CCHP Health Plan

HIPAA, HITECH Act, and Final Rule / Regulations

Compliance Department

Reporting Potential HIPAA Incidents, Breaches, or Non-Compliant Issues

Greg Gertz, JD, MPH, CHC
CCHP Chief Compliance Officer
Greg.gertz@cchphealthplan.com
(628) 228 - 3207

CCHP must have a mechanism for reporting potential HIPAA breaches or non-compliant issues by the CCHP employees, contracted providers, and other contractors. CCHP must accept anonymous reports and cannot retaliate against good-faith reporting.

- Report HIPAA Incidents or potential breaches. When in doubt, call the CCHP's Chief Compliance Officer, Compliance Department or the CCHP Compliance Hotline.

CCHP Compliance Dept: CCHPComplinanceDept@cchphealthplan.com

CCHP Compliance Hotline is: 415 – 955 – 8810, 24/7

Contents

Overview of HIPAA, HITECH, and Final Rule

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted as Public Law 104-191 on August 21, 1996. Among its mandates, HIPAA required the Secretary of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy and security of health information. These provisions are known as the Administrative Simplification rules.
HIPAA also required the HHS Secretary to issue privacy regulations governing individually identifiable health information. The final version known as the Privacy Rule, was published December 28, 2000. The Privacy Rule governs healthcare entities that have access to protected health information (PHI). Final modifications to the Privacy Rule were published on August 14, 2002.

In addition, to the Privacy Rule, HIPAA also required the Secretary to issue security regulations to protect the integrity, confidentiality, and availability of electronic PHI (e-PHI). The final regulation, the Security Rule, was published February 20, 2003. The Security Rule ensures that only those who are authorized to have access to an individual's e-PHI actually do have access. The Security Rule specifies a series of administrative, technical, and physical security procedures for covered entities to ensure the confidentiality, integrity, and availability of electronic protected health information.

In 2009, the passage of the American Recovery Reinvestment Act of 2009 (ARRA) led to additional modifications to HIPAA – those contained in the Health Information Technology for Economic and Clinical Health Act (HITECH Act). One of the goals of ARRA is to prepare for the government aim of establishing secure electronic health records for all Americans by 2014. As a result, concern for the security of e-PHI is even greater.

So among the changes, HITECH expands the regulations for what happens if unauthorized individuals obtain access to e-PHI. Known as a "breach," this occurrence triggers the need for "breach notifications." In addition, the privacy and security requirements have been strengthened for organizations that process or otherwise handle e-PHI known as "business associates."

Overview of HIPAA, HITECH, and Final Rule

The ARRA modifies HIPAA regulations in three broad categories:

(1) Breach Notifications

(2) Business Associates

(3) Penalties

More specifically, HITECH strengthens the HIPAA privacy, security and enforcement rules and increases the penalty amounts the HHS Secretary may impose for violations of HIPAA rules.

On January 17, 2013, the HHS Office of Civil Rights (OCR) released its omnibus rule, also known as the Final Rule. This rule further modifies the HIPAA privacy, security, enforcement and breach notification rules required by HITECH as well as modifications required by the Genetic Information Nondiscrimination Act of 2008 (GINA). The Final Rule became effective as of March 26, 2013; however, covered entities and business associates were given until September 23, 2013, to comply with most Final Rule requirements.

CCHP Health Plan

Privacy and Security Rule: Permitted Use and Disclosure

Every person has a basic right to expect that their PHI remains private – that is, their personal health information will be kept from being shared with or used by those not authorized to do so. Therefore, HIPAA, as modified by the HITECH Act and the Final Rule, spells out the circumstances where the sharing of PHI is permitted and where it is not permitted. First and foremost, the Privacy Rule applies to covered entities, and parts of it apply to those covered entities' business associates.

Privacy and Security Rule: Permitted Use and Disclosure - 1

“Covered Entities” include healthcare providers, health plans and healthcare clearinghouses. In more detail:
Healthcare providers are defined as any provider that electronically transmits health information pursuant to standard healthcare transactions; (e.g., doctors, clinics, dentists, chiropractors, nursing homes, pharmacies, psychologists…but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard).

Health plans are defined as individual and group plans that provide or pay the cost of medical care; (e.g., HMOs, government programs that pay for health care, such as Medicare, Medicaid, veterans health care program, health insurance companies, and the military.)

Healthcare clearinghouses are defined as entities that process nonstandard information received from another entity into a standard format (standard electronic format or data content), or vice versa.
A covered entity may not use or disclose PHI, except either:

As Privacy Rule permits or requires; or
As the individual who is the subject of the information (or the individual’s personal representative) authorizes in writing.

Privacy and Security Rule: Permitted Use and Disclosure - 2

Required Disclosures. A covered entity must disclose PHI:
To individuals (or their personal representatives) specifically when they request access to, or accounting of disclosures of, their PHI;
To HHS when it is undertaking a compliance investigation or review of enforcement action;
When otherwise required by law, and the disclosure is permitted by HIPAA, such as pursuant to a court order.

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose PHI (subject to limitations), without an individual's authorization, for the following purposes or situations:
To the individual (unless required for access or accounting of disclosures);
For treatment, payment, and healthcare operations;
When the opportunity to agree or object is provided;
Incident to an otherwise permitted use and disclosure;

For public interest and benefit activities; and
When part of a limited data set for the purposes of research, public health or healthcare operations.
Covered entities may rely on professional ethics and best judgements in deciding which of these permissive uses and disclosures to make.

Privacy and Security Rule: Permitted Use and Disclosure - 3

Required Disclosures. A covered entity must disclose PHI:
To individuals (or their personal representatives) specifically when they request access to, or accounting of disclosures of, their PHI;
To HHS when it is undertaking a compliance investigation or review of enforcement action;
When otherwise required by law, and the disclosure is permitted by HIPAA, such as pursuant to a court order.

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose PHI (subject to limitations), without an individual's authorization, for the following purposes or situations:
To the individual (unless required for access or accounting of disclosures);
For treatment, payment, and healthcare operations;
When the opportunity to agree or object is provided;
Incident to an otherwise permitted use and disclosure;

For public interest and benefit activities; and
When part of a limited data set for the purposes of research, public health or healthcare operations.
Covered entities may rely on professional ethics and best judgements in deciding which of these permissive uses and disclosures to make.

Privacy and Security Rule: Permitted Use and Disclosure - 4

I. Treatment, Payment, Healthcare Operations (TPO). A covered entity may use and disclose PHI for:
Covered entity's owns treatment, payment, and healthcare operations activities, where:

- Treatment = the provision, coordination, or management of healthcare and related services for an individual by one or more healthcare providers.
- Payment = encompassing activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for healthcare delivered to an individual.
- Healthcare operations = any of the following activities:

1. Quality assessment and improvement activities, including case management and care coordination.
2. Competence assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation.
3. Performance of medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs.
4. Specified insurance functions, such as underwriting, risk rating, and reinsuring risk.
5. Business planning, development, management, and administration.
6. Treatment activities of any healthcare provider.
7. Payment activities of another covered entity and of any healthcare provider.

Healthcare operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities so long as both covered entities have or had a relationship with the individual.

II. Uses and Disclosures with Opportunity to Agree or Object.

Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiese, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgement, the use or disclosure is determined to be in the best interests of the individual. Such occasions may include:

Facility Directories. It is common practice in many healthcare facilities, such as hospitals, to maintain a directory of patient contact information. A covered healthcare provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility. The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy.

For Notification and Other Purposes. An individual's informal permission may be relied upon by a covered entity in order to disclose to the individual's family, relatives or friends (actually, to ANYBODY the individual informally indicates).

III. Incidental Use and Disclosure.
The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated. If use or disclosure is “incident to,” an otherwise permitted use or disclosure, then the incident to disclosure is permitted as long as reasonable safeguards in conformity with the Privacy Rule exist and the disclosure is limited to “minimum necessary,” conforming to the Privacy Rule.

IV. Disclosure for Public Interest/Benefit. Covered entities may disclose for 12 national priority purposes:

1. Required by law.
2. Public health activities.
3. Victims of abuse, neglect or domestic violence.
4. Health oversight activities.
5. Judicial and administrative proceeding.
6. Law enforcement purposes.
7. Decedents.
8. Organ procurement/donation.

III. Incidental Use and Disclosure.
The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated. If use or disclosure is "incident to," an otherwise permitted use or disclosure, then the incident to disclosure is permitted as long as reasonable safeguards in conformity with the Privacy Rule exist and the disclosure is limited to "minimum necessary," conforming to the Privacy Rule.

IV. Disclosure for Public Interest/Benefit. Covered entities may disclose for 12 national priority purposes:

1. Required by law.
2. Public health activities.
3. Victims of abuse, neglect or domestic violence.
4. Health oversight activities.
5. Judicial and administrative proceeding.
6. Law enforcement purposes.
7. Decedents.
8. Organ procurement/donation.

. Research

10. Serious threat to health or safety.
11. Essential government functions.
12. Worker's compensation.

CCHP Health Plan

Privacy and Security Rule: Authorized Use and Disclosure

Privacy and Security Rule: Use and Disclosure - 1

I. Authorization. Covered entities must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or healthcare operations or otherwise permitted. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility upon an individual granting an authorization. Some limited exceptions do exist (recommend to seek advise of an attorney on limited exceptions). **An authorization must:**

1. Contain specific terms.
2. Limit use and disclosure to a covered entity or a third party.

All authorizations must be in plain language, and contain the following:

1. A description of the PHI to be used or disclosed.
2. The name or other specific identification of people authorized to make use of the PHI.
3. The purpose of each requested use or disclosure.
4. The expiration date of the authorization.
5. The signature and date signed by the individual.
6. A statement informing the individual of the right to revoke the authorization in writing.
7. A description of any restrictions on the individual's right to revoke with instructions for how to do so.
8. An indication of whether the signing of the authorization can be a pre-condition to the individual's treatment.
9. A statement informing the individual that the recipient of the PHI may re-disclose the date in a manner that makes it no longer protected.

Privacy and Security Rule: Use and Disclosure - 2

II. Minimum Necessary. "Minimum necessary" use and disclosure means that a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request.

To ensure minimum necessary is achieved:

1. Develop and implement policies and procedures to reasonably limit uses and disclosure.
2. Do not use, disclose, or request the entire medical record for a particular purpose, unless the entire record is absolutely required.

Minimum necessary doesn't apply in the following circumstances:

1. Disclosure to or a request by a healthcare provider for treatment.
2. Disclosure to an individual who is the subject of the information or the individual's personal representative.
3. Use or disclosure made pursuant to an authorization.
4. Disclosure to HHS for complaint investigation, compliance review or enforcement.
5. Use or disclosure required by law.
6. Use or disclosure required for compliance with other regulations.

Privacy and Security Rule: Use and Disclosure - 3

III. Individual Rights. The rights of individuals with respect to PHI have been enhanced by the Final Rule. For example, individuals have the right to examine and request disclosure restrictions of their protected health information. Covered entities must comply with these rights as requested by an individual.
To ensure compliance with the Privacy Rule with respect to expanded individual rights, healthcare professionals, covered entities and business associates should follow these guidelines.

Individual Rights	Action By Individual	Action by Covered Entity
Right to Restrict Disclosures	Individual requests no sharing of PHI with his or her provider(s) and/or health plan for payment, treatment or healthcare operations when service is paid by the individual-out of pocket.	Covered entity must establish a system to distinguish restricted PHI to avoid an inadvertent disclosure by the covered entity.
Right to Access	Individual requests access to/copies of his/her PHI.	If maintained electronically, covered entity must provide the individual with a copy of his/her PHI in electronic form on in the form and format that the individual requests if readily producible. If the information is not readily producible, the covered entity must provide the information in a readily readable format as agreed to by the individual and the covered entity. This request can be denied if fulfilling it might expose an individual to substantial risk.

Privacy and Security Rule: Use and Disclosure - 4

Individual Rights	Action By Individual	Action by Covered Entity
Right to Share PHI with Third Parties	Individual requests that his/her PHI be sent to another person designated by the individual. The request must be in writing, signed by the individual and clearly identify the person, including address, to whom the information is to be sent.	The covered entity must transmit the information as designated by the individual.
Right to Reasonable Fees	Individual requests access to/copies of his/her PHI.	The covered entity may charge reasonable cost-based fees for providing electronic copies of PHI to an individual or their designee.
Right to Amendment of PHI	Individual requests that inaccurate or incomplete information in medical record be corrected.	If information is found to be inaccurate or incomplete, the covered entity may correct the record in a manner consistent with the entity's policies and procedures. The entity may deny the request if it determines the record is correct and incomplete; if the information was not generated by the covered entity; or if the information is that to which he or she is not entitled to have access.

Privacy and Security Rule: Use and Disclosure - 5

Individual Rights	Action By Individual	Action by Covered Entity
Right to Timeliness	Individual requests copies of his/her PHI.	The covered entity must provide the requested information within 30 days of the individual's request. A one-time 30-day extension is allowed if the individual is notified of the extension request within the original 30-day timeframe and a reason for the delay and expected completion date is provided to the individual within the request.
Right to Accounting Disclosure	Individual requests an accounting of who has received his or her PHI.	An accounting is not required if disclosure was: • For Treatment, Payment, and Operations (TPO) • An incidental disclosure • Made in a limited data set • Made with an authorization from the individual • Made for national security purposes • A disclosure to the subject of the information • A disclosure that only required giving the individual an opportunity to object • A disclosure to a correctional institution or other law enforcement official having custody of the individual.

Privacy and Security Rule: Use and Disclosure - 6

Individual Rights	Action By Individual	Action by Covered Entity
Right to Receive Notice of Privacy Practices (NPP)	Not Applicable	Covered entities must revise and redistribute their NPP for PHI. The revisions must include statements addressing: • The use and disclosure of psycho-therapy notes, uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of protected health information; • That any uses and disclosures not described in the NPP will only be made with prior authorization; • An individual's right to opt out of receiving fundraising communications; • An individual's right to restrict certain disclosures of PHI if the service(s) covered in the PHI are paid for out of pocket; • The duty of a covered entity to notify affected individuals of a breach of unsecured PHI; • That disclosure of genetic information for underwriting purposes is prohibited.

CCHP Health Plan

Privacy and Security Rule: Business Associates

Note: Persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of PHI, and where any access to PHI by such persons would be incidental, if at all

Privacy and Security Rule: Business Associates - 1

I. **Business Associates.** The Privacy Rule allows covered entities to enter into contractual arrangements with business associates to perform PHI-related work or services on behalf of a covered entity. This is allowed only so long as the business associate protects the PHI as outlined in the agreement with the covered entity and as outlined in HIPAA and HITECH Act. Prior to HITECH and the Final Rule, business associates were not held directly liable for a violation of HIPAA– the business associate contract governed enforcement and penalties for business associates. Through the Final Rule, business associates (and business associates' subcontractors) **are now held directly liable** for many provisions of the Privacy Rule and Security Rule.

"Business Associates" are persons or organizations that perform certain functions or services that involve the use or disclosure of PHI. **These involve:**

Functions on behalf of a covered entity—which may include claims processing, data analysis, utilization review and billing.

Services to a covered entity, which may include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services.

The following specific entities (as detailed by the Final Rule):

1.Subcontractors
2.E-prescribing gateways (electronic prescription services)
3.Vendors of personal health records that provide services to a covered entity.
4.Patient safety organizations.
5.Health Information organizations (generally includes organization that oversee and govern the exchange of health-related information among organizations).

Privacy and Security Rule: Business Associates - 2

II. Business Associate Agreements. The Final Rule establishes direct liability for business associates, which must be spelled out in a formal business associate agreement. The required elements of a business associate agreement has been expanded, such that they now must require:

Conforming to the same standards as those of the covered entity for protecting PHI (including completion of a risk assessment and implementation of a risk assessment plan);
Compliance with the Security Rule (where applicable);
Reporting breaches of unsecured PHI to covered entities;
Assurance that subcontractors creating or receiving PHI on behalf of a business associate agree, in writing, to meet the same, or more stringent, restrictions and conditions that apply to the business associate; and
Assurance that any compliance obligations delegated to the business associate via the business associate agreement are performed in compliance with the Privacy Rule.

Background Information:
The Final Rule established a transition period that allowed covered entities and business associates to operate under their existing agreements for up to one year after the compliance date of September 23, 2013. In other words, covered entities and business associates had until September 22, 2014,to revise their existing contracts to comply with the expanded provisions.

Privacy and Security Rule: Business Associates - 3

III. Direct Liability. Business associates are now held directly liable for uses and disclosures of PHI that are not as set forth in their business associate agreements and in the Privacy Rule (and Security Rule, where applicable). Specifically, business associates are held directly liable for the following:

Failing to disclose PHI when required by the HHS Secretary to do so; such instances would be requested by the HHS Secretary to investigate and determine the business associate's compliance with HIPAA rules;
Failing to disclose PHI to the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations to meet an individual's request for an electronic copy of his or her PHI;
Failing to make reasonable efforts to limit PHI access to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
Failing to enter into business associate contracts with subcontractors that create or receive PHI on behalf of the business associate;
Failure to comply with all other Privacy Rule obligations that are included in their contracts or other arrangements with covered entities.

IV. Agency Liability. The Final Rule establishes that HHS will also hold covered entities liable for the actions of a business associate, if that associate qualifies as an agent. Per the Final Rule, an agency relationship exists if the principal (covered entity) has the authority to control the conduct of the agent in the performance of the agent's duties. If that authority is lacking, then an agency relationship does not exist, and the covered entity cannot be held liable for the business associate's actions. Covered entities should keep this in mind when revising/updating their business associate agreements. If no agency relationship exists, a business associate agreement should clearly indicate that the parties are independent contractors and not agents of each other. If an agency relationship exists, the covered entity should ensure that it is monitoring the business associate's compliance obligations effectively.

Privacy and Security Rule: Business Associates - 4

V. Subcontractors. A subcontractor of a business associate that creates, receives, maintains or transmits PHI on behalf of a business associate is now considered a business associate and therefore can be held liable for any violations to HIPAA, HITECH and Final Rule regulations. Covered entities, however, are not required to establish formal agreements with subcontractors of business associates. Instead, the covered entity's business associate is responsible for securing written agreements with its subcontractors.

CCHP Health Plan

HIPAA Security Rule

HIPAA Security Rule - 1

Security Rule. The HIPAA Security Rule requires covered entities and business associates to ensure the security of e-PHI, which means protecting the confidentiality, integrity and availability of all e-PHI created, received or maintained by the covered entity or business associate.

Confidentiality means protecting information from being made available or disclosed to unauthorized persons or processes.

Integrity means the data is kept safe from unauthorized alteration or destruction.

Availability means data is accessible and usable for the covered entity's TPO needs or upon an authorized request.

Covered entities and business associates are also required to protect all e-PHI from any anticipated threats or unauthorized uses or disclosures of e-PHI. These goals are accomplished by instituting certain required administrative, technical and physical safeguards. Generally, these safeguards are developed and managed by Information Technology (IT) personnel. Basic understanding of the security measures is required, since some will have impact on frontline healthcare workers and staff. These safeguards include, but are not limited to:

Administrative Controls. This includes policies to prevent, detect, contain, and correct security violations; sanction policies; risk analyses; workforce security policies and procedures; security and awareness training for the workforce; and, business associate contracts.

HIPAA Security Rule - 2

Physical Controls. This includes facility access controls; workstation usage controls; and device and media controls.

Technical Controls. This includes access controls; audit controls; user authentication; and transmission security.

Provisions of the Security Rule that will impact day-to-day work generally relate to the usage of workstations and portable devices. Notably, all computer users are required to have a unique user-name and password that must not be shared with others. In addition, portable devices and media that offer access to ePHI must be kept safe from access by unauthorized persons. For instance, if a clinician takes home a laptop with access to ePHI, he or she will be expected to ensure that the laptop is used and stored securely. A covered entity's policies and procedures will likely specify the steps required for ensuring such security.

CCHP Health Plan

HIPAA Breach Notification Standards

HIPAA Breach Notification Standards - 1

When unauthorized individuals get access to e-PHI, the data breach can have a devastating effect on a covered entity or business associate. Whether the breach affects one (1) individual or 1,000, the **penalties are severe**, especially if it is found that the breach was the result of willful negligence.

The Final Rule dictates that a breach is presumed to have occurred whenever acquisition, access, use, or disclosure of PHI happens in a manner not permitted by the HIPAA Privacy Rule. A breach notification is then **required** unless a covered entity or business associate can demonstrate through a **risk assessment** that there is a low probability that the PHI's security or privacy has been compromised.

Once a breach is discovered, and the covered entity or business associate cannot demonstrate that there is a low probability that the PHI's security or privacy has been compromised, **timely notification** by the covered entity (or business associate, if applicable) to the affected individuals, the Secretary and, in some cases, the media, is imperative. Generally, following the discovery of a breach, covered entities are to notify each affected individual whose unsecured protected information has been, or it is believed to have been, accessed, acquired, used, or disclosed.

The discovery of a breach is **defined** as the first day the breach becomes known to the covered entity (or business associate) or, if by exercising reasonable diligence, it would have become known to the covered entity (or business associate).

HIPAA Breach Notification Standards - 2

Timeliness.
Breach notification timeliness standards for covered entities **are as follows**:

To the affected individual: Without unreasonable delay and **no later than 60 days** after the discovery of the breach.

To the media (only if affected individuals total 500 or more): Without reasonable delay and no later than 60 days after discovery of breach.

To the HHS Secretary:
For instances involving *500 or more affected individuals*, without reasonable delay and no later that 60 days after the discovery of a breach in a manner as specified by the HIPAA Privacy and Security Rules and HITECH Act.
For instances involving less than 500 affected individuals, covered entities shall maintain a log or other documentation of breaches and, not later than 60 days after the end of each calendar year, provide the required notification in the manner as specified by the HIPAA Privacy and Security Rules and HITECH Act.

HIPAA Breach Notification Standards - 3

Elements of Notification. The notification to affected individuals must include:
A brief description of how the breach occurred;
A description of the type(s) of unsecured PHI involved in the breach;
Steps the individual should take to protect himself/herself from potential harm as a result of the breach;
A description of what the covered entity is doing to investigate; and
Contact procedures if the individual has questions.

Business associates are to **notify the covered entity** upon the discovery of a breach of unsecured PHI. The discovery of a breach by a business associate is defined similarly as that for a covered entity and includes discovery of a breach by an employee of the business associate. Notification to the covered entity **must occur** without reasonable delay and in no case longer than 60 days after the discovery of the breach. The notification to the covered entity must include the identification of each affected individual and any other available information.

CCHP Health Plan

HIPAA Marketing, Fundraising, and Research

HIPAA Marketing, Fundraising, and Research - 1

I. Marketing. A communication about a product or service is considered marketing when the recipients are encouraged to purchase or use that product or service. Patient authorizations are required for all marketing communications related to treatment and healthcare operations when the covered entity receives direct or indirect financial remuneration for the communications from the party whose product or service is the subject therein; (e.g., if a company that manufacturers radiology equipment pays a covered entity to market their machines to oncology patients).
This requirement means that before such a mailing can be sent to patients, the covered entity must get an authorization from each patient, the covered entity must get authorization from each patient who is to receive the mailing. An exception exists for prescription drugs, provided the payment for the communication is reasonably related to the covered entity's cost of executing communication.

II. Fundraising. The Final Rule has expanded the categories of PHI that may be used and disclosed for fundraising purposes. Therefore, a covered entity can use or disclose demographic information, dates of service, department of service, treating physician, outcome information and health insurance information to better target its fundraising efforts. However, covered entities are now required to provide individuals with a "clear and conspicuous" opportunity to opt out of receiving future fundraising communications and may not send communications to those individuals who opt out. They can, though, offer an individual who has opted out of fundraising communications with a method to opt back in. But a covered entity may not condition treatment on the decision an individual makes regarding opting out.

HIPAA Marketing, Fundraising, and Research - 2

III. Research. While PHI disclosure authorization is generally not permitted to serve as a condition for treatment, a significant exception exists in the case of clinical research. A covered entity may condition research-related treatment on the execution of an authorization to use and disclose the individual's PHI in the research. What's more, covered entities are now allowed to combine conditioned and unconditioned authorizations for research purposes. The authorizations must clearly note the difference between the conditioned and unconditioned components of the research and provide each individual with the opportunity to opt-in to unconditioned activities. In addition, covered entities may now request authorization from research subjects to use their PHI data in future research studies, provided the authorization offers a description offers a description of the purpose of the future research.

CCHP Health Plan

Additional Information - Privacy

Privacy – Additional Information - 1

I. Sale of PHI.

The sale of PHI is, generally, a disclosure of PHI by a covered entity or business associate for which that entity receives payment from the recipient of the PHI.
Covered entities are required to obtain authorization from a patient for the sale of his or her PHI. Exceptions to this rule are:

1. Public health activities.
2. Research purposes in certain circumstances.
3. Treatment and payment purposes.
4. Sale, transfer or merger of all or part of a covered entity.
5. Services rendered by a contracted business associate at the request of a covered entity.
6. Provision of access to an individual his or her own PHI or an accounting of the disclosures of his or her PHI.
7. Disclosures required by law.
8. Other purposes deemed necessary and appropriate by HHS.

Background Information:
Authorizations that existed prior to the Final Rule compliance date (September 23, 2013) were honored for up to one year from the compliance date of the Final Rule (September 22, 2014) if the authorizations were not modified.

Privacy – Additional Information - 2

II. Child Immunizations.
The Final Rule allows covered entities to disclose, without written authorization, proof of immunization to a school, provided the State where the school resides requires the school to have the immunization records prior to admitting students. This provision does not apply to adult students or students deemed emancipated.

III. Decedent Health Information.
Covered entities must continue to comply with the Privacy Rule's requirements for the decedent health information but are only required to do so for 50 years following the individual's death. The Final Rule also permits covered entities to disclose decedent health information to family members or others involved in the individual's healthcare prior to the death of the individual.

IV. Genetic Information.
Pursuant to the Final Rule, genetic information is considered health information. As such, all types of health plans, except long-term care policies, are prohibited from using genetic information for underwriting purposes. A health plan that intends to use PHI for underwriting purposes must add a statement to its NPP stating that it will not use genetic information for underwriting purposes.

CCHP Health Plan

HIPAA ENFORCEMENT and PENALTIES

HIPAA ENFORCEMENT and PENALTIES - 1

The Final Rule extends HHS' enforcement reach to business associates (including their subcontractors), which means business associates are now subject to civil money penalties and other enforcement actions. Also established is a tiered liability system for HIPAA violations. That means a wrongful disclosure of PHI is subject to different levels of penalties, depending on whether reasonable cause or willful neglect occurred. These levels are defined as follows:

Reasonable cause applies to an action or omission in which a covered entity or business associate knew, or by exercising reasonable diligence would have known, that the action or omission violated a HIPAA provision. Note that **reasonable diligence** means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

Penalty: between $1K and $50K for each violation, with a maximum penalty of $1.5 million in yearly liability for identical violations.

Willful neglect applies to a conscious, intentional failure or reckless indifference toward compliance with a HIPAA provision.

Penalty: if covered entity corrected the violation within 30 days of knowledge of the violation: between $10K and $50K for each violation, with a maximum penalty of $1.5 million in yearly liability for identical violations;

Penalty: If covered entity did not correct the violation with 30 days of knowledge of the violation: at least $50K for each violation, with a maximum penalty of $1.5 million in yearly liability for identical violations.

HHS has wide latitude in determining a specific entity's penalties, **based on factors** such as the number of people affected, the nature of the harm caused, the history of the entity's prior noncompliance, and the financial condition of the entity.

CCHP Health Plan

HIPAA DEFINITIONS

HIPAA DEFINITIONS - 1

Breach: the acquisition, access, use or disclosure of protected health information in a manner not permitted under the HIPAA Privacy Rule that compromises the security or privacy of the protected health information. A disclosure is presumed to be a breach unless a covered entity or business associate can demonstrate, based on a risk assessment, that there is a low probability the PHI has been compromised.

Business Associate: a person or entity who, on behalf of a covered entity, other that in the capacity of a member of the workforce of the covered entity, creates, receives, maintains, or transmits protected health information for a function or activity regulated by 45 Code of Federal Regulations (CFR) Part 160, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management and repricing. A business associate is also a person or entity who, other than in the capacity of a member of the workforce of the covered entity, provides legal, actuarial, accounting, consulting and management services to or for the covered entity.

A business associate is also a person or entity who, other than in the capacity of a member of the workforce of the covered entity, provides legal, actuarial, accounting, consulting and management services to or for the covered entity.
A covered entity may also be a business associate of another covered entity.

A business associate **includes** (i) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to PHI to a covered entity; (ii) a person that offers a personal health record to one or more individuals on behalf of a covered entity; and (iii) a subcontractor that creates, receives or transmits PHI on behalf of the business associate.

HIPAA DEFINITIONS - 2

A business associate *does not include:* (1) a healthcare provider, with respect to disclosures made to the healthcare provider by a covered entity concerning treatment of the individual; (2) a plan sponsor, with respect to disclosures by a group health plan, health insurance issuer or HMO, to the plan sponsor to the extent that certain requirements apply and are met; (3) a government agency, with respect to determining the eligibility for our enrollment in a government health plan; and (4) in some instances, a covered entity participating in an organized healthcare arrangement that performs certain covered services.

Civil Money Penalty: a monetary penalty imposed by the HHS Secretary upon a covered entity or business associate if the Secretary determines that the covered entity or business associate has violated an administrative simplification provision. The amount of the civil money penalty is determined according to 45 CFR §160.404.

De-identified Health Information: health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual.

Disclosure: the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Electronic Media: (i) electronic storage material on which data is or may be recorded electronically; and (ii) transmission media used to exchange information already in electronic storage media.

HIPAA DEFINITIONS - 3

Genetic Information: with respect to an individual, (i) the individual's genetic tests; (ii) the genetic tests of family members of the individual; (iii) the manifestation of a disease or disorder in family members of an individual; or, iv) any request for, or receipt of, genetic services, by the individual or any family member of the individual.

Genetic Services: (i) a genetic test; (ii) genetic counseling; or (iii) genetic education.

Healthcare: care, services, or supplies related to the health of an individual, including, but not limited to: preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care and counseling of an individual or care that affects the structure or function of the body, and the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Healthcare clearinghouse: a public or private entity, including but not limited to, a billing service, repricing company or a community health management information system that processes or facilities the processing of health information received from another entity is a standard or nonstandard format.

Healthcare Provider: as defined in section 1861(u) of the Social Security Act and, generally, a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for healthcare in the normal course of business.

Health Information: any information, including genetic information, whether oral or recorded in any form or medium that is created or received by, but not limited to, a healthcare provider, health plan or healthcare clearinghouse and relates to the past, present or future physical or mental health or condition of an individual.

HIPAA DEFINITIONS - 4

DHHS: United States Department of Health and Human Service.

Individually Identifiable Health Information: a subset of health information, including demographic information, collected from an individual.

Limited Data Set: PHI that excludes certain direct identifiers of an individual or of relatives, employers or household members of an individual.

Minimum Necessary Standard: requires a covered entity to make a reasonable effort to limit access to PHI to those persons who need access to PHI to carry out duties and to disclose an amount of PHI reasonably necessary to achieve the purpose of a disclosure.

Notice of Privacy Practices (NPP): notice of the uses and disclosures of PHI that may be made by covered entity, and of the individual's rights and the covered entity's legal obligations with respect to PHI.

Protected Health Information (PHI) /Electronic PHI (PHI/ePHI): individually identifiable health information that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or, (iii) transmitted or maintained in any other form or medium. PHI/e-PHI excludes individually identifiable health information: (a) in education records covered by the Family Educational Rights and Privacy Act, as amended, 20 United States Code (U.S.C) 1232g; (b) in records described at 20 U.S.C. 1232g(a)(4)B)(iv); (c) in employment records held by a covered entity in its role as employer; and (iv) regarding a person who has been deceased for more than 50 years.

HIPAA DEFINITIONS - 5

Secretary: Secretary of the U.S. Department of HHS.

Subconractor: a person t whom a business associate delegates a function, activity, or service other than an employee of the business associate.

Transaction: the transmission of information between two parties to carry out financial or administrative activities related to healthcare (i.e., healthcare claims or encounter information, healthcare payment or remittance advice, etc.).

Unsecured Protected Health Information: PHI that is not rendered unusable, unreadable or undecipherable to unauthorized persons through the use of technology or methodology specified by the HHS Secretary.

Use: with respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information with an entity that maintains such information.

REFERENCES

45 CFR Part 160 and Part 164, Subparts A, C, and E

45 CFR §164.522; §164.524; §164.526; §164.528;§164.520;1§64.404(a)(1)(2); §164.404(b);§164.404(c); §164.506(b); §164.5085(a); §164.508(a)(4); §164.508(b); §164.508(b)(3); §164.408(c); §164.410; §164.501; §164.514(f);§164.532(f); §164.502(f); §164.502(a)(5)(i); §164.401; §164.402; §164.514(e)(2)(i) through (xvi); §164.514(d)(1) through (5); and,§164.520(1).


THE END
THAT'S ALL FOLKS
"That's all folks!"