HURON CONSULTING GROUP INC

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

Adopted December 2008
Revised effective February 16, 2009

Table of Contents

OVERVIEW OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

The Huron HIPAA Compliance Program addresses issues concerning the privacy and security of health information mandated in the Health Insurance Portability Accountability Act of 1996 (HIPAA). Huron's HIPAA Compliance 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 individual identifiable health information carefully and responsibly in accordance with the provisions of HIPAA 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). HIPAA applies directly to a Covered Entity (CE), defined as "a health plan, a health care clearinghouse, health care provider, or drug discount card program sponsor that transmits any health information in electronic form in connection with a HIPAA transaction".

- Business Associates are persons or organizations who perform functions for the Covered Entity that involves the use of disclosure of individually identifiable information. CEs may only share PHI with other persons or organizations (Business Associates) where the CE has signed a Business Associate Agreement with the Business Associate in which the Business Associate promises to treat PHI received from the CE in accordance with HIPAA provisions.

- Protected Health Information (PHI), generally defined as individually identifiable health information, includes health and demographic information created or received by a Covered Entity that identifies or could be used to identify an individual. (Section 160.103). The specific identifiers that are considered PHI, and must be removed if the data is considered to be "de-identified", include 18 categories of data. [1]

[1] HIPAA Section 164.514(2)(i)
De-identified information excludes all information concerning the individual or the individual's relatives, employers or household members: names, all geographic subdivisions smaller than a state, including street address and zip codes (except for the initial three digits of a zip code if, according to current data available from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same initial three digits contains more than 20,000 people, and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000), all elements of dates (except year), for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) (except that ages may be aggregated into a category of age 90 or older), telephone numbers, fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate /license numbers, vehicle identification and serial numbers, including license plate numbers, device identifiers and serial numbers, Web Universal Resource Identifiers, Internet Protocol address numbers, biometric identifiers, full face photographic images and comparable images, and any other identifier from a record which could be used to identify an individual.

- 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 sufficient patient permission 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 take all steps necessary 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). The Business Associate is required to:

  a) Use or further disclose PHI only as permitted or required by the contract,
  b) Restrict its uses and disclosures of PHI to those outlined in the contract or as required by law,
  c) Implement safeguards to prevent unauthorized uses and disclosures of PHI,
  d) Report violations of the agreement to the Covered Entity,
  e) 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,
  f) Provide individuals with access to designated record sets in the Business Associate's possession,
  g) Make PHI contained in designated record sets available for amendment and incorporate amendments as requested by a Covered Entity,
  h) Make available information for a Covered Entity to provide an accounting of disclosures,
  i) Make its internal practices, books and records relating to the use and disclosure of PHI by the Business Associate available to the Secretary of Health and Human Services for purposes of determining the Covered Entity's compliance with the standards, and
  j) If feasible, 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. This is critical for all Huron personnel to understand, as it affects Huron's continued viability.

INTRODUCTION AND PURPOSE

The goals of the Huron HIPAA Compliance Program are 1) to provide guidance on the requirements of the Health Insurance Portability and Accountability Act of 1996 (known as HIPAA) so that Huron Consulting Group ("Huron") can maintain compliance with the Act, 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.

PROGRAM ADMINISTRATION

HIPAA Compliance Committee and Officers

The HIPAA Advisory Committee serves as an advisory body to the HIPAA Compliance and Privacy Officers, and provides a source of discussion and exchange of information among various functional areas of Huron. The Advisory Committee 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 HIPAA Compliance Officer shall be Ken Jones, who shall also serve as HIPAA Security Officer, or such other person named by the General Counsel from time to time. The HIPAA Privacy Officer shall be Beatriz Olivera or such other person named by the General Counsel from time to time. They are jointly responsible for the development, organization, and maintenance of the HIPAA Compliance Program and will provide reports to the HIPAA Advisory Committee not less often than annually. The HIPAA Compliance Officer serves as the Executive Director of the HIPAA Advisory Committee.

The HIPAA Advisory Committee is comprised of the HIPAA Compliance and Security Officer, HIPAA Privacy Officer, and may include one or more representatives from each of the following: a) Huron's Information Technology group, b) Human Resources, and c) the Combined Healthcare, Higher Education, Clinical Research Solution and Healthcare Compliance and Pharma/Health Plan practices.

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 and periodically evaluate the effectiveness of the HIPAA Compliance Program. The Privacy and Security Officers shall conduct risk assessments of practice areas where criminal violations may occur.

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 Privacy or Security and Compliance Officer.

The HIPAA Privacy Officer and/or HIPAA Security Officer are responsible to investigate all reports of actual or potential Program violations.

Disciplinary Actions

In accordance with the provisions of the Huron Code of Business Conduct and Ethics, personnel found to have violated the HIPAA Compliance Program will be disciplined in an appropriate, measured, and consistent fashion, regardless of their position within the organization. Violations (including failure to

report the misconduct of other personnel) may result in disciplinary actions, including possible immediate termination. The specific disciplinary action taken shall be determined on a case-by-case basis by the Huron Vice President of Human Resources or her designee after recommendation by the HIPAA Privacy or Security Officer. The range of sanctions shall include mandatory retraining, verbal warnings, reduction of bonus, suspension, or termination.

Certain violations of the Compliance Program are particularly likely to justify immediate termination. These offenses include: a) violation of any state or federal statute; b) failure to report conduct by Huron personnel or client personnel that a reasonable person under the circumstances should have known was a criminal violation of law, or a violation of the Huron HIPAA Compliance Program; c) 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; and d) taking or attempting to take any retaliatory action against any person for making any compliance report or raising any compliance issue in good faith.

GENERAL RESPONSIBILITIES OF HURON PERSONNEL

Restrictions to Employment

No business or employment is offered to individuals or entities excluded from participation with Medicare or Medicaid programs, and sanctioned individuals and /or organizations cannot be employed or contracted. Each new individual or organization will be required to certify that he / she has not been convicted of a criminal offense related to healthcare or is not listed by a federal agency as debarred, excluded, or otherwise ineligible for participation in federally funded healthcare programs.

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. 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 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, as well as the Code of Business Conduct and Ethics. 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 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, unless there is a need to go elsewhere in the organization for advice. Personnel are required to promptly report any violations of law 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 Security or Privacy 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 by contacting EthicsPoint. (See Code of Business Conduct and Ethics)

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 Corporate Compliance Officer immediately for discussion with the HIPAA Privacy and Security Officers.

Training and Education of Huron Personnel and Contractors

The Huron Human Resources Department will ensure that personnel who are engaged in activities for which the HIPAA Compliance Program is applicable receive and provide written acknowledgement of training on HIPAA policies and procedures before that person is allowed access to information systems that contain PHI and at least annually thereafter. Educational efforts will be coordinated through the HIPAA Privacy and Security Officers and include training provided by line management.

Acknowledgement of receipt of the Huron HIPAA Compliance Program and its components is required of all staff and contractors who are engaged in activities for which the HIPAA Compliance Program is applicable.

HIPAA PRIVACY REQUIREMENTS- CORPORATE

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 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 or as required by law. Each Huron employee who supports, views and/or retains client PHI will have access to a copy of the applicable Business Associate contract. 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 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 covered by the Privacy Standards 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, 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 by redacting any identifier required by the de-identification provisions of HIPAA.

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 its Business Associate Agreement to cover this information.

Requests for Information

Requests for access to information by the Secretary of Health and Human Services (HHS), for 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 HIPAA requirements.

PRIVACY RESPONSIBILITIES OF HURON PERSONNEL

Huron will implement reasonable safeguards to protect its clients' PHI from any intentional or unintentional uses or disclosures in violation of its Business Associate contract Huron personnel will take appropriate safeguards to protect PHI including 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 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 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.

HIPAA SECURITY REQUIREMENTS- CORPORATE

Huron is responsible to ensure the confidentiality, integrity, and availability of its information systems containing 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 health information. The HIPAA Security Requirements are a component of Huron's Security Policies, which are applicable to all Huron personnel.

The Managing Director of Information Technology 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 may be modified by the Security Officer, after consultation with the Privacy Officer, 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 Privacy Officer and Huron's Regulatory Counsel, IT will perform regular log checks that will include review of logins to the network, file accesses at the file level, and security incidents. Any unusual or irregular activity will be promptly investigated. IT will report incidents of unauthorized use or activity to the Huron 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 of PHI.

SECURITY RESPONSIBILITIES OF HURON PERSONNEL

Equipment Security

Huron personnel may receive a standard issue computer in connection with the services they are called upon to provide. Huron personnel must take all reasonable steps to protect their laptops, Huron computer systems, data, software and documentation from misuse, loss, theft, unauthorized access and environmental hazards in accordance with Huron's Security Policies.

Huron personnel shall take reasonable steps including the following to avoid introducing any virus (in any form) into any computer system: 1) not open or execute any e-mail attachments from un-trusted sources, 2) not open or execute any suspicious e-mail attachment from any source, 3) scan all downloaded Internet executable files, 4) scan all removable media, and 5) immediately disconnect from any network and contact support personnel if a virus is encountered.

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 intranet 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 IT 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 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.

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. Consultation shall not be required where Huron personnel set the security features for a client.

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 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 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 such as Secure Transport or Accelion. Placing PHI on an unsecured medium, for example any type of removable disk or drive, is strongly discouraged and, if used, must be encrypted in accordance with Huron policies and must be documented.

IT will use SSL or similar encryption technology to secure Internet communications containing PHI. IT will use an encryption application on all laptops so that if a laptop 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 by unless a client has put in place certain 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.