HIPAA & FWA Guidelines

Health Insurance Portability & Accountability Act (HIPAA)

What is HIPAA?

HIPAA is an acronym for Health Insurance Portability & Accountability Act of 1996 (45 C.F.R. parts 160 & 164).

This act provides a framework for establishment of nationwide protection of patient confidentiality, security of electronic systems, and standards and requirements for electronic transmission of health information.

What is protected by HIPAA?

Health information is protected if it directly or indirectly identifies someone.

- Direct identifiers: individual's name, SSN, driver's license numbers
- Indirect identifiers: information about an individual that can be matched with other available information to identify the individual.

Direct and Indirect Identifiers

▪ Name
▪ Geographic subdivisions smaller than a State
  ○ Street Address
  ○ City
  ○ County
  ○ Precinct
  ○ Zip Code & their equivalent geocodes, except for the initial three digits
▪ Dates, except year
  ○ Birth date
  ○ Admission date
  ○ Discharge date
  ○ Date of death
▪ Telephone numbers
▪ Fax number
▪ E-mail Address
▪ Social Security numbers
	▪ Medical record numbers
	▪ Health plan beneficiary numbers
	▪ Account numbers
	▪ Certificate/license numbers
	▪ Vehicle identifiers and serial numbers, including license plate numbers
	▪ Device identifiers and serial numbers
	▪ Web universal resource locations (URLs)
	▪ Internet Protocol (IP) address numbers
	▪ Biometric identifiers, including finger and voice prints
	▪ Full face photographic images and any comparable data
	▪ Any other unique identifying number, characteristic, or code

How HIPAA Protects PHI

PHI stands for Protected Health Information. It is generally defined as any information that can be used to identify a patient – whether living or deceased – that relates to the patient's past, present, or future physical or mental health or condition, including healthcare services provided and payment for those services.

Privacy Rule

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information by:

- Limiting who may use or disclose PHI.
- Limiting the purposes for which PHI may be used or disclosed

- Limiting the amount of information that may be used or disclosed (Minimum Necessary rule)
- Requiring use of safeguards over how PHI is used, stored and disclosed

Why do we need to protect PHI?

It is everyone's responsibility to take the confidentiality of patient information seriously. Anytime you come in contact with patient information or any PHI that is written, spoken or electronically stored, **YOU** become involved with some facet of the privacy and security regulations. Additionally, we need to keep in mind:

- It is the law
- We need to protect our organization
- Trust must be established between providers and patients

Who protects PHI?

- **Federal Government**, through HIPAA regulations and by imposing penalties on those who do not follow the law.
- **Our organization**, by providing security and compliance guidelines.
- **You**, by following our policies and procedures.

How may PHI be used?

Workforce members may use or disclose PHI only for permitted uses without an individual's specific written authorization.

Permitted Uses For PHI

- "TPO"
  - Treatment
  - Payment
  - Health care operations
- Specified public policy exceptions (public health and law enforcement)

Minimum Necessary Rule

Generally, a patient's authorization is required for the use or disclosure of PHI. When a use or disclosure of PHI is permitted, via patient authorization or otherwise, HIPAA requires that only the amount of PHI that is the MINIMUM NECESSARY to accomplish the intended purpose be used or disclosed.

Disclosures of PHI

HIPAA regulations permit use or disclosure of PHI for:

- Providing medical treatment
- Processing healthcare payments
- Conducting healthcare business operations
- Public health purposes as required by law

One **may not** otherwise access or disclose PHI *unless*:

- The patient has given written permission
- It is within the scope of an your job duties
- Proper procedures are followed for using data in research
- Required or permitted by law

Note: The Final Rule now protects the PHI of a **deceased individual** for period of 50 years following the death of that individual.

Types of Privacy Violations

- **Type I -- Inadvertent or Unintentional Disclosure**

- Inadvertent, unintentional or negligent act which violates policy and which may or may not result in PHI being disclosed.
- Disciplinary action for a Type I disclosure will typically be a verbal warning, re-education, and review and signing of the Confidentiality Agreement. However, disciplinary action is determined with the collaboration of the Privacy Officer, Director of Human Resources and the department manager.

- **Type II – Intentional Disclosure**

- Intentional act which violates the organization's policies pertaining to that PHI which may or may not result in actual harm to the patient or personal gain to the user.
- Breach notification processes will be followed as described in the Breach Notification Policy.

Security Rule

Whereas the HIPAA Privacy Rule deals with Protected Health Information (PHI) in general, the **HIPAA Security Rule** (SR) deals with electronic Protected Health Information (ePHI).

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

> **ePHI** or electronic Protected Health Information is patient health information which is computer based, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media. }
>
> **Electronic media** includes computers, laptops, CDs/DVDs/disks, memory sticks, smart phones, PDAs, servers, networks, dial-modems, email, web-sites, etc.

Security (IT) regulations went into effect **April 21, 2005.**

- Security means controlling:
  - **Confidentiality** of electronic protected health information (ePHI).
  - **Storage** of electronic protected health information (ePHI)
  - **Access** into electronic information

General Requirements of the Security Rule

Ensure the "CIA" (confidentiality, integrity and availability) of all electronic protected health information (ePHI) that the covered entity creates, receives, maintains, or transmits.

- **Confidentiality** means that data or information is not made available or disclosed to unauthorized persons or processes.
- **Integrity** means that data or information has not been altered or destroyed in an unauthorized manner.
- **Availability** means that data or information is accessible and useable upon demand only by an authorized person.

Security Standards and Safeguards

- Protect PHI from accidental or intentional unauthorized use/disclosure in computer systems (including social networking sites such as Facebook, Twitter and others) and work areas
- Limit accidental disclosures (such as discussions in waiting rooms and hallways)
- Include practices such as encryption, document shredding, locking doors and file storage areas, and use of passwords and codes for access.
- Keep passwords and codes confidential

- Access information only as necessary for your authorized job responsibilities.
- Avoid storing sensitive information on mobile devices and portable media, but if you must, you must use encryption.

HITECH

HITECH stands for Health Information Technology for Economic and Clinical Health Act of 2009.

HITECH expanded the responsibilities of business associates under the security and privacy rules by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

HITECH also includes new limitations on the sale of protected health information, marketing, and fundraising communications; and stronger individual rights to access electronic medical records and restrict the disclosure of certain information.

Breach Notification Rule

Breach occurs when information that, by law, must be protected is:

- lost, stolen or improperly disposed of (i.e. paper or device upon which the information is recorded cannot be accounted for);
- "Hacked" into by people or mechanized programs that are not authorized to have access (e.g. the system in which the information is located is compromised through a "worm"), or
- Communicated or sent to others who have no official need to receive it (e.g. gossip about information learned from a medical record).

Report breaches

Part of everyone's responsibility is to report privacy or security breaches involving PHI. In most cases, before reporting a breach, a *risk assessment* must be done.

Risk Assessment

An impermissible use or disclosure of protected health information is presumed to be a breach unless the **covered entity** (see next page) or business associate, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the protected health information was actually acquired or viewed; and
4. The extent to which the risk to the protected health information has been mitigated.

Covered entities and business associates, where applicable, have discretion to provide the required breach notifications following an impermissible use or disclosure without performing a risk assessment to determine the probability that the protected health information has been compromised.

> **Covered entities** are defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which HHS has adopted standards.

Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals, the Secretary, and, in certain circumstances, to the media. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

- **Individual Notice** - Covered entities must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.
- **Media Notice** - Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.

FRAUD, WASTE, AND ABUSE (FWA)

Scope

This policy applies to all Hanna subcontractors. The provisions of this policy apply to any instance of fraud, waste, or abuse involving all company stakeholders including external organizations and contractors doing business with Hanna.

What is Fraud, Waste, and Abuse (FWA)?

Fraud

Intentionally submitting false information to the government or a government contractor in order to get money or a benefit.

Waste

Overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare program. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.

Abuse

Includes actions that may, directly or indirectly, result in unnecessary costs to the Medicare Program. Abuse involves payment for items or services when there is not a legal entitlement to that payment and the provider has not knowingly and/or intentionally misrepresented facts to obtain payment.

Commitment to Confidentiality and Anonymity

When you report, please remember the following concerning confidentially and anonymity:

- Even if you report anonymously, once the report has been filed and the investigation begins, anyone who is familiar with the situation you are reporting may still be able to guess your identity.
- Whether you report anonymously or not, the Hanna will treat your report confidentially.
- It is not possible to guarantee absolute confidentiality in all circumstances. Disclosure to others inside or outside Hanna may be required by law in certain cases.
- Please do not let these possibilities discourage you from reporting an incident.

Whistleblower Protection

Retaliation against someone who in good faith filed a report of alleged fraud, waste, or abuse, or who participated in an investigation, is a violation of this Policy.

Responsibilities for Subcontractors

Any Hanna subcontractor who has knowledge of fraud, waste, or abuse, or who has good reason to suspect that such conduct has occurred, shall adhere to the procedures in this Policy. When suspected fraudulent activity, waste, or abuse is observed by, or made known to, an subcontractor, he/she shall immediately report the activity to his/her direct supervisor. If the subcontractor believes that the supervisor is involved with the activity, he/she shall immediately report the activity to the supervisor's manager as well as the General Manager of the Department/Office. If the subcontractor believes that the supervisor's manager and/or the General Manager may be involved with the activity, he/she shall file a report via the Fraud, Waste, and Abuse Referral System (also known as the Fraud, Waste, and Abuse Hotline). See section of Policy titled "Filing a Report."The subcontractor shall not make any attempt to investigate the suspected activity prior to reporting it. Hanna shall coordinate investigations of fraud, waste, or abuse. Subcontractors who intentionally fail to report a known violation or fail to satisfactorily implement corrective actions may be suspended or terminated. A subcontractor shall not destroy, or allow to be destroyed, any document or record of any kind that the he/she knows may be relevant to a past, present, or future investigation.

Citizens and Customers

Hanna cannot compel citizens and customers (non-employees) to report suspected instances of fraud, waste, or abuse. However, Hanna strongly encourages them to do so.

Management's Responsibilities

Once management has been informed of suspected fraud, waste, or abuse (or if management itself suspects fraud, waste, or abuse), management shall either contact Hanna executive staff or file a report via the Fraud, Waste, and Abuse Referral System (also known as the Fraud, Waste, and Abuse Hotline)within two weeks of time. Conclusion of investigations of FWA must be done within a reasonable time after the activity is discovered.

FWA Compliance Requirements

Subcontractors should review FWA protocols within 90 days of contracting and annually thereafter. Subcontractors must certify that they have reviewed the CMS modules incorporated into Hanna's Business Associate Agreement provided upon on-boarding. Further documentation can always be requested by contacting Hanna at any time.

FWA Safeguards

Hanna and all Medicare Advantage Organizations are prohibited from using federal funds to pay for services, equipment or drugs prescribed or provided by a provider, supplier, employee or FDR excluded by the DHHS OIG or GSA. Medicare payment may not be made for items or services furnished or prescribed by an excluded provider, individual or entity. Hanna must review the DHHS OIG List of Excluded Individuals and Entities (LEIE list) and the GSA Excluded Parties Lists System (EPLS) prior to the hiring or contracting of any subcontractor, new employee, temporary employee, volunteer, consultant, Board member, or FDR, and monthly thereafter, to ensure that none of these persons or entities are excluded or become excluded from participation in federal programs. Monthly screening is essential to prevent inappropriate payment to providers, pharmacies, and other entities that have been added to exclusions lists since the last time the list was checked. After entities are initially screened against the entire LEIE and EPLS at the time of hire or contracting, sponsors need only review the LEIE supplement file provided each month, which lists the entities added to the list that month, and review the EPLS updates provided during the specified monthly time frame. In some cases, an organization or individual may be excluded altogether from participating in Medicare, Medicaid, or any other federal or state healthcare program. This generally occurs when the Department of Health and Human Services (DHHS) Office of Inspector General (OIG) does not believe that the organization or individual is trustworthy enough to adhere to federal and state healthcare program requirements and avoid fraudulent and abusive practices. Any Hanna employee, owner, or FDR found on the OIG List of Excluded Individuals/ Entities (LEIE) may have their job duties altered as necessary to preclude those individuals from having any involvement with state or federal programs, or have their employment or contract

terminated. OIG's LEIE includes all healthcare providers and suppliers that are excluded from participation in federal health care programs, including those health care providers and suppliers that might also be on the EPLS. In addition to healthcare providers (that are also included on the OIG LEIE) the EPLS includes non-health care contractors.

Use of Data Analysis

Hanna utilizes multiple methodologies to perform effective monitoring in order to prevent and detect FWA through the use of data analysis. We utilize personnel specifically trained to identify unusual patterns suggesting potential errors and/or potential fraud and abuse. Data analysis includes monitoring billing and utilization to detect unusual patterns. We also analyze data to detect potential FWA, including inappropriate billing and overpayments. Additionally, our Part C and D data analysis is used to identify potential errors that pose the greatest risk for potential FWA to the Medicare program including identifying overutilization, problem areas with data submission or finance, and to identify potential problem areas with FDRs.

Investigations

The Compliance Officer is responsible for leading, tracking and closing all investigations, recommends corrective actions or changes that need to be made. To the extent that the monitoring activities reveal conduct which could potentially constitute violations of the Hanna Code of Conduct, Medicare Compliance and FWA Plan, failure to comply with applicable state or federal law, and other types of misconduct, Hanna has an obligation to investigate the conduct in question immediately to determine whether any such violation has occurred, take action to discipline the person or persons involved, and correct the problem. It is expected that all subcontractors, owners and FDRs will cooperate with investigation efforts. Any suspected noncompliance or FWA report through the Compliance Hotline or any other mechanism is sent to the Compliance Officer for tracking, investigation and corrective or disciplinary action as necessary and applicable. All incidents receive a response (unless anonymous).The extent of the investigation will vary depending upon the concern. The assigned department will document responses to requests for information in investigations conducted and forward the findings to the Compliance Officer who will include a summary of the results in the Compliance Program Status Report. Under no circumstance is retaliation for discussing a compliance concern acceptable, which includes questions and concerns that are discussed with an immediate manager, oversight authority, or Compliance Officer. Issues reported that are not compliance related will be addressed by the assigned investigating department (i.e., reported issues constituting non-compliance with employment law and HR policies, will be addressed by Human Resources). Processes and procedures have been documented and are to be followed for investigation and documentation of compliance issues.

Remediation

The Compliance Officer develops a remediation plan when a compliance violation is detected. The plan is designed to prevent a recurrence of the violation. Remediation plans are developed on a case-by-case basis and may include:

- Additional or modified coaching and education
- Corrective action
- Development of new policies, processes and procedures
- Revision to existing policies, processes and procedures
- Revision of the Compliance Plan
- Additional monitoring and auditing
- Reporting to clients and/or outside agencies

The Compliance Officer is involved in the development of all remediation plans that

- Result from a significant compliance violation
- Affect multiple business units or shared services departments
- Involve revisions or additions to the Compliance Plan or company-wide policies and procedures

NBI Medic

Medicare Drug Integrity Contractors (MEDIC) are organizations that CMS contracts with to perform specific program integrity functions for Parts C and D under the Medicare Integrity Program. The MEDIC's primary role is to identify potential fraud and abuse in Medicare Part C and Part D. There is currently one National Benefit Integrity (NBI) MEDIC.NBI MEDICs will investigate referrals from sponsors, develop the investigations, and make referrals to appropriate law enforcement agencies or other outside entities when necessary. The NBI MEDIC will keep the sponsor apprised of the development and status of the investigation. If the NBI MEDIC determines a referral to be a matter related to noncompliance or mere error rather than fraud or abuse, the matter will be returned to CMS and/or the sponsor for appropriate follow-up.

Hanna's Compliance Officer upon completion of review of cases involving potential fraud or abuse may determine a need to report an incident that meet any of the following criteria to the NBI MEDIC:

• Suspected, detected or reported criminal, civil, or administrative law violations
• Allegations that extend beyond the Parts C and D plans, involving multiple health plans, multiple states, or widespread schemes
• Allegations involving known patterns of fraud
• Pattern of fraud or abuse threatening the life or well-being of beneficiaries
• Scheme with large financial risk to the Medicare Program or beneficiaries

Filing A Report

Please keep the following in mind when reporting via the hotline:

- If possible, report the issue to your supervisor or manager first.
- You must be able to provide adequate information to support an investigation. Mere speculation does not suffice.
- Your report must be made in good faith. Knowingly making a false or bad faith complaint will be subject to disciplinary and/or legal action.

How to report potential noncompliance:
Suspected Fraud, Waste, & Abuse or other noncompliance may be reported by:

- Anonymously Emailing:
  info@hannais.com
- Calling
  Medi-Cal (800) 822-6222
  Medicare (800) 447-8477 or (800) HHS-TIPS