HIPAA Overview

02TRGINT000008 Rev: 006 Effective: March 18, 2010
Reviewer: Rick Schupp Approver: Sandy Adams

What is HIPAA?

- **Passed in 1996 by the US Congress, the Health Insurance Portability and Accountability Act (HIPAA) created a set of uniform standards relating to security, privacy and data which had several main objectives; here are just a few:**
  - To improve portability and continuity of health coverage when employees change jobs
  - To combat waste, fraud and abuse in health insurance
  - To simplify the administration of health insurance
  - To protect the privacy and security of health information

What is HIPAA? Myth and Fact

- MYTH:
  - The HIPAA "Privacy Rule" is really a "Disclosure Rule"; HIPAA took away privacy rights that are based in the US constitution and common Law
- FACT:
  - Prior to HIPAA, there was no national health privacy law, and there were no limits on how health care providers, employers or insurers collected and shared health information, both within and outside the healthcare system. There was no federal right granting people access to their health information.
  - The Privacy Rule:
    - *Requires health care providers to give individuals notice of their rights and to inform them about how their health information will be used*
    - *Grants individuals the right to see and copy their own medical records*
    - *Imposes limits on disclosing patient records to employers, marketers, etc.*
    - *Authorizes civil and criminal penalties for violations of health privacy*

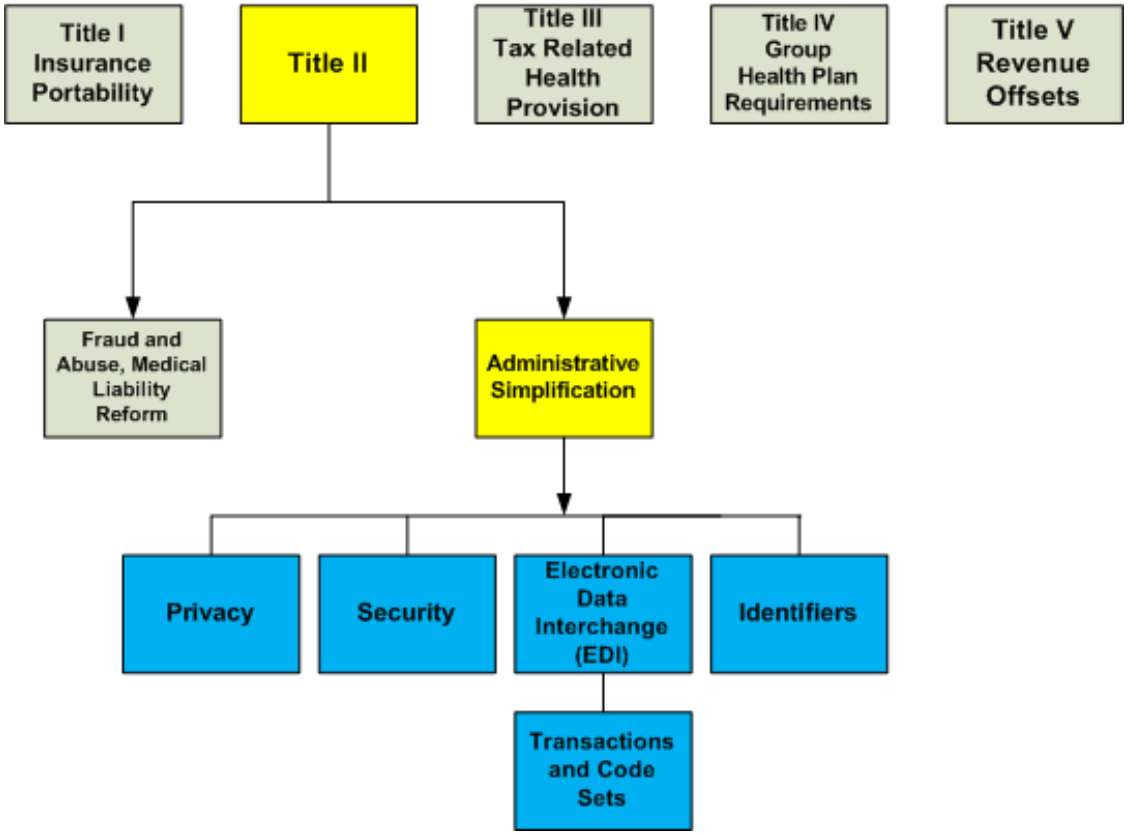
HIPAA – the Titles

- There are five main titles included in HIPAA:
  - Title I: Health care access, portability, and renewability
  - Title II: Preventing health care fraud and abuse, **administrative simplification**, medical liability reform
  - Title III: Tax-related health provisions
  - Title IV: Application and enforcement of group health plan requirements
  - Title V: Revenue offsets

THIS COURSE FOCUSES ON THE ADMINISTRATIVE SIMPLIFICATION SECTION OF TITLE II

HIPAA Title II

The following diagram illustrates the titles within HIPAA and, in particular, the Administrative Simplification sections within Title II:



Title II deals with the standardization of healthcare-related information systems.

HIPAA – Administrative Simplification Rules

HIPAA became effective using a phased approach, so that the health care industry could implement the different provisions of the regulation over time.

- Code Sets and Transactions Rule
  - *Passed on October 16, 2000*
  - *Established a standardized means for transmitting healthcare transactions*
- Privacy Rule
  - *Passed on April 14, 2001 (Revised August 14, 2002)*
  - *Set national standards for the protection of health information in all forms*
- Security Rule
  - *Passed on February 20, 2003*
  - *Set national security standards for maintaining the confidentiality, integrity and availability of electronic Protected Health Information (ePHI)*
- American Reinvestment and Recovery Act (ARRA)/HITECH Provisions
  - *Passed on February 17, 2009*
  - *Established, among other things, breach notification requirements and additional responsibilities for business associates to comply with the Security Rule and portions of the Privacy Rule or face penalties. Prior to ARRA, business associates were not directly regulated by HIPAA.*

HIPAA – Covered Entity

Covered Entity:

- The entities directly regulated by HIPAA. These include health care providers, health plans and clearinghouses.
  - ***Providers*** *are those that provide treatment and medical services, such as physicians, hospitals, dentists and pharmacies.*
  - ***Health Plans*** *are those entities involved in providing and/or paying the cost for health care, such as insurance companies, Medicare, and Medicaid.*
  - ***Clearinghouses*** *are entities involved in the processing and reformatting of healthcare transactions, such as claims and remittances, for providers and insurers.*
  - *MOST CERNER CLIENTS ARE* ***COVERED ENTITIES.***

HIPAA – Cerner Covered Entities

- Did you Know?
  - *Cerner currently includes two organizations that are Covered Entities: The self-insured Cerner Health Plan and the Healthe Clinic. These organizations, as covered entities, must have processes in place that are "HIPAA compliant".*

HIPAA – Business Associate

- Business Associate:
  - *A person or organization that performs functions or activities on behalf of a covered entity that involve the use or disclosure of individually identifiable health information.*
  - *These functions or activities cover a broad range and can include claims processing, data analysis, utilization review, billing, data aggregation, remote hosting services and software vendor support, just to name a few.*

HIPAA – Business Associate

- Did you know?
  - *The majority of the services Cerner performs for our clients puts us in the category of a **business associate**. This includes the implementation and support services we provide for our software, and our remote hosting services, just to name a few.*

HIPAA – Key Concepts

- Business Associate Contract:
  - *The agreement that HIPAA requires to be in place between a covered entity and a business associate that performs activities on behalf of the covered entity.*
  - *The business associate contract must include certain required provisions that impose safeguards on the individually identifiable health information so that it is used or disclosed only for the purposes for which it was shared by the covered entity.*

HIPAA – Key Concepts

- Did you know?
  - *Cerner has a standard boilerplate business associate contract that we typically put in place with clients; however, some clients may request that Cerner sign their organization-specific contract.*
  - *The covered entity who is sharing their individually identifiable health information with the business associate is responsible for ensuring that a business associate contract is in place.*

HIPAA – Key Concepts

- Individually Identifiable Health Information (IIHI)
  - *IIHI is created or received by a covered entity;*
  - *Can relate to a past, present or future medical or mental health condition;*
  - *Either identifies or could be used to identify a specific person;*
  - *Examples of IIHI include electronic medical records, paper charts, claims, and payments.*
- Protected Health Information (PHI)
  - *PHI is individually identifiable health information protected under the HIPAA Privacy Rule;*
  - *PHI must be protected while it is held or transmitted by a covered entity or their business associate;*
  - *PHI includes IIHI in any form or media, whether electronic, paper or oral.*

HIPAA – Key Concepts

- Use vs. Disclosure (in relation to PHI)
  - ***Use*** *- covered entities and business associates* ***use*** *PHI within their organization as part of normal treatment, payment and healthcare operations activities.*

    Examples: a client ***uses*** *PHI to treat patients and generate bills for services. Cerner* ***uses*** *PHI to troubleshoot client service requests.*
  - ***Disclosure*** *– when a covered entity releases PHI outside their organization it is known as a* ***disclosure****.*

    Example: a client may ***disclose*** *PHI to Cerner as part of a service request, if the PHI is needed by Cerner to troubleshoot the issue. The client should only disclose the* ***minimum necessary*** *amount of PHI to Cerner.*
  - *Cerner rarely, if ever, would have a need to* ***disclose*** *PHI outside our organization.*

HIPAA – Transactions

- HIPAA Transactions
  - *The HIPAA Administrative Simplification Standard for Electronic Transactions, also known as the Transactions and Code Sets Rule, facilitates standardized information exchange between providers and payers. This helps facilitate faster payment and reduces the number of claims that are rejected because they are in the wrong format.*

HIPAA – Code Sets

- HIPAA Code Sets
  - *HIPAA transactions contain both **Code Sets** and **Identifiers***
  - ***Code Sets** are standardized and certain fields within transactions must be completed only with values from code sets. Code Sets help eliminate subjectivity and ensure uniformity of data in the transactions.*
  - ***Code Sets** are used for encoding data elements and their primary purpose is to standardize the identification of services for which health care providers commonly bill for.*

HIPAA – Identifiers

- HIPAA Identifiers
- HIPAA transactions contain both **Code Sets** and **Identifiers**
  - ***Identifiers*** *are codes that uniquely identify each entity sending or receiving a health care transaction:*
    - National Provider Identifier (NPI) – 10 digit number that health care providers can use to personally identify themselves
    - National Employer Identifier (EIN) – 9 digit number that uniquely identifies employers who provide insurance for their employees.
    - National Health Plan Identifier (NPlanID) – proposed identifier, currently on hold, that would uniquely identify individual or group health plans and other payers of claims
    - National Health Identifier for Individuals (NHI) - proposed identifier, currently suspended, that would uniquely identify every individual receiving healthcare in the U.S.

HIPAA – The Privacy Rule

- The Privacy Rule – Some Covered Entity Responsibilities
  - Covered entities are required to **provide patients with a notice of their privacy rights** and the privacy practices of the covered entity. The notice should address the use and disclosure of individually identifiable health information by the covered entity in the provision of care. The notice provision requires direct treatment providers to make a good faith effort to obtain the patient's written acknowledgement that they received a notice of privacy rights and practices.
  - Covered entities also must **adhere to the minimum necessary standards**, meaning that they will use or disclose only that information which is *absolutely necessary* for treatment, payment and healthcare operations purposes.
  - A covered entity must **define policies and procedures** that identify what information is necessary for each staff member or business associate to carry out their jobs.
  - A covered entity must get the **patient's authorization** to use their identifiable information for non-routine purposes, such as marketing or research, or insure that the information is fully de-identified.

HIPAA – Patient Rights

- The Privacy Rule – Patient Rights:
  - The right to request restrictions on how their information can be used or disclosed
  - The right to be able to inspect their own records
  - The right to request a copy of their own records
  - The right to request amendments to their own records
  - The right to receive an accounting of disclosures for their records, within certain limitations
  - The right to request confidential communications
  - Patients who believe their information has been improperly used or disclosed can file a complaint with the covered entity or the Office of Civil Rights.

HIPAA – The Security Rule

- The Security Rule
  - The rule establishes guidelines for ensuring the confidentiality, integrity, and availability of PHI that is received, processed, maintained, stored, archived, disposed of, or transmitted in electronic form.
  - The Security Rule's requirements set forth a framework of physical, administrative, and technical controls to support the privacy and confidentiality needs outlined by the Privacy Rule. The two rules are intended to be complementary because privacy cannot be credibly protected without security.
  - HIPAA Security standards are scalable, so that organizations of differing sizes and complexity can implement security procedures appropriate to their needs. The standards are technology-neutral in order to address the individual circumstances of organizations, and to allow for inevitable changes and advances in technology over time.
  - The Rule is intended to set a minimum level or "floor" of acceptable security practices. Organizations may choose to implement safeguards that exceed the HIPAA standards, and commonly may find that their business strategies require stronger protections than what is mandated by HIPAA.

Cerner

HIPAA – The Security Rule

- The Security Rule – Organizational Responsibilities:
  - Under HIPAA, information security is a comprehensive framework of administrative, physical and technical safeguards that focus on protecting the confidentiality, integrity and availability of protected health information. Some of these safeguards are described below:
    - *Assessing potential risks and vulnerabilities*
    - *Implementing appropriate and adequate measures to protect against threats to information security or integrity, and against unauthorized use or disclosure.*
    - *Establishing and implementing disaster recovery plans to guard against the permanent loss of critical data. These plans should be periodically tested, and reviewed and updated as needed to reflect current practices*
    - *Ensuring compliance with the organization's security measures by all staff, and implementing workforce security awareness training that is reinforced by periodic security reminders*
    - *Implementing a security incident reporting system and a sanction policy to hold individuals accountable for security incidents stemming from negligence or misconduct*
    - *Periodically reassessing the security program to ensure that it remains effective*

HIPAA – ARRA/HITECH

- ARRA/HITECH Provisions – Passed February 17, 2009
  - The American Reinvestment and Recovery Act of 2009 (ARRA) HITECH Provisions included several key changes to HIPAA:
    - *New provisions that extend HIPAA privacy, security, and administrative requirements to business associates;*
    - *Breach identification and notification requirements for HIPAA-covered entities **and** business associates;*
    - *Additional restrictions on the sale of health information;*
    - *A new accounting requirement is established for disclosures related to treatment, payment, and healthcare operations, if made via an EHR;*
    - *New access requirements related to the ability of individuals to access their healthcare information in electronic format;*
    - *Additional conditions established for marketing and fundraising;*
    - *Personal health record (PHR) information held by non-HIPAA entities is now protected;*
    - *Improved enforcement and increased civil and criminal penalties for non-compliance for covered entities **and** business associates*
    - *Additional patient rights to request restrictions on disclosures of their PHI*

HIPAA – ARRA/HITECH

- ARRA/HITECH Changes to HIPAA – Some Key Points for Cerner:
  - Cerner will now be directly regulated by the HIPAA Security Rule and some portions of the Privacy Rule
  - Cerner must have a breach escalation and notification process in place:
    - *Cerner implemented 01POL017491 Breach Notification Policy and 01SOP017492 Breach Notification SOP to address this requirement.*
    - *01POL017491 defines a breach as "the unauthorized acquisition, access, use, or disclosure of PHI that compromises the security or privacy of the PHI, such that it would pose a significant risk of financial, reputational, or other harm to the individual".*
    - *A breach does not include the unintentional acquisition, access, or use of PHI by an associate or other authorized individual acting under the authority of Cerner or a Cerner client, if such acquisition, access, or use was made in good faith and within the scope of the associate's role and responsibilities, as long as the PHI in question is not subject to further unauthorized disclosure*
    - *01SOP017492 describes how breaches must be escalated, investigated and, when applicable, reported to clients. Cerner also must help clients in their efforts to notify the impacted patients.*
  - Clients will likely require Cerner to sign updated business associate agreements that contains the new requirements.

HIPAA – ARRA/HITECH

- ARRA/HITECH Changes to HIPAA – Some HIPAA Privacy requirements will apply directly to Business Associates, including Cerner:
  - If Cerner learns of a material breach by a client, Cerner is required to:
    - *Take action to cure breach or end the violation, or*
    - *If that is not feasible, terminate its contract with the client*
    - *If neither is feasible, report the breach to HHS*
  - Accounting of disclosures now includes disclosures made by business associates; the covered entity may direct patients to their business associate(s) to obtain the accounting. The accounting must cover the 3 years prior to the patient's request.
  - Clients and Cerner may not profit from the sale of PHI unless the patient has given a valid authorization.
  - Reporting of breaches to covered entities is now required.
  - Increased enforcement activities by Health & Human Services (HHS) and increased civil and criminal penalties that also will apply to Cerner if we don't comply
  - HHS to audit Covered Entities **and** Business Associates
- Essentially, ARRA/HITECH represents the most major changes to HIPAA since its inception.

HIPAA – Penalties

A look at the significantly increased civil and criminal penalties that also will apply to Cerner under the HITECH Act:

Civil Penalties		
Violation Category	Per Violation	Max Per Year
Single violation, or multiple if each for a different provision	$100	$25,000
Reasonable cause not due to willful neglect	$1000	$100,000
Willful neglect – issue corrected	$10,000	$250,000
Willful neglect, multiple violations	$50,000	$1.5 Million

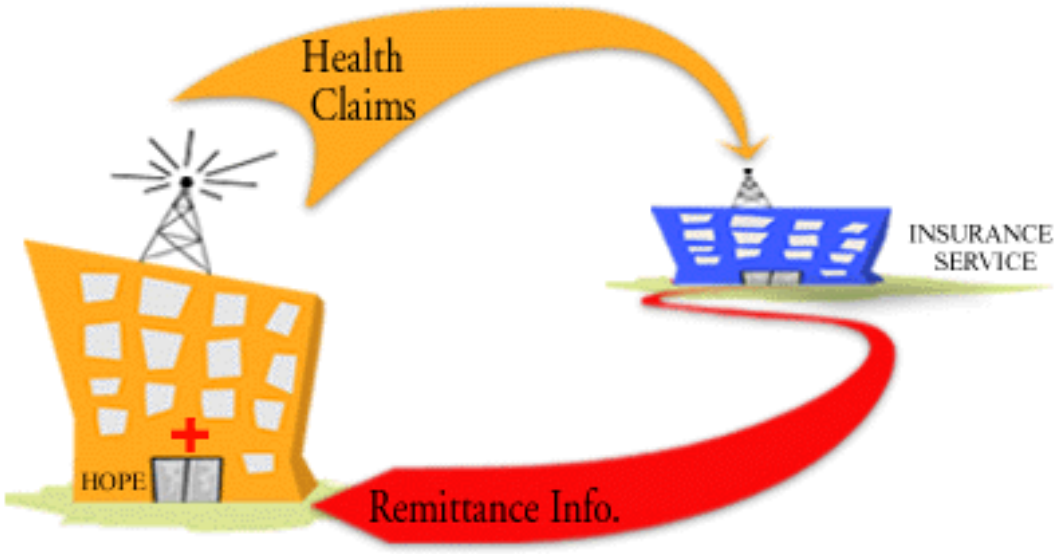
Criminal Penalties		
Violation Category	Fine	Imprisonment
Wrongful disclosure of IIHI with intent to sell or use for commercial or personal gain, or with intent to maliciously harm	Up to $250,000	Up to 10 Years
Wrongful disclosure of IIHI under false pretenses	Up to $100,000	Up to 5 Years
Wrongful disclosure of IIHI	Up to $50,000	Up to 1 Year

HIPAA Key Concepts – Practical Scenarios

The following scenarios provide examples of the difference between HIPAA duties and responsibilities for covered entities and those of business associates, and also illustrate examples of key HIPAA concepts in practice.

HIPAA Scenarios

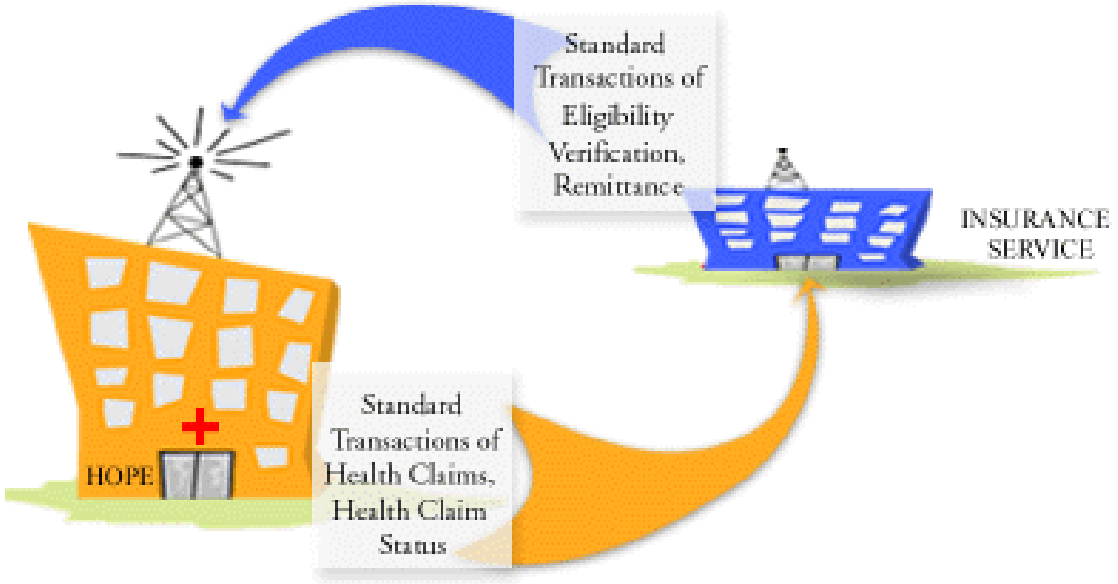
A. An example of HIPAA's requirements on a covered entity.



Hope Hospital is a community hospital. Every day the hospital transmits health claims to health plans and receives remittance information. The hospital processes eligibility verification to ensure that patients and their treatments are covered by the insurance plan. All the information exchanged between the hospital and the health plans is in electronic format. Therefore, Hope Hospital is considered a covered entity under the EDI portion of the HIPAA regulation.

HIPAA Scenarios

A. An example of HIPAA's requirements on a covered entity.



As a covered entity, Hope is required to use the standard transactions that have been specified for health claims, health claims status, remittance, and eligibility verification. It is also required to use the standard code sets when transmitting health information electronically. For example, when transmitting the code for a patient's broken leg, Hope Hospital is required to identify this condition by its standard ICD9 code. When transmitting non-medical information about a patient, such as their gender and religion, Hope is required to identify these non-medical attributes by standard code sets.

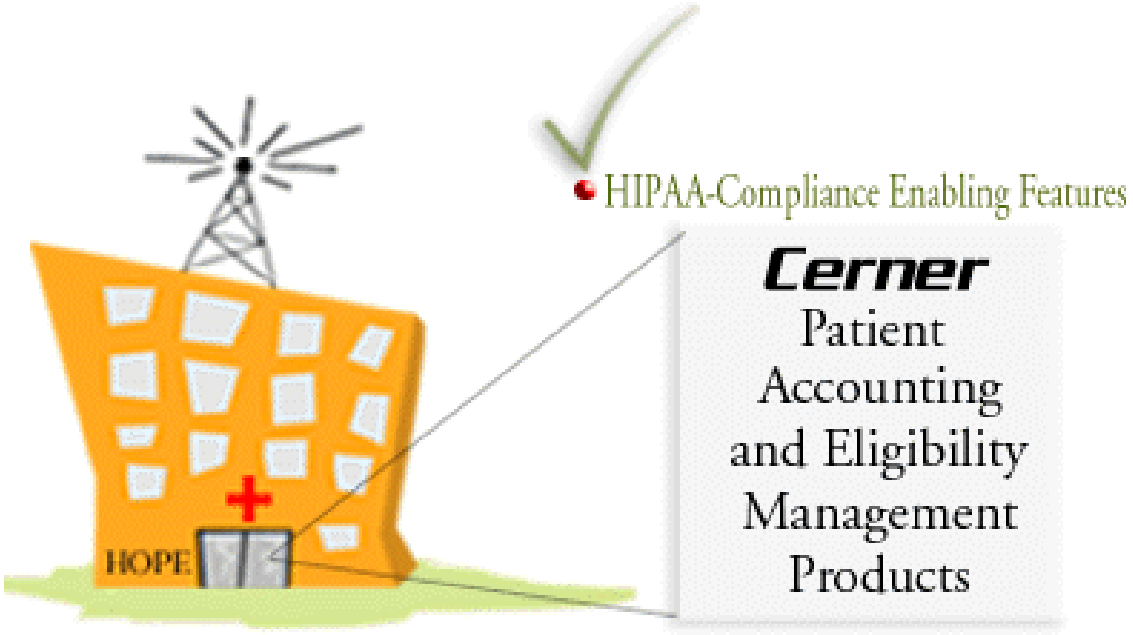
HIPAA Scenarios

A. An example of HIPAA's requirements on a covered entity.

Hope Hospital has the option of sending their electronic information through a clearinghouse if this helps them translate their information into a standard transaction format. Health plans must accept transactions sent in standard format.

HIPAA Scenarios

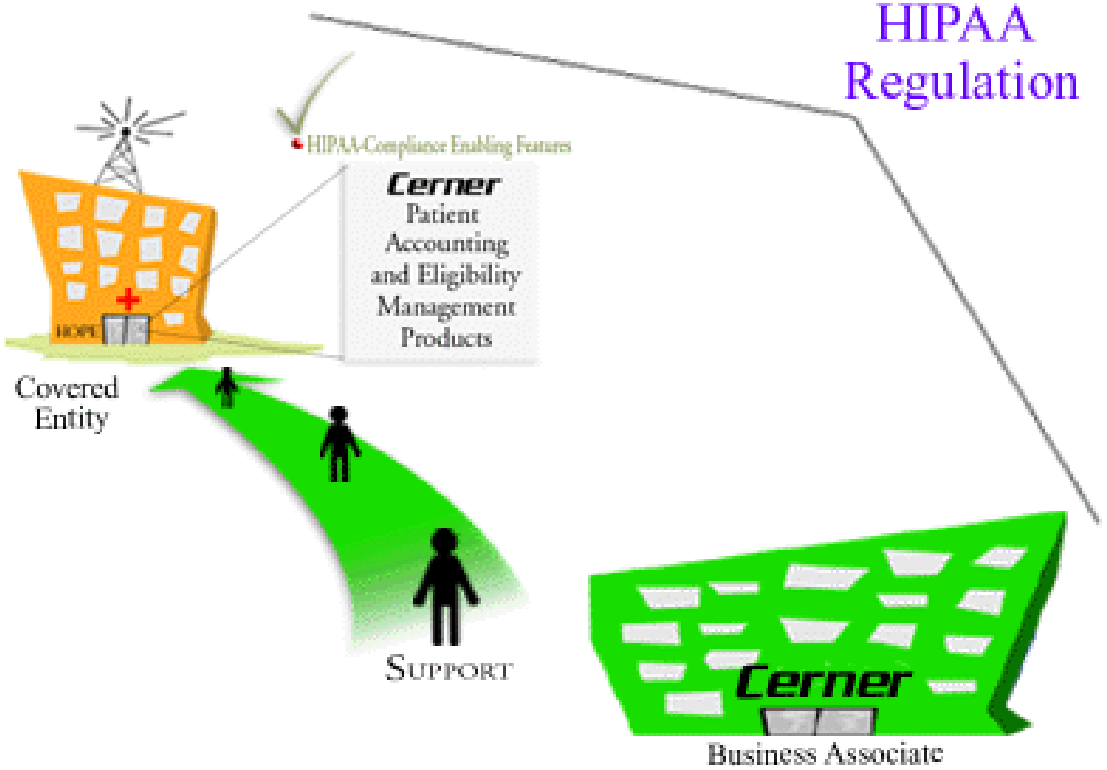
B. Cerner's role as a business associate.



Hope Hospital is using Cerner's Patient Accounting and Eligibility Management products. These products have HIPAA-compliance enabling features that will assist Hope Hospital in their effort to be HIPAA-compliant.

HIPAA Scenarios

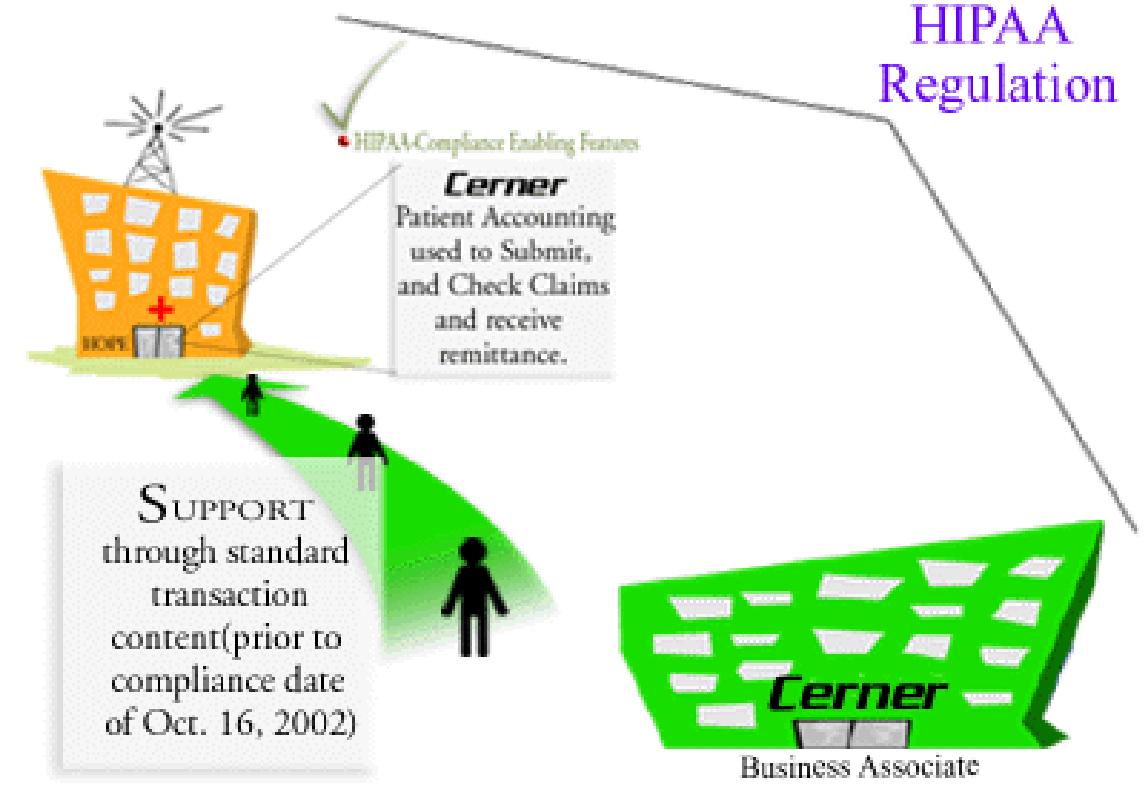
B. Cerner's role as a business associate.



Because Cerner software is used to assist the covered entity (Hope Hospital) in performing standard transactions, and because Cerner provides support for the use of its software, Cerner is considered a business associate under the HIPAA regulation.

HIPAA Scenarios

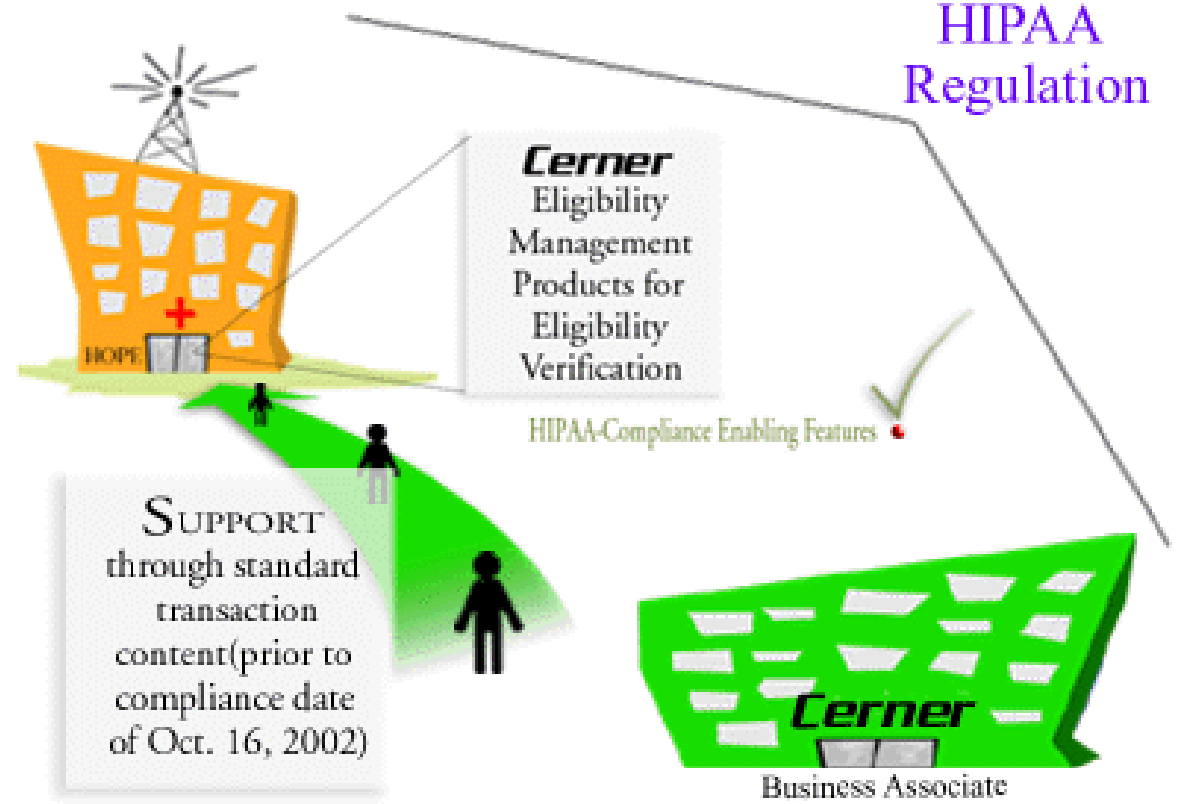
B. Cerner's role as a business associate.



Hope will use the Patient Accounting product to submit claims, check claim status, and to receive remittance. In order to support the use of this product, Cerner will have to provide standard transaction content for these transactions prior to the compliance date of October 16, 2002.

HIPAA Scenarios

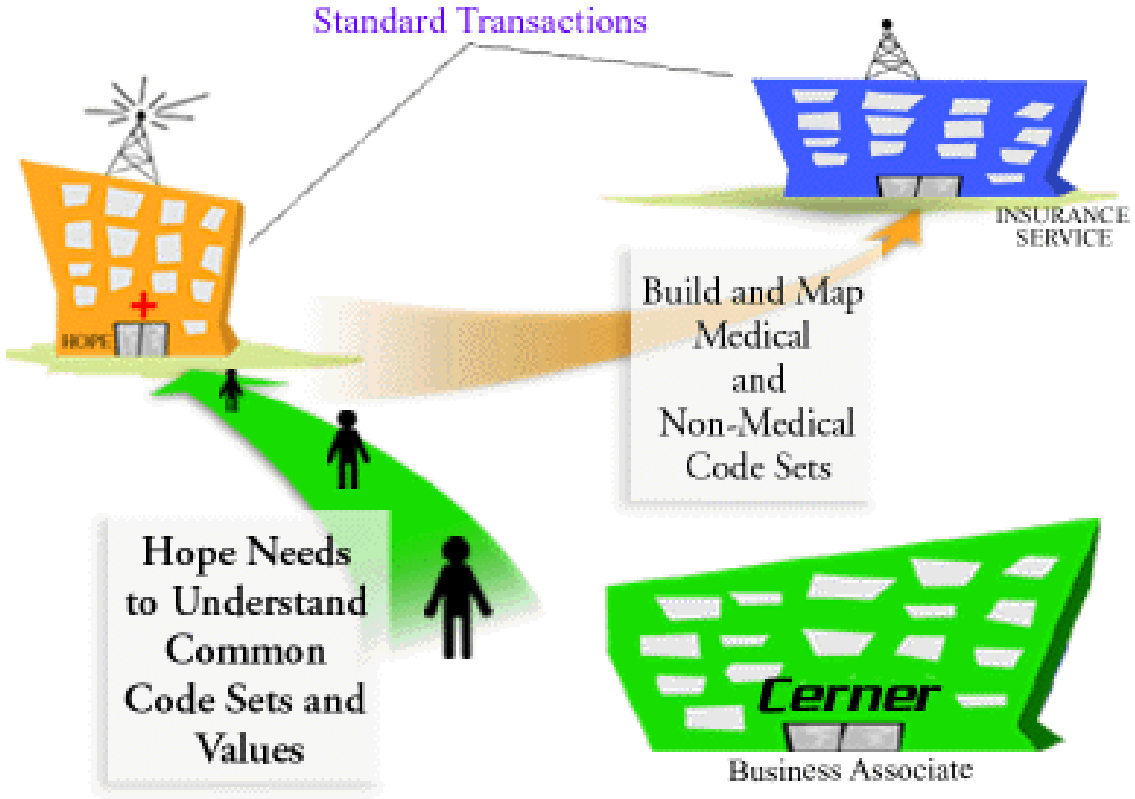
B. Cerner's role as a business associate.



Meanwhile, Hope will use Cerner's Eligibility Management product to perform eligibility verification. To support the use of this product, Cerner will have to provide standard transaction content for the eligibility verification transaction prior to the compliance date.

HIPAA Scenarios

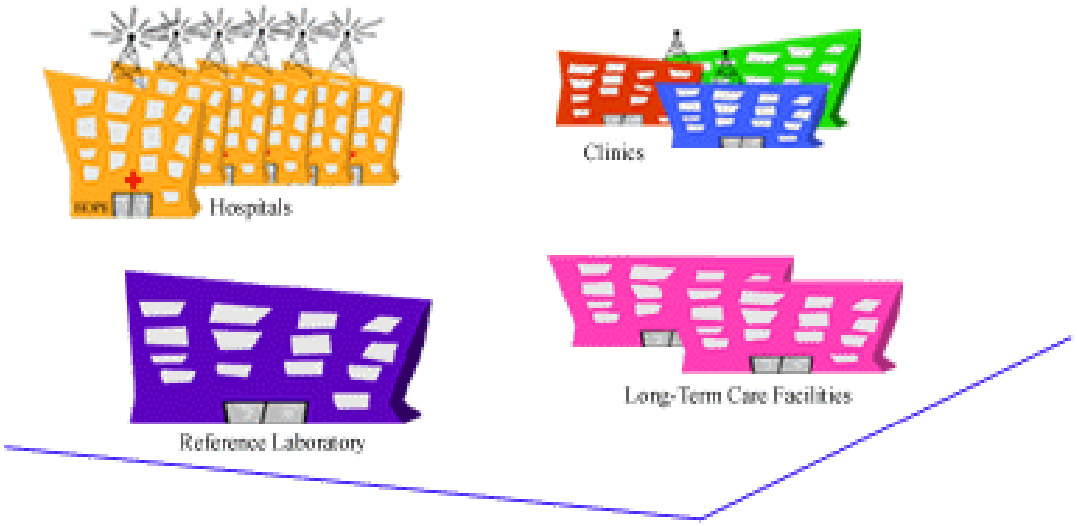
B. Cerner's role as a business associate.



Additionally, as Cerner's client, Hope will need to understand how to use Cerner's common code sets and code set values to build and map medical and non-medical code sets for use in the standard transactions.

HIPAA Scenarios

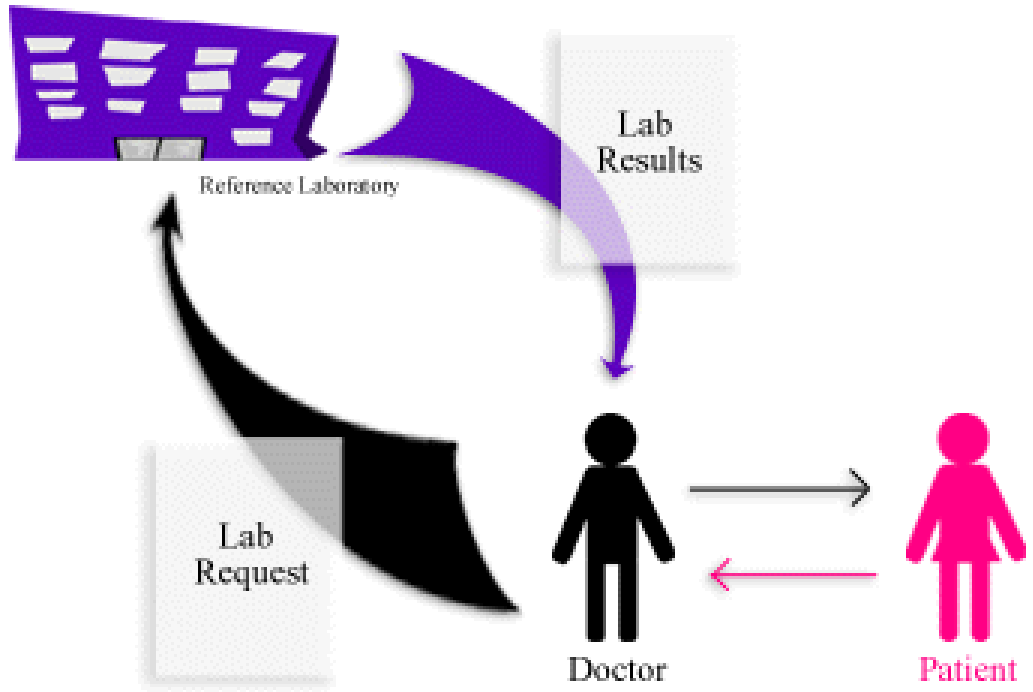
C. An example of an organized health care arrangement.



Hope Hospital is a member of a large healthcare organization, Saddleback Regional Health System. Saddleback includes 6 hospitals, 2 long-term care facilities, a reference laboratory, and 3 clinics. All of them are covered entities. Saddleback acknowledges publicly that these covered entities are part of its joint system of healthcare delivery. This system is, therefore, considered an organized health care arrangement under the HIPAA Privacy regulation. It is common for patients to receive services from multiple facilities of an organized health care arrangement.

HIPAA Scenarios

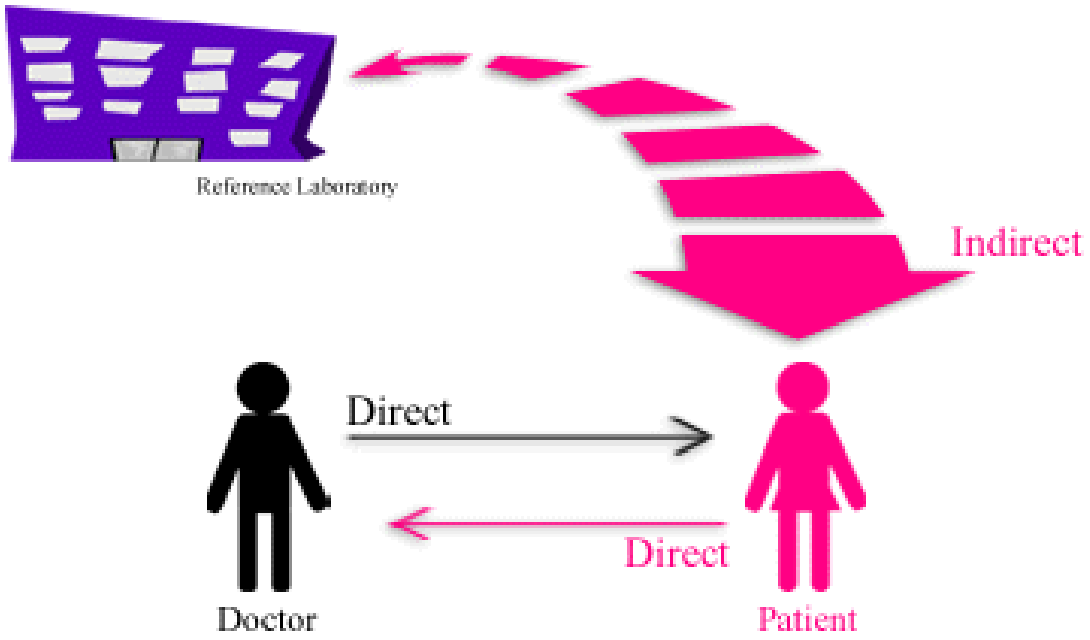
D. An example of direct and indirect treatment relationship.



Monika Jones visits one of the Saddleback clinics to see her primary care physician, Dr. Allen Marconi, for a check up. Dr. Marconi performs several tests and sends the specimens to the Saddleback Reference Laboratory to be resulted. The reference laboratory performs the results and sends them back to Dr. Marconi, who then shares the results with Ms. Jones.

HIPAA Scenarios

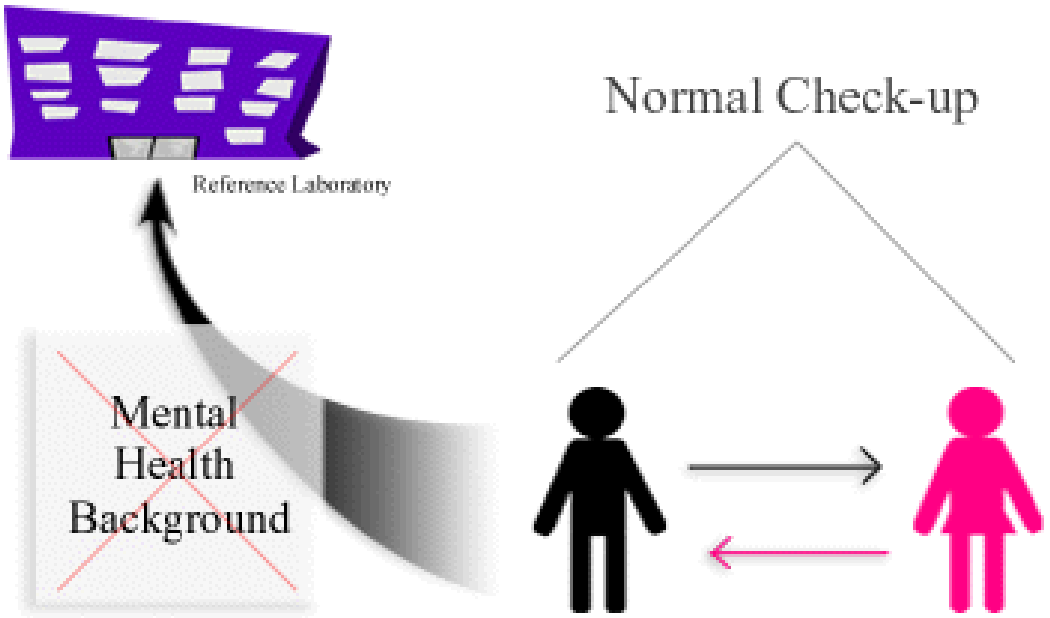
D. An example of direct and indirect treatment relationship.



In this example, Dr. Marconi has a direct treatment relationship with Ms. Jones, because he is interacting directly with Ms. Jones during the office visit and is also informing her of the outcome of the treatment rendered. The reference laboratory, although they are processing Ms. Jones' results, has an indirect treatment relationship with her because they send the results to Dr. Marconi and never have any direct interaction with Ms. Jones.

HIPAA Scenarios

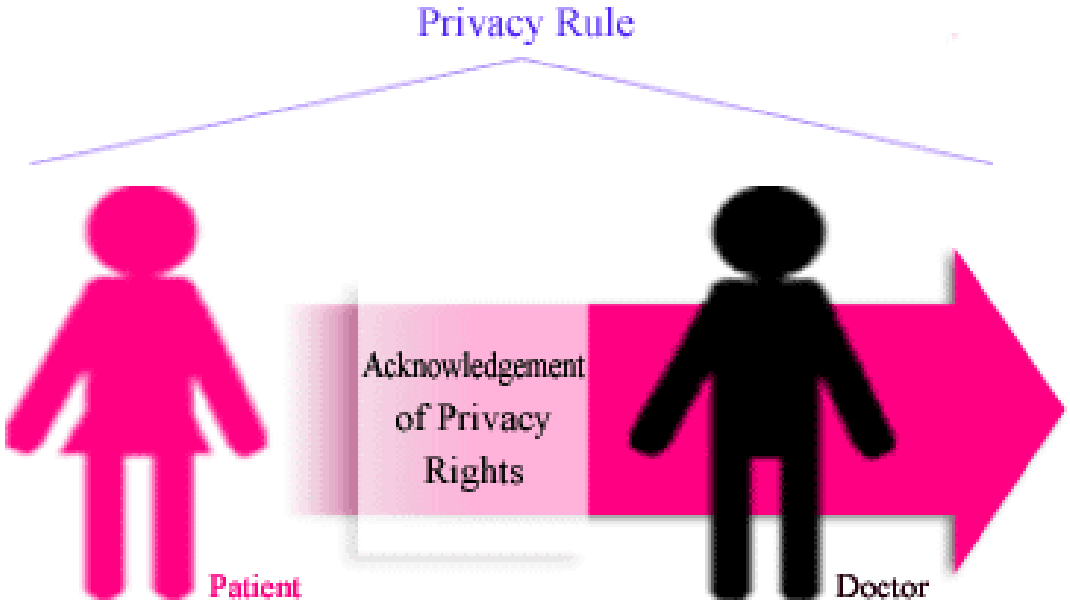
E. An example of the term "minimum necessary" in practice.



When Dr. Marconi's office sends the tests to the reference laboratory to be resulted, they are obligated under HIPAA to send the minimum necessary amount of protected health information about Ms. Jones – this would be just enough information for the reference laboratory to accomplish the resulting of the tests for Ms. Jones. It would be inappropriate for Dr. Marconi's office to release any information about a mental health referral Ms. Jones had 2 years ago because it has no bearing on the treatment currently being performed by the reference laboratory.

HIPAA Scenarios

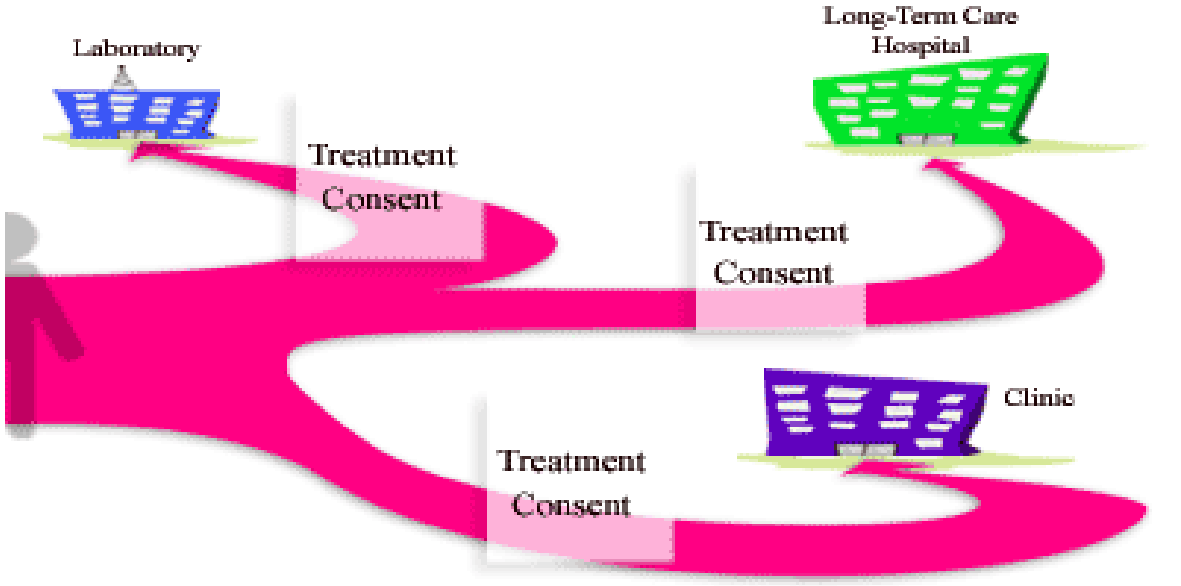
F. An example of a situation in which a Healthcare provider would obtain consent and authorization prior to releasing protected health information.



Covered entities can choose whether they want to obtain consent prior to using a patient's information for treatment, payment and healthcare operations purposes. The healthcare organization Dr. Marconi belongs to has elected to put a consent process in place, so Dr Marconi will obtain consent from Ms. Jones. HIPAA also requires Dr. Marconi to provide Ms. Jones with notice of his organization's privacy practices and her privacy rights. Dr. Marconi must attempt to gain written acknowledgement from Ms. Jones that she received this notice.

HIPAA Scenarios

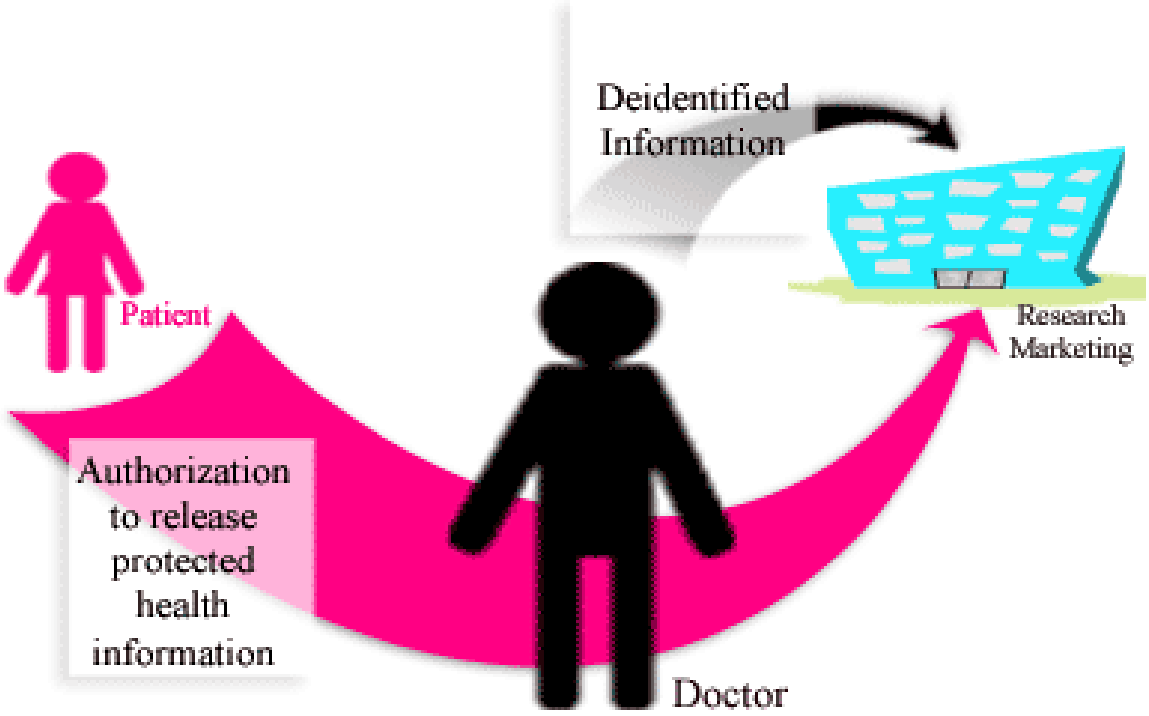
F. An example of a situation in which a Healthcare provider would obtain consent and authorization prior to releasing protected health information.



Once consent has been given, Dr. Marconi's office is not required to obtain an authorization before releasing Ms. Jones' information to the reference laboratory, because they are releasing this information solely to carry out treatment, and because the reference lab is part of the organized healthcare entity. All parts of the Saddleback Health System may rely on the consent obtained by Dr. Marconi at the clinic. The consent only has to be obtained once within the Saddleback Health System.

HIPAA Scenarios

F. An example of a situation in which a Healthcare provider would obtain consent and authorization prior to releasing protected health information.



If Dr. Marconi wanted to disclose Ms. Jones protected information outside of treatment purposes, such as for marketing purposes, he would have to obtain authorization from Ms. Jones prior to doing so. However, if the information could be completely de-identified, the authorization would not be required.

HIPAA – Key Takeaways

HIPAA and its Relationship to our Clients

Our clients are **covered entities** under the HIPAA regulation. This means they are required to keep patient information confidential, and to not use it for other purposes unless a valid patient authorization is obtained – such as for marketing or research purposes, for example.

Our clients must have policies, procedures, and adequate physical and technical security safeguards in place to ensure that the **confidentiality, integrity and availability** of patient information is maintained. Our clients also are required to obtain contractual assurances that their third party business associates, such as Cerner, will protect patient information they use or access when providing services and support.

For Cerner, this means that our clients will require us to sign a **business associate contract** to confirm that we will maintain the confidentiality and security of the patient information that may be exchanged or accessed during our business relationship. For example, any patient information that is viewed while on site during implementation, or viewed during the course of working on a service request must be kept confidential, and any patient data stored by Cerner must be secured.

Cerner is responsible for ensuring that associates are aware of the need to protect our client's patient information **and to not use or disclose it inappropriately**. Cerner also is required to have **adequate security safeguards** in place, and to ensure that any third parties we bring into the business relationship also agree to similar protections. We also are required to report to our clients **breaches of their PHI that have the potential to harm the impacted individuals**.

HIPAA – Key Takeaways

HIPAA and its Relationship to Cerner

Cerner is a **hybrid entity** under HIPAA. This means that we perform both **covered entity** and **business associate** functions. Business associate functions would be those in which we are performing functions on behalf of our clients – the delivery and implementation of our software solutions and our provision of service and support, for example. Covered entity functions would be those that make us a **covered entity** under HIPAA – as mentioned previously, examples of these would include the Cerner Clinic and Cerner's self-insured health plan.

The areas within Cerner that are covered entities must be compliant with all provisions of the HIPAA regulation. This means that the necessary policies and procedures must be in place to govern the behavior of those who work with protected health information. It also means that adequate security mechanisms must be in place to guard the confidentiality, integrity, and availability of the protected health information. With ARRA/HITECH changes to HIPAA, the business associate portions of Cerner now must also comply with the HIPAA security provisions and also some portions of the Privacy Rule.

Hybrid entities like Cerner have an obligation to keep their covered entity and non-covered-entity areas separate as much as possible (procedurally separate, not necessarily physically separate). For example, the Cerner self-insured health plan would not be allowed to share an associate's personal health information with Cerner Corporation the employer, if the information was to be used for employment-related purposes or to make decisions about promotions.

Both covered entities **and** business associates that misuse or fail to protect patient information appropriately can be subject to substantial monetary penalties.

HIPAA – Key Takeaways

Cerner Solutions' Support of HIPAA Requirements

Cerner solutions support the transmission and receipt of standard HIPAA transactions (for example, Cerner solutions that are involved with patient registration, billing, scheduling, and eligibility), which helps enable our clients' compliance with the HIPAA Transaction and Code Set standards.

These solutions are involved in supporting the claims, claim status, eligibility inquiry and response, payment and remittance, and the referral certification and authorization transactions. Cerner's Retail Pharmacy solution also has the capability to transmit the National Council on Prescription Drug Processing (NCPDP) Retail Drug Claim standard transaction. Cerner solutions also support the use of standard code sets for encoding medical information that is stored in the system and also transmitted via the standard transactions.

All Cerner solutions support unique usernames and secure passwords, to control access to the system by only authorized and authenticated users. Cerner solutions also support authorization levels for users, so that their access to PHI can be tailored appropriately to their role. Cerner solutions also support audit capabilities so that our clients can track users' access to PHI.

HIPAA – Key Takeaways

Tips for Associates – Protecting PHI:

- Only access PHI to provide implementation, monitoring, management, investigation, or support services that are authorized by the client and directly related to the scope of the work requested by the client.
- Do not copy identifiable patient information to databases, network drives or other locations for purposes not directly related to supporting the client - such as testing, training, sales demos, etc.
- If PHI is printed out, shred it once it is no longer needed. Do not place it in the trash or recycle bin.
- Do not leave PHI unattended on your computer screen or desk. Store it securely out of sight when not in use.
- Always use secure means when PHI must be transmitted.
- When accessing PHI, only access the minimum amount needed for the purpose at hand.
- Do not disclose PHI inappropriately to those inside or outside of Cerner who do not have a direct business need to know the information.
- Do not store PHI on your laptop. If the laptop is lost or stolen this could lead to a breach.

HIPAA – Key Takeaways

Tips for Associates – Protecting PHI:

- Do not email unencrypted PHI. Use a more secure means of transmitting it such as Secure File Transfer Protocol (SFTP), which is the preferred method, or alternatively, by sending an encrypted WinZip attachment.
- If a client emails you unencrypted PHI, encourage them to use a more secure means of transmittal. Also, delete the email and do not forward it on inside or outside of Cerner.
- Never post patient information to a public folder in Outlook, or on KR, MyCerner, Cerner.com, uCern, SharePoint, a Wiki page, or any other public location. Any such action by an Associate will result in immediate disciplinary action, and will require a security incident to be documented.
- If entering PHI into an SR in Navigator, make sure to enter it in the encrypted Protected Health Information field.
- Immediately report any suspected breaches of patient information to your manager and Regulatory Affairs.

For more info on protecting PHI, refer to Cerner's Corporate Protection of Patient Information SOP (01SOP000008).

Additional Suggested Reading

- Associates should be very familiar with the information contained in the following policies and SOPs.
  - 01POL000010, Protection of Patient Information Policy
  - 01SOP000008, Protection of Patient Information SOP
  - 01POL000035 Remote Client Access Policy
  - 01POL017491 Corporate Breach Notification Policy
  - 01SOP017492 Corporate Breach Notification Procedure
  - 01GD000003 Guidelines for Secure Paper Disposal

These documents can be found on the corporate document file share:
\\cernerwhq1\regaffrs\ControlledDoc\01 - Corporate

Contact Information

Questions or comments?

- myCerner
  - myCerner → Company → Regulatory & Industry → HIPAA
- Reg Affairs mailbox
  - REGAFFR – Cerner