromises the security or privacy of the PHI. Under the HIPAA Breach Notification Rule, a Breach of Unsecured PHI presumptively compromises the security or privacy of the PHI unless it can be demonstrated through a documented risk assessment that there is a low probability that the Unsecured PHI has been compromised.

   b. In conducting a documented risk assessment, the Legal Department will consider:

      *i.* the nature and extent of the Unsecured PHI involved, including the types of identifiers and the likelihood of re-identification;

      *ii.* the unauthorized person who used the Unsecured PHI or to whom the disclosure was made;

      *iii.* whether the Unsecured PHI was actually acquired or viewed; and

      *iv.* the extent to which the risk to the Unsecured PHI has been mitigated.

   c. In addition, given the circumstances of the impermissible use or disclosure, additional factors may need to be considered to appropriately assess the risk that the Unsecured PHI has been compromised. These factors may be determined on case-by-case basis in the reasonable judgment of the Huron HIPAA Compliance Officer, in consultation with others in the Legal Department, as appropriate.

   d. The burden of proof to demonstrate that there is a low probability that the PHI has been compromised lies with Huron. However, if the risk assessment establishes that a potential Breach of Unsecured PHI presents a low probability that PHI has been compromised, then a reportable Breach has not occurred and Huron must next consider Section 5 of this Process

4. If it is determined that: 1) a Breach of Unsecured PHI has occurred, 2) no exception to the reporting requirement applies, and 3) there is more than a low probability that the Unsecured PHI has been compromised, Huron's HIPAA Compliance Officer will notify the affected Covered Entity or Entities in accordance with the terms of the applicable Business Associate Agreement.(s) Where Huron is responsible for providing notification of a Breach to affected individuals under the applicable Business Associate Agreement, Huron will work with the affected Covered Entity or Covered Entities to provide notice in accordance with requirements under the HIPAA Breach Notification Rule and the applicable Business Associate Agreement(s).

5. If no, does the incident rise to the level of a Security Incident? If yes, Huron will notify the affected Covered Entity or Entities in accordance with the reporting requirements applicable to Security Incidents as set forth in the applicable Business Associate Agreement(s).

   a. Even where an incident is determined by the Huron Legal Department to not result in a Breach of Unsecured PHI, the Legal Department must evaluate whether the incident constitutes a Security Incident within the meaning of the HIPAA Security Rules and applicable Business Associate Agreement(s). If so, then Huron must comply with the mitigation, documentation, and reporting requirements of the applicable Business Associate Agreement(s) and its obligations under the HIPAA Security Rules.

b. Any Security Incident mitigation efforts and notices to affected Business Associates shall be done under the direction of the Huron HIPAA Compliance Officer in coordination with the Huron Legal Department.

**D. Documentation Requirements**

All investigations conducted pursuant to this Process must be appropriately documented by or under the direction of the Huron Legal Department.

**Change History**

| Date | Version | Created by | Description of change |
|---|---|---|---|
| December 2008 | V1.0 | Compliance | Adopted |
| February 2009 | V2.0 | Compliance | |
| May 2012 | V3.0 | Compliance | |
| August 2013 | V4.0 | Compliance | |
| February 2017 | V5.0 | Compliance | |
| June 2019 | V6.0 | Compliance | |
| October 2023 | V7.0 | Compliance | Annual review and minor updates |