



Guide to Understanding and Complying with HIPAA Security and Privacy Regulations

(Originally Published February 1, 2000)

Revised January 8, 2001

To Include the Final Privacy Rule Published December 28, 2000)

By Thomas L. Hanks

Practice Director, Enterprise Security and HIPAA Compliance

Beacon Partners, Inc.

tom.hanks@beaconpartners.com

Chicago Office:

400 Barrington Pointe
2300 North Barrington Rd.
Hoffman Estates, IL 60195
(847) 490-5306
www.hipaacomply.com

Corporate Offices:

200 Cordwainer Drive
Suite 300
Norwell, MA 02061
www.beaconpartners.com
1-800-4BEACON

HIPAA OVERVIEW

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted on August 21, 1999. This legislation was expanded far beyond its original intention, which was the “Portability” portion. Portability refers to the section that provides for the waiver of pre-existing conditions when persons who are covered under a group policy with their current employer move to a new employer. This was extremely important for those persons (or family members) that suffered from expensive chronic conditions. As is the case with most popular legislation, there were a number of other provisions added as the bill moved through congress. These amendments provide funding for the OIG health care fraud and abuse investigations, and incorporates Administrative Simplification Section that includes: (1) Standardization of electronic formats for transmission of nine specific transactions including claims, electronic remittance advice, eligibility, authorization, pharmacy, enrollment, coordination of benefits, attachments and first notice of claim, (2) Security of electronic health information and electronic signatures, and (3) Privacy of such patient identifiable information. We are going to focus on the Security and Privacy portions of the Act with the goal of providing a basic understanding of the impact of the regulations and a common sense road map for navigating the compliance process.

Please note that this is intended to be a “living document” and will be updated to reflect changes as rules become final and DHHS clarifies interpretations. I would recommend registering (subscribing) at the HIPAAComply.com web site (www.HIPAAComply.com) and you can receive updates as they are published.

SECURITY VS. PRIVACY... DEFINITIONS

When initially tasked with the writing of the security NPRM, there were a number of issues that weaved privacy into the security rules. However, since privacy and security are two separate entities, the industry and DHHS felt that it was important to differentiate between the two. For example, it is possible to secure information without making it private, however it is not possible to protect privacy without having security.

For the purposes of this document, the following definitions are used:

- 1) Security is defined as the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction or loss.
- 2) Privacy is defined as controlling who is authorized to access information (the right of individuals to keep information about themselves from being disclosed).

HIPAA PRIVACY PROCESS

HIPAA legislation addresses privacy in a unique fashion. First, it calls for Congress to pass “Comprehensive health care privacy legislation” by August 21, 1999 and requires the Secretary of the Department of Health and Human Services (DHHS) to submitted detailed recommendations that Congress could use to craft privacy legislation. If Congress fails to pass privacy legislation by the August 21, 1999 deadline, then HIPAA mandates DHHS to promulgate privacy rules. If DHHS is forced to promulgate rules; after publication of the final rule, Congress has 60 days to review it. After the 60-day

period, affected entities have two years to comply.

DHHS kept their end and delivered comprehensive recommendations on privacy standards to Congress on September 11, 1997. Unfortunately, as we will soon see, Congress did not hold up their end of the mandate. DHHS then wrote a document detailing the proposed privacy rules and released it November 29th, with much fanfare from the Clinton administration.

Under the rules for promulgating regulations, this Notice of Proposed Rule Making (NPRM) was published in the Federal Register on November 3, 1999. Traditionally, the public has sixty (60) days to deliver any comments to the NPRM to DHHS. However, with the massiveness of the rules (150 type-set pages) and looming Y2K issues, there were a number of petitions to DHHS to extend the comment period and as a result, DHHS extended the comment period to February 17, 2000. Although, under HIPAA, the rules were required to be final by February 21, 2000, they were not finalized and published until December 28, 2000.

The final Privacy Rule made numerous and significant changes to the original Privacy NPRM. In the final rule, DHHS continues to call for comprehensive Privacy legislation in order to cover a number of areas that the Act does not give DHHS the authority to adequately address. This is primarily due to Congress not giving DHHS the authority to preempt State law and there are many entities that can maintain patient information that the Act does not give DHHS authority to regulate. Hopefully, the publication of this final Privacy rule will light a fire under congress to pass comprehensive Privacy legislation, which would most probably produce Privacy laws that would be less onerous to comply with than the current Privacy rule.

Overall, in the final rule, DHHS had done a good job of clarifying a number of previously nebulous areas. Unfortunately, as in the NPRM, the resulting regulations are unable to supercede State law and the methodologies that DHHS had to resort to in order to extend protection of patient information were tortured and onerous. Essentially, in order to get as much protection as possible – and they still were unable to cover all aspects of patient information – DHHS was forced to mandate that: (1) covered entities must provide contract language with their Business Associates that binds their Business Associates to comply with the privacy regulations, (2) makes the covered entities responsible for any violations that their Business Associates might propagate and business associate. The HIPAA legislation also specifically prevented DHHS from writing privacy regulations that superceded State law. That means that any State law that is contrary and more restrictive than the Privacy regulations would take precedence.

I would highly recommend monitoring the DHHS Administrative Simplification web site (address under resources at the end of this document) and reviewing the FAQ as questions are submitted and answered.

SECURITY STANDARDS PROCESS

Under HIPAA, DHHS was mandated to promulgate security standards for the protection of electronic health information.

On August 12, 1998, DHHS Security and Electronic Signature Standards NPRM were published. This was followed by a 60-day comment period, ending October 13, 1998. The publication of the final rule has been delayed for a number of reasons. First, there was an large volume of comments (2,000+) that had to be analyzed, next DHHS did not want to overload HCFA or other health care entities by publishing the final rule in 1999 during the final Y2K remediation. The current delay is due in part to allow DHHS to align the Security rule with the final Privacy rule, including a number of definitions and clarifications.

Although there have been many announcements of when the Security rule will be finalized, as of this writing, January 1, 2001, there is no published final date for the Security regulations. Although, they were initially slated to be second on the priority list – behind Transactions, the last announcement targets finalization the first quarter of 2001. From all accounts, we are very confident that there will not be any substantial changes in the final rules. We anticipate, for example: (1) That all of the definitions will be aligned with the definitions in the final Transactions and Privacy rules, (2) Electronic signatures will be carved out and included in a later rule or a separate NPRM, (3) Increased audit trail requirements, and (4) Clarification of inclusion of paper and oral communication.

HIPAA SECURITY AND PRIVACY - WHY?

Let us quickly examine the need for Security and Privacy legislation. It is really quite simple, protecting patient data is the right thing to do, and, it is the right time to do it. There are three basic imperatives:

Imperative # 1: Moral imperative. Protecting patient records is the right thing to do. That is, patients have a right to privacy of their health information. (protecting patient records is the right thing to do). As a consumer, I would not appreciate indiscriminate sharing of my private health information. It is just not anybody else's business. As an example, one afternoon I took my son to the emergency room. There is an unwritten rule in our family that male children must visit the emergency room at least once per year. When we were ready to leave, I was standing by the front desk waiting for the paperwork to free us. I was also looking over the shoulder of an ER physician and very interested in the "cool" IS system that showed each treatment room as an icon. As I looked on, he clicked on the treatment room icons and I was able to ascertain the treatment capabilities of each treatment room including supply inventories, crash cart status, monitoring devices, etc. I was also able to view the treatment information and learn that the injuries of the son of the nice young couple in treatment room two met the hospital's profile for notifying the authorities about suspected child abuse and that the elderly lady in treatment room five had attempted suicide. It became very clear that information was none of my business. Since, as I found out, 90% of the suspected abuse reports are cleared without incident, if I had been a talkative co-worker or neighbor of one of the parents, the outcome could have been disastrous.

Imperative # 2: Business imperative. Protecting business information is the right thing to do. Businesses have a need to protect their confidential data, and, protecting business data is the right thing to do. If we are not protecting patient information, the odds are that we are not protecting our business information. The same methodologies that we can deploy to protect patient information are also used to protect our business information. One example is the high number of

premature announcements of mergers and/or acquisitions that can result in high employee turnover and lowered moral. Most businesses want the ability to positively frame a merger announcement to their employees. We have found examples of complete HR and salary information open for public inspection.

Imperative # 3: Legal imperative (risk avoidance). Protecting our organization from litigation is right thing to do. Health care organizations have a need to protect themselves from litigation. The fact is that protecting patient information reduces risk of litigation. There is considerable support that in the event of an inadvertent release of patient information, that being certified compliant to HIPAA Security rules may provide an entity proof that they took reasonable and diligent security precautions to protect that information.

And, there are significant penalties associated with non-compliance, including criminal penalties (imprisonment of 1 - 5 years and fines of \$50,000 - 250,000).

HIPAA FINAL PRIVACY REGULATIONS

The DHHS Privacy regulations do not preempt state law or other federal law and as such effectively establish a statutory floor for privacy. That is, any State law or regulation that is contrary and more stringent than the Privacy rule retains primacy. The same is true if a federal law prohibiting a covered entity from using or disclosing PHI and the Privacy rule permits the use or disclosure of that same information, then the other federal law retains primacy. The downside is that this means that every covered entity will have to maintain some form of State to federal regulation matrix to ensure that they are complying with the correct laws and/or regulations. In order to determine which state laws are contrary and more stringent, the rule has defined “contrary” and “more stringent”. Under the definitions, essentially, the State law will retain primacy if the covered entity would find it impossible to comply with both the State and federal requirements or if the State law was an obstacle to implementing the federal regulations AND the State law provided greater privacy protections than the Federal regulations.

Although the Privacy rule does not preempt State law, the rule does provide a process for any person (not just a State) to submit a request for an exception determination. This process would be applied to all the regulations. Note: The final Privacy rule eliminates previous provisions for advisory opinions.

DHHS does not have the power to define penalties more stringent than those already found in the HIPAA legislation. The civil and criminal penalties currently contained in HIPAA will apply. Up to \$250,000 or five years for criminal penalties and up to \$25,000 per violation for civil penalties. Unlike fraud and abuse compliance where the OIG has negotiated and assessed huge civil financial penalties (some estimated up to \$100M), HIPAA civil penalties are considered inconsequential and if levied would be less than the cost of compliance for most larger organizations. Since the civil penalties are not considered severe enough to discourage violation, there is concern that the HIPAA enforcement may focus on the criminal penalties when unauthorized disclosure of protected patient information is involved. The good news is that criminal prosecution is easier to defend than civil prosecution since the plaintiff (government) has to have to have a unanimous

verdict vs. majority, proof beyond reasonable doubt vs. preponderance of evidence and normally the prosecution must prove intent. If a covered entity can show reasonable diligence in complying with the privacy and security regulations, they should be able to avoid criminal prosecution. **DISCLAIMER: The foregoing or any other mention of legal recourse in this document concerning HIPAA legislation is the personal opinion of the author and not to be construed as a legal opinion for the reader or the reader's organization. The reader should consult with their professional legal counsel to obtain a legal opinion appropriate for their circumstance.**

ENFORCEMENT PROVISIONS

The Privacy rule mandates that a covered entity provide a complaint logging and tracking process for both employees and patients. DHHS may receive complaints on privacy violations, so it behooves a covered entity to ensure that it has communication channels open to both employees and patients to circumvent their complaining directly to DHHS. There is also a whistleblower provision that protects individuals, employees, covered entities and their business associates from prosecution and retribution. There are also provisions that a covered entity would not take retributions against individuals or employees reporting violations. This provides that a covered entity is not in violation if an employee or business associate discloses PHI to a health oversight agency or health care accreditation organization or attorney for the purpose of determining legal options with respect to whistle blowing. This is very similar to the process that the OIG mandates for fraud and abuse compliance and a covered entity should be able to incorporate a Privacy Hotline concept into their current fraud and abuse compliance process.

While DHHS has promised an Enforcement NPRM mid 2001, they have delegated all of their HIPAA enforcement authority to the Office of Civil Rights (OCR) and have given us a peek at their intentions. This means that OCR will handle all HIPAA compliance issues, including; (1) Imposing civil penalties and making referrals for criminal prosecution, (2) Making exception determinations, (3) overseeing-Overseeing voluntary compliance through technical assistance and other means, (4) Responding to questions regarding the rules and providing interpretation and guidance, and (5) Responding to state requests for exception determinations.

For purposes of enforcement, the Secretary must be provided access to a covered entity's facilities, records, books, accounts and other sources of information, including PHI, at any time and without notice where exigent circumstances apply. Further, covered entities must cooperate with investigations as well as compliance reviews.

Note 1: The sanctions and penalties do not apply to workforce members of a covered entity.

Note 2: Covered entities must give individuals notice of the right to file complaints with the Secretary – see notice consent and authorization below.

Note 3: Any complaints to the secretary must be filed within 180 days of when the complainant know or should have known that the

KEY PRINCIPLES OF THE PRIVACY REGULATIONS

The Privacy rule incorporates five key principles: Boundaries, Security, Consumer Control, Public Responsibility and Administrative Requirements.

Boundaries – What are the limits of coverage and who is covered?

What's Covered? – Protected Health Information (PHI)

With a couple of exceptions, PHI includes all individually identifiable health information that is transmitted or maintained in any form or medium. This includes paper and oral. In this context, “individual” is defined as the person who is the subject of the individually identifiable health information. A personal representative is any person that the individual designates to act on their behalf and must be treated as the individual, except under specified circumstances. Unless state law has given minors the ability to obtain health care without consent of a parent, minors do not have the authority to act under the rule. Nor does the rule affect parental notification laws. If, under applicable law, a parent can act on behalf of unemancipated minor, the covered entity must treat the parent as the personal representative. The authority of a personal representative is limited only to the extent that PHI is relevant to the matters that the personal representative is authorized to act.

The exceptions are for individually identifiable health information in “education records” governed by FERPA and for records of students held by post-secondary educational institutions of students 18 or older that are used exclusively for health care treatment and which have not been disclosed to anyone other than a health care provider, at the student’s request.

Note 1: The FERPA exception only applies to federally funded schools and only to the records. If the school employs a school nurse then they would be a health care provider and would be a covered entity if they transmitted a standard transaction.

Note 2: If information about a second person is included in the medical record of the individual, the information about the second person does not have the individual’s rights is not protected as an individual.

De-identified Information: The Privacy rule gives us specific guidelines on de-identifying health information. There are two methods outlined where a covered entity can render PHI de-identified.

- 1) A person with appropriate knowledge applying generally accepted statistical and scientific methods makes a determination that the risk of re-identification of certain information is very small that the information could be re-identified by the anticipated recipients.
- 2) Removes all of the following identifiers of the individual, relatives, employers and household members. – Providing that the covered entity has no actual knowledge that after removal of the following could be used alone or combined with other information to re-identify an individual.
 - a. Names

- b. All geographic codes smaller than State, including street, city, county, precinct or zip code. However, the first three digits of the zip code may be used if it represents more than 20,000 people (per the most recent data from the Bureau of Census).
- c. All date elements related to an individual. The year element can be kept except for any age indicator for individuals over age 89. For individuals over 89, the age may be aggregated into a 90+ category.
- d. Telephone number, fax number, Email address, SSN, medical record numbers, health plan beneficiary number, account numbers, certificate/license numbers, any vehicle identifiers (serial number, license plate, etc.), device identifiers & serial numbers, URL's, IP address, biometric identifiers (e.g. fingerprint, voice print, etc.), full face photographic or comparable images, any other unique identifying number, characteristic or code.

Note: Gender, race, ethnicity and marital status do not need to be removed.

Whose Covered – Covered Entities and Business Associate Agreements:

Covered Entities:

A covered entity may be a multiple function entity, that is they may combine the functions or operations of health care providers, health plans and clearinghouses under a single legal entity, affiliated entity or other arrangement. It is the components that must be looked at and meet the rule, depending on the component's function. That is, if a component is operating as a health care provider, then that component must meet the requirements of the rule applicable to a health care provider. However, components may not share PHI and must keep it segregated from any joint information systems. For example, a provider component could not share PHI with a health plan component unless the individual was a member of both components.

For "hybrid entities", those that have separate components that perform both non-health care and health care functions, the determination of whether the entire entity or just the component that performing health care functions is based on whether the component performing the health care functions is most of what the entity does. For example, for an insurance company that has multiple lines of business, property & casualty, liability, life and health, we would look at the health line and if the health line represented most of the revenue of the insurance company, then the whole company would be a covered entity, if not then only the health line component would be a covered entity. In the case of hybrid entities, where only a component is a covered entity, there would have to be firewalls established to protect the PHI of the covered component.

There are also "affiliated entities", such as hospital chains that are legally distinct but share common ownership (5 percent or more) or control (if the entity has the power to significantly influence or direct the actions or policies of another entity). These entities can designate themselves or their health care components as a single covered entity.

Health Care Providers

Health care providers are not covered unless they first transmit any health information in electronic form in connection with

any of the covered transactions. However, a provider that does not submit covered transactions becomes covered when other entities (hospital, billing service, etc.) transmit standard transactions on their behalf.

In the context of the Privacy rule, “health care” includes: (1) Preventative, diagnostic, therapeutic, rehabilitative, maintenance or palliative care and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Specifically, health care provider means a provider of services as defined in Section 1861(u) and 1861(s) of the Act and any other person or organization who furnishes, bills or is paid for health care services or supplies in the normal course of business.

Note: Procurement or banking of organs, blood, tissue, sperm, eyes or other human product is not considered as health care under the rule and entities solely providing those services are not health care providers.

Examples of Health Care Providers and/or services that would qualify as a provider:

1. Services: Physicians’ services, hospital services, diagnostic, physical and occupational therapy, rural health clinic services, home dialysis supplies and equipment, counselors, clinical psychologists and social workers, certified midwives, podiatrists, dentists, chiropractors, physicians, assistants, nurses, paramedics, emergency medical technicians, etc.
2. Facilities: Hospital, critical access hospital, dialysis centers, skilled nursing facility, comprehensive outpatient rehab facility, home health agency, diabetes outpatient facility, portable screening mammography, hospice program, etc.
3. Other: Pharmacies, durable medical equipment suppliers, ambulance service, nursing homes, prosthetic device suppliers, drug manufacturers (to the extent they provide services to physicians to assist in determining the use of their drugs), etc.

Health Plans

The rule specifically names the following as covered under a health plan: (1) Group health plan qualifying under ERISA, including insured and self-insured plans that have fifty or more participants –or- is administered by an entity other than the employer that establishes and maintains the plan, (2) Health insurance issuer, insurance company, insurance service or insurance organization licensed to engage in the business of insurance in a state and is subject to state or other law that regulates insurance, (3) Health maintenance organization (HMO), (4) Medicare Part A and B, Medicaid title 19, (5) Issuer of Medicare supplemental policy, (6) Issuer of long-term care policy, but NOT including a nursing home fixed indemnity policy, (8) Employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering health benefits to employees of two or more employers, (9) CHAMPUS, (10) VA, (11) Health care program for active military personnel, (12) Indian Health Services, (13) Federal Employees Health Benefit Program (FEHBP), (14) Approved state child health plan, (15) Medicare Plus Choice program, (16) high risk pools, including those that do not meet the definition of high risk pool under section 2744, AND....

Any other individual plan or group health plan or combination that provides or pays for the cost of medical care.

There are some exceptions: (1) Any plan, policy or program that provides or pays for the cost of excepted benefits as defined in sec. 2791©(1) of the PHS Act, 42 U.S.C. 300gg-91©(1), (2) Any government funded program that does not have as their principal purpose the provision of or payment of the cost of health care, but which do incidentally provide such services (e.g. WIC & Food Stamp Program). (3) Any government funded program that has as their principal purpose the provision of health care (e.g. Ryan White Comprehensive AIDS Resources Emergency Act & immunization programs). Note: While these may not be covered as health plans, most will be covered as health care providers.

Clearinghouses

Clearinghouse is treated the same in the Privacy rule as in the final Transactions rule. Essentially, a clearinghouse is any entity, including billing services, repricing companies (e.g. TPO), community health management information systems (CHIN), and value added networks (VAN) networks and switches that: (1) Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction, or (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into a nonstandard format or nonstandard data content for the receiving entity.

The above definition would include any billing service or TPO that transmits a standard transaction, but does not include a VAN unless they also perform the described translation services. Also not covered as a clearinghouse are departments or components of health plans and health providers that may translate internally for their own use.

Business Associates and Business Associate Contracts (BAC)

Unfortunately, under HIPAA legislation, the “Covered Entities” are limited to a provider organization that transmits any of the nine-named transaction in the EDI standards portion (claims, ERA, eligibility, etc.), payers and clearinghouses. This is unfortunate because the administration clearly wants to protect health information no matter where it resides and the only way they can impact entities other than the specific covered entities is to hold those covered entities responsible for the violations of their business associates. Therefore, DHHS has mandated that covered entities must have a Business Associate Contract (BAC) with their business associates that binds the business associate, among other things, to comply with the covered entities’ privacy practices and to provide protections for any PHI that it receives from the covered entity. A business associate is any entity that performs services to or on behalf of a covered entity and uses or discloses protected health information that belongs to the covered entity. This includes business associates that create or receive protected health information on behalf of a covered entity. That is, if the performance of any service involves disclosure of protected health information by the covered entity to the business associate. It is the relationship of the entities that creates the business associate relationship, not the type of entity. It should be noted here that since covered entities can also have business associate relationships that a violation of a BAC by a covered entity is a direct violation of the Privacy rule. Under the Privacy rule the covered entity is subject to sanctions, but only if they knowledge of their business associates wrongful activity and fail to take the required action address them.

Exceptions to the BAC requirements:

1. For disclosure of PHI to a health care provider for the purpose of treatment.
2. Financial institutions processing consumer-conducted financial transactions by debit, credit or other payment card, clears checks, funds transfers or any other activity that directly facilitates the transfer of funds for compensation for health care. However, when a financial institution performs any other service, such as billing or remittance processing, they become a business associate. A financial institution could be the conduit of a remittance advice (X12N 835) and not be a business associate only if the transaction were encrypted such that the financial institution had no access.
3. Group health plan is not required to have a BAC with their plan sponsor. – However, the plan sponsor is required to have plan documents that specify (1) the permitted uses and disclosures of PHI, (2) disclosure is permitted only upon receipt of certification from the plan sponsor that the plan documents have been amended and the plan sponsor has agreed to certain conditions regarding the use and disclosure of PHI and (3) provide adequate firewalls to identify the employees or classes of employees who will have access to PHI; restrict access solely to the employees (or class of employees) identified and for only the functions performed on behalf of the group health plan; and provide a mechanism for resolving issues of noncompliance. Any disclosure to employees to classes of employees not identified in the plan documents is not permissible.

Instead of the a group health plan having to audit or examine the sponsors plan documents, the plan sponsor is required to certify to the group health plan that the plan documents have been amended to agree to: (1) not use or further disclose PHI other than in accordance to the plan documents, or as required by law, (2) ensure that any subcontractors or agents to whom the plan sponsor provides PHI also agree to the same restrictions; (3) not use or disclose the PHI for employment related actions; (4) report to the group health plan any use or disclosure that is inconsistent with the plan documents or this regulation; (5) make the PHI accessible to individuals; (6) allow individuals to amend their information, (7) provide an accounting of its disclosures; (8) make its practices available to the Secretary for determining compliance; (9) return and destroy all PHI when no longer needed, if feasible and (10) ensure that the firewalls have been established.

4. Certain jointly administered government programs that are health plans if eligibility or enrollment in the health plan is determined by an agency other than the agency administering the health plan. This referred to programs offering benefits to members of the public – not to those offering benefits to government employees or retirees.
5. A conduit is not a business associate and a BAC is not required with conduits. Conduits are persons or organizations that act merely as a conduit for PHI. This include US Postal Service, ISP's, phone companies, etc.
6. Just because two covered entities participate in an organized health care arrangement does not make either of them business associates of the other. Participating in joint activities does not mean that one party is performing services to or on the behalf of another entity.

Some examples relationships requiring and not requiring a BAC:

1. BAC is required for billing services, collection agencies, and software vendors who have access to patient information for support and/or implementation.
2. BAC is required for a clearinghouse, when the clearinghouse is performing a function on the behalf of the provider or health plan.
 - a) BAC required if clearinghouse is receiving transactions from a provider on behalf of health plan.
 - b) BAC required if clearinghouse is sending transactions to a health plan on behalf of a provider.
3. BAC required for business associates performing legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation and financial services.
4. A provider in private practice and contracting with a health plan to perform case management would be both a business associate of the health plan and directly covered under the Act as a provider in their private practice.
5. Employer contracting with an insurance carrier to insure their health plan would not require a BAC – but may require a plan sponsor certification.
6. Employees to not require a BAC.
7. Contracted employees that perform a substantial proportion of their work at a covered entities premises may either be treated as employees or as business associates using a BAC. If there is no BAC, for compliance purposes, HHS will treat the contracted employee as a member of the workforce.
8. A hospital would not need a BAC with staff physician or other providers.
9. A hospital that performed billing services for staff providers would be a business associate of the provider and the provider would need to have a BAC with the hospital.
10. Oversight agencies are not business associates, therefore a provider would not need to enter into a BAC with a state reporting agency to provide information required by law.
11. A group health plan purchasing insurance coverage from a health insurance issuer does not make the issuer a business associate; therefore no BAC would be required.

Business Associate Contract Terms & Requirements

A covered entity must take reasonable steps to cure a breach or violation of the BAC only if they know of a pattern of activity, or practice, of the business associate that was a material breach or violation of the BAC. However, if the covered entity does take action, but fails to cure the breach or violation, they must terminate their contract with the business associate – or if that is not feasible – inform the Secretary of the problem. The “not feasible” provision is intended to accommodate a covered entity when there are no other viable alternatives to their business associate – but not because their business associate is more convenient or less costly than other alternatives. If the covered entity fails to take action, then they are subject to sanctions.

Terms of the BAC:

1. State the purpose for which the business associate can use and disclose PHI and generally indicate the reasons and types of persons to whom the business associate can make further disclosures. The purpose may be for data

aggregation to undertake quality assurance and comparative analyses that involve the PHI of more than one contracting entity.

2. May allow a business associate to use the PHI as necessary to carry out their proper management and administration – or- to carry out their legal obligations.
3. May allow a business associate to disclose PHI if such disclosure is required by law – or- the business associate obtains reasonable assurances from the person whom the PHI is disclosed that it will be held confidentially –and- the person agrees to notify the business associate of any circumstances in which it is aware that confidentiality has been breached.
4. Provide that the business associate will not use or disclose the PHI other than as permitted in the BAC or required by law.
5. That the business associate will use appropriate safeguards to prevent use or disclosure of the information other than as provided for in the BAC.
6. Report to the covered entity any use or disclosure of the information not provided for in the BAC for which it becomes aware.
7. Ensure that any of the business associates agents or subcontractors that it provides PHI agree to the same conditions and restrictions as BAC. ** This does not apply to disclosures that the covered entity could make to other entities without a BAC. E.g. a billing service providing PHI to a health plan for the purpose of payment.
8. Make available PHI in accordance with the “access of individuals to PHI” provisions of the rule.
9. Make available PHI in accordance with “right to amend PHI” provisions of the rule.
10. Make its internal practices, books, and records relating to the use and disclosure (including creating or receipt) of the PHI relating to the covered entity available to the Secretary for the purposes of determining the covered entity’s compliance.
11. At termination of the contract, if feasible, return or destroy all PHI received from or created or received on the behalf of the business associate. If the return is not feasible, extend the protections to limit the uses and disclosures to those that make it necessary for the business associate to retain the information.
12. Authorize termination of the contract by the covered entity in the event the covered entity determines that the business associate has violated a material term of the contract.

Notes:

1. If the covered entity and the business associate are both government entities, a Memo of Understanding (MOU) can be used if it contains terms that accomplish the requirements of the BAC – or if other law (including regulations promulgated by either entity) contains requirements that accomplish the objectives of the BAC.
2. If a business associate is required by law to perform services for a covered entity, then the covered entity, without need of a BAC, can disclose PHI to the extent necessary for the business associate to comply with t he law. Provided however, that the covered entity makes a good faith attempt to obtain satisfactory assurances of protections from the business associate and documents the attempt and any reasons assurances were not obtained.
3. BAC may not authorize a business associate to make disclosures that would not be permitted to be made by the covered entity.

4. A business associate that contracts with multiple covered entities cannot use or disclose PHI received or created in its relationship with one covered entity to another covered entity. Unless such disclosure or use would be a lawful disclosure permitted between the covered entities and the BAC with each of the covered entities permits such disclosure. An example would be a clearinghouse that contracts with a MSO and all of the MSO participants agree to allow the clearinghouse to send their PHI to the MSO.
5. A business associate providing data aggregation to different covered entities could combine and use the PHI of the covered entities to assist the covered entities in their health care operations (e.g. utilization review, fraud & abuse determination).
6. Covered entities may rely on the professional judgment of their business associates as to how much PHI is needed by them to perform their activity.

Security – Protection of PHI

The Privacy rule requires safeguards defined as appropriate administrative, technical and physical safeguards to protect the privacy of PHI. That is, a covered entity must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of the Privacy rule. There are no proscribed implementation measures and as in the Security NPRM, the implementations will vary according to the type and size of the covered entity. Examples given are requiring documents with PHI to be shredded prior to disposal, requiring doors and/or file cabinets housing medical records to be locked and limiting access to authorized personnel. This is intended to be a common sense, scalable standard. Covered entities are NOT required to guarantee the safety of PHI against all threats. Theft of PHI would not be a violation of the Privacy rule if the covered entity had reasonable policies to protect against theft.

DHHS will closely harmonize the final Security rule with the Privacy rule. The Privacy rule requires covered entities to develop role-based access rules in order to implement the requirements for “minimum necessary” uses and disclosures of PHI. For example, the current Security NPRM has a “need to know” provision for access control that we expect to be aligned with the “minimum necessary” provision in the Privacy rule.

There is also language in the Privacy rule that suggests that the audit trail provisions in the Security NPRM are limited to recording each time a record is altered, but not viewed or browsed and that audit trails may not distinguish the difference between access for use and accesses for disclosure. Currently audit trails in the security NPRM are left to the discretion of the covered entity. However, the Privacy rule is clear that some form of log is required for all disclosures of PHI not for the purpose of treatment, payment or health care operations (see Consumer Control below).

Consumer Control – Controlling Disclosures and Right to Access

The underlying principal of consumer control, is that with some exceptions for the purpose of treatment and limited exceptions for public responsibility (see the next section), the individual should be able to know the circumstances under which their PHI is used and disclosed and be able to control when and to whom their PHI is disclosed, and the purpose for

such disclosures. Except for disclosures for the purpose of treatment, payment and health care operations, the individual has the right to request and receive an accounting for all of the disclosures of their PHI and know to whom their information has been disclosed and the purpose for such disclosures, even in the event of disclosures that do not require individual consent or authorization. The individual has a right to be informed of the privacy policies of the covered entity and be able to take that information into account in the process of choosing a covered entity. For the purpose of the rule, use is defined as internal use within an entity that maintains the PHI and disclosure is defined as the release, access or transfer of the PHI outside the covered entity.

The protection of an individual's PHI survives an individual's death and must be given for as long as the covered entity maintains the information.

Minimum Necessary Disclosure/Use Provision:

One stipulation for disclosure is the minimum necessary provision that states that, with the exception of uses and disclosures for the purpose of treatment, any patient information disclosed be limited to the minimum amount necessary to accomplish purpose of disclosure. The provider is responsible for determining the minimum amount needed except when responding to payer requests and then it becomes the responsibility of the payer to request only the minimum amount necessary. This includes internal uses so that each entity must define what information will be made available to each employee by role. For example, a billing clerk may have access to the information needed to performing the billing role that would not include the clinical information that would be available to a coding specialist. This also means that each covered entity must develop policies and procedures that define the PHI that an employee needs to perform their job function and limit their access to only that information. This is predicated on reasonableness and the technical feasibility of controlling such access.

DHHS was also very concerned that there be a balance and common sense applied to the disclosures for the purpose of patient care and gave the provider some latitude in making such disclosures. For example, providers should have the freedom to exchange information, consult and review other patient records for comparison purposes (e.g., radiologist looking at the last 10 MRIs for a particular diagnostic scan). There is no intent in the rule to impose unreasonable barriers to the provision of health care.

The final Privacy rule provides a three-tiered approach to individual control.

1. Covered entities must provide a notice of their privacy practices;
2. With a some exceptions of use and disclosure of PHI not requiring permission of the individual, covered in detail below, covered entities must seek permission from the individual to use or disclose their PHI. This is divided into three distinct forms of providing permission. First is "consent" which addresses the use and disclosure of PHI for treatment, payment and health care operations, second is uses and disclosures which require an opportunity for the individual to agree or object and third, an authorization, which essentially addresses the use of PHI for all other purposes.
3. Right of the individual to access, copy and amend their medical record.

Notice of Privacy Practices:

All individuals, except inmates, have a right to receive a notice from any covered entity that communicates their privacy practices. The individual does not have to have a customer or patient relationship with the covered entity to receive a notice; the covered entity's notice is intended to be a public document.

All covered entities, including group health plans, including self-insured plans are required to provide a notice to individuals of how they plan to use and disclose the individual's PHI and of the individual's rights with respect to that information. An organized health care arrangement or covered entities under common ownership and control who have designated themselves as a single covered affiliated entity and have agreed to abide by all the terms in the notice, may produce a single notice for all of their controlled entities. However, affiliated entities that remain separate must produce separate notices for each of the entities. Correctional institutions and clearinghouses that only use or disclose PHI only as business associate of other covered entities do not have to produce notice. If a covered provider who is part of an organized health care arrangement has different privacy practices at their office then the practices described in the joint notice, they are required to produce a separate notice that accurately describes their privacy practices.

A covered entity's notice does not need to document all of the entity's privacy practices. The notice need only explain the entity's privacy practices in generalities. For example, while the rule requires detailed policies and procedures regarding the implementation of the individual's right to access and amend their record, the covered entity need only explain generally that individuals have the right to inspect, copy and amend information about them and tell them how to exercise that right.

Covered entities may be also be required to produce more than one notice. Those covered entities operating in more than one state may need to produce more than one notice to reflect the unique laws of each state in which they operate or a covered entity that has both provider and health plan components would need to produce separate notices for each component. Notices must accurately convey the privacy policies that are relevant to the individuals receiving them.

HHS encourages covered entities to be as clear as possible the language used for the notice and to include optional elements in the notice that describe more limited use and disclosures than are actually permitted under law. For example, some covered entity's may want to assure the individual that even though the law permits them to disclose PHI for a wide array of purposes, that they will only disclose PHI in very specific circumstances as required by law or to avert a serious and imminent threat to health or safety.

The covered entity is not permitted to use or disclose PHI beyond what is stated in their notice. In the event the entity materially changes their privacy practices, polices or procedures, the notice must be revised to reflect those changes. See reservation of rights to revise below.

The notice is intended to be a public document available to anyone making a request. It is HHS intent that it be available for people to make informed decision about purchasing health care products. Notices can be delivered electronically, if the individual has agreed to such receive materials electronically. However, any covered entity providing notices electronically must also be able to provide one on paper, if requested and state in the notice the individual's right to receive a paper copy. All covered entities that obtain consent must provide notice in conjunction with obtaining consent.

Health plans must provide notice to all enrollees by the compliance date and after the compliance date to all new enrollees. Health plans must also notify enrollees at least once every three years informing them how to obtain a copy of the notice. Once copy to the member (name insured) also serves for all dependents.

Health care providers with direct treatment relationships must provide notice by the first day of service, whether delivered on-site or electronically, after the compliance date. The notice, and any revisions to the notice, must be also be promptly and prominently posted at the site of service and be available for individuals to receive on request. Providers with indirect relationships are only required to produce notices on request. In the event an individual's first service from a covered provider is electronic (e.g. web pharmacy), then the notice must automatically be provided to the individual concurrently with the request for service. If any covered entity included in a joint notice distributes the notice, then the notice has been distributed for all the entities included in the joint notice.

Requirements For The Notice:

1. Plain Language: The notice must be written in plain language. Plain language means a reasonable effort to: (1) Organize material to serve the needs of the reader; (2) Write short sentences in the active voice, using "you" and other pronouns; (3) use common, everyday words in sentences; and (4) divide material into short sections.
Note: There appears to be some expectation for covered entities in cases where they serve a significant population of non-English speaking persons to provide notice in the language of the recipient. While this would appear to be a requirement under The Civil Rights Act of 1964 for covered entities receiving federal assistance, it is unclear how HHS would treat those covered entities not receiving federal assistance. Likewise there appears to be some expectation by HHS that covered entities would accommodate the needs of individuals who cannot read.
2. Header Wording: The header of the notice must contain the specific wording; "THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."
3. Uses and Disclosure Under Law: Must inform individuals of all the uses and disclosures that the covered entity is required or permitted to make under all applicable law. However, the covered entity may not include statements that would limit the entity's ability to make uses or disclosures that are required by law, or necessary to avoid a serious and imminent threat to health or safety.
 - a. Clearly describe all the uses and disclosures of PHI they are permitted or required to make under the rule without individual authorization or consent. Each use and disclosure must be described separately.

- b. Clearly describe all the uses and disclosures of PHI, including at least one example of each, that they are permitted to make with consent for treatment, payment and health care operations.

Note: If any other applicable law prohibits or limits the covered entity's ability to use or disclose PHI that would be permitted under the Privacy rule, the notice must describe only the uses and disclosures permitted under the more stringent law.

4. Authorization: Must state that any uses and disclosures other than those in 3 above will be made only with the individual's authorization, and that the individual has the right to revoke such authorization.
5. Separate Statements of Use and Disclosure: If the covered entity intends to conduct any of the following uses and disclosures, a separate statement is required for each.
 - a. That the covered entity may contact the individual to provide appointment reminders or information about treatment alternatives or other health related benefits and services that may be of interest to the individual.
 - b. That the covered entity may contact the individual to raise funds for the covered entity.
 - c. A group health plan, health insurer or HMO may disclose PHI to the sponsor of the plan (employer).
6. Statement of Individual Rights: Statement of individual rights with a brief description of how the individual may exercise each of those rights as follows:
 - a. Right to request restrictions on specific uses and disclosures of PHI – and – a statement that the covered entity may refuse the request.
 - b. Right to receive confidential communications.
 - c. Right to inspect and copy their PHI.
 - d. Right to amend their PHI.
 - e. Right to receive an accounting of disclosure of PHI not for the purpose of treatment, payment and health care operations.
 - f. Right to receive a paper copy of their notice upon request.
7. Entity's Requirements Under Law: Must state that the covered entity has a legal requirement to maintain privacy of PHI, provide a notice of their duties and privacy practices, and to abide by the terms of the notice.
8. Reservation of Right to Revise: Should state that the covered entity reserves the right to change and revise its privacy practices to PHI previously created or received and how it will provide individuals with a revised notice. If this statement is not included in the notice, then if the covered entity changes its privacy practices, any PHI previously created or received prior to the date of revision, cannot be included in any use or disclosure which was not contained in the notice prior to the date of revision. In fact, if there is no reservation of right to revise stated, then the records must be segregated so that any information created or received prior to the revision date would be prevented from being used for any additional uses and disclosures contained in the revised notice.
9. Complaint Procedures: Statement of how, if an individual believes their privacy rights have been violated, how they may file a complaint with the covered entity, including naming a person as a point of contact and the contact person's phone number. There must also be a statement that the individual has a right to file a complaint with the Secretary and that there would be no retaliation for filing such complaint.

10. Effective Date: Must state the date the notice went into effect, not the date it was produced. The effective date cannot be earlier than the date the notice was published.
11. Special Requirement for Joint Notices: The joint notice must meet all requirements above, plus it must reasonably identify all of the covered entities, or class of covered entities, to whom the joint notice applies. It must also list the service delivery sites or classes of delivery sites. If the covered entities will share PHI as necessary to perform treatment, payment and health care operations, then that must be stated in the notice.

Consent:

Consent pertains to disclosures only for the purpose of “treatment”, “payment” and “health care operations”. A consent does not have to include all three factors, but a covered entity cannot use or disclose PHI beyond what is covered in the consent. There are also distinctions drawn between “direct treatment” – where providers typically provide direct, face-to-face care and “indirect treatment” – where providers are acting on orders of another provider and may not directly see the patient or are acting under the direction of another provider’s order and where the results are typically furnished to the ordering provider and not the patient (e.g. radiologist, pathology, clinical lab, pharmacy). Generally, health care providers who are in a direct treatment relationship must obtain “consent” from the individual to use and disclose PHI for the purpose of treatment, payment and health care operations. Providers in an indirect treatment relationship are not required to obtain consent, but are not prohibited from obtaining consent. Other covered entities, at their option, may obtain consent, but any covered entity that attempts to obtain consent and consent is refused, the covered entity cannot use or disclose any PHI for the purposes included in the consent.

1. “Payment”: Is essentially any activity that is undertaken by a health plan to obtain premiums or fulfill its responsibility for coverage or health care providers’ activities undertaken to obtain or provide reimbursement for the provision of health care. This includes (1) Determination of eligibility and coverage (e.g. COB); and adjudication or subrogation of health benefit claims; (2) Risk adjusting amounts based on enrollee health status and demographics; (3) Billing, claims management, collection activities, obtaining payments from reinsurance, and related health care data processing; (4) Review of health care services, with respect to medical necessity, coverage, appropriateness of care, or justification of charges; (5) Utilization review activities, including pre-certification and preauthorization of services, concurrent and retrospective review of services.

Note 1: Any disclosure for payment process to a financial institution may include only the following information; (1) name and address of the account holder; (2) the name and address of the payer or provider; (3) the amount of the charge for health services; (4) the date on which health services were rendered; (5) the expiration date for the payment mechanism, if applicable; and (6) the individual’s signature.

Note 2: Only the following PHI may be disclosed to a consumer reporting agency relating to collection of premiums or reimbursement: (1) Name & address; (2) Date of birth; (3) Social Security Number; (4) Payment history; (5) Account number and (6) Name and address of the health plan or health care provider.

2. “Treatment”: Means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party;

consultation between health care providers relating to the patient; or the referral of a patient for health care from one provider to another. A health care provider may only undertake treatment; activities of health plans are not considered treatment.

3. “Health Care Operations”: The rule provides a list of activities that are included as health care operations. Since this is an area of continued confusion and concern, the following activities are exactly as found in the final rule:

- A. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
- B. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
- C. Underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of 164.514(g) (that is if a health plan receives PHI for the purpose of 3, and if benefits are not placed with the plan, then the plan may use or disclose the PHI received for that purpose) are met, if applicable;
- D. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
- E. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
- F. Business management and general administrative activities of the entity, including, but not limited to:
 - 1) Management activities relating to implementation of an compliance with the requirements of this subchapter (privacy standard);
 - 2) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;
 - 3) Resolution of internal grievances;
 - 4) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity or, following completion of the sale or transfer, will become a covered entity; and
 - 5) Consistent with the applicable requirements of 164.514 (other requirements relating to uses and disclosures of PHI), creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in 164.514(e) (uses and disclosures of protected information for marketing).

Generally, with the exception of business associates, a consent obtained by one covered entity may not be used for another covered entity. The only exception is the “joint consent” in which covered entities that participate in an “organized health care arrangement” may develop a “joint consent” in which the individual consents to the uses and disclosures of PHI by each of the covered entities in the arrangement. A joint consent must either identify the individual covered entities or class of covered entities to which the consent applies.

An “organized health care arrangement” is one that individuals who obtain services have an expectation that these arrangements are integrated and the operations are jointly managed. One example given is a covered hospital and their clinical laboratory, emergency department and providers on staff. Affiliated entities may designate themselves as a single covered entity and produce a single consent.

Health care providers may condition treatment on consent and a health plan may condition enrollment on consent, if consent is sought in conjunction with enrollment. Once, consent is obtained, it is valid until revoked in writing, which may be done by the individual at any time. However, a health care provider may refuse to continue to treat an individual who has revoked consent and a health plan may disenroll an individual who revokes consent, provided that the consent was sought in conjunction with the individual’s enrollment. Upon receipt of a revocation, the covered entity must stop processing the PHI for use or disclosure, except to that extent that it has taken action on reliance of the consent (e.g. bill for treatment already performed before the consent was revoked).

There are some exceptions to the requirement of consent for health care providers in certain treatment situations. These are; (1) Emergency treatment situations, however, the health care provider must attempt to obtain consent as soon as reasonably practical; (2) Where the health care provider is required by law to treat the individual and the health care provider attempts to obtain consent and; (3) Where there are substantial barriers to communication and, in the exercise of professional judgment, the circumstances infer the individual’s consent. In all of these cases, if consent is not obtained, the provider must document the attempt and the reason consent was not obtained.

Specific rules and parameters concerning the consent document are as follows:

1. Consent must reference and refer the individual to the covered entity’s notice of privacy practices. A consent may not be combined in a single document with the notice.
2. Consent must indicate that the individual has the right to review the notice prior to signing. If the provider has reserved the right to change its privacy practices the consent must state that the notice may change and describe how to obtain a revised notice.
3. In addition to treatment, payment and health care operations, the consent may combine other forms of legal permission. For example, the consent may be combined with a state law requirement for consent to use or disclose HIV/AIDS information.

4. If other legal permission is combined in the consent document then they must be visually and organizationally separate from the consent for treatment, payment and health care operations and require separate signatures and dates.
5. Where research includes treatment of the individual, consent may be combined with an authorization for the use or disclosure of PHI created for the research. NOTE: This is the only circumstance consent may be combined with an authorization.
6. Consent must state that the individual has the right to request restrictions on the use and disclosure of their PHI, but must also state that the covered entity may refuse the request.
7. If the consent lacks a required element, it is not valid.
8. Covered entities must document and retain any consents.

NOTE: There may be occasions where an individual has signed multiple consents and/or authorizations that may conflict. The covered entity must abide by the most restrictive consent or authorization. For example, a nursing home may have had an individual sign an authorization to obtain a copy of their medical record from their physician. However, the physician may have previously obtained consent from the individual for treatment purposes. If the nursing home authorization granted permission for the physician to disclose genetic information but the consent excluded such information, then the physician must adhere to the more restrictive consent. When there is such a conflict, a covered entity may resolve the conflict by obtaining either a new written or oral consent – oral consent must be documented.

Authorization:

Generally, authorizations are required for all use and disclosure not required by law, for the purpose of public safety (see Public Responsibility below) or covered under consent or right of an individual to agree or object. Authorizations must be obtained by covered entities even to use the PHI for their own use.

1. If a Covered provider produces an authorization, then it must contain a statement that treatment may not be conditioned on an authorization, except when providing research related treatment. In the case the authorization is for the use of the covered entity, it must also include a description of the extent to which it will not use or disclose the PHI it obtains in connection with the research protocol for purposes that are permitted without individual authorization.
2. For the purposes of research, covered health care providers must obtain separate authorizations for; (1) The use of PHI created during the research and (2) Any existing PHI that the covered provider may maintain.
3. A description of each purpose for which the PHI will be used or disclosed.
4. If by a health plan, a statement that enrollment or eligibility of benefits may not be conditioned on an authorization, except to the extent that the authorization is not for psychotherapy notes and is sought for the health plans eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations. However, A health plan may condition payment of a claim for specific benefits on an authorization, if it is not for psychotherapy notes and is needed to determine payment of a claim;
5. Statement that the individual may refuse to sign and that they may inspect or copy the PHI to be used or disclosed.
6. A covered entity may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party.

7. An individual may revoke an authorization in writing at any time. If the authorization was obtained as a condition of obtaining insurance coverage, the health insurer has the right under other law to contest the claim.
8. A covered entity must document and retain any signed authorizations.
9. Contain a specific description of the information to be used or disclosed.
10. Identify the name or class of persons to whom the PHI will be disclosed.
11. Contain an expiration date or event that relates to the purpose.
12. Define the purpose of disclosure.
13. Contain a statement that the individual has the right to revoke the authorization in writing and describe how it may be revoked.
14. A statement that the PHI used or disclosed may be subject to re-disclosure and may not longer be protected.
15. Signature of the individual or personal representative (including a description of the personal representatives authority) and date. A copy must be provided to the individual.
16. Be written in plain language – see plain language in Notice above.
17. If any remuneration results from the use or disclosure, a statement that the covered entity will receive remuneration.
18. If the covered entity has received consent or provided notice, the authorization must refer to the consent and/or notice and state that any respective statements are binding.
19. An authorization may not be combined with any other document to create a compound except for research that included treatment.

Special considerations of authorization:

Marketing: Defined as a communication about a product or service of which is to encourage recipients of the communication to purchase or use the product or service. There is no limit to the type or means of communication. Generally authorization must be obtained for any marketing activities, however the rule gives providers and health plan quite a bit of leeway in discussing treatment related services or products. The exceptions to marketing that do not require authorization are: (1) Any activity related to treatment, payment or health care operations; (2) Communications made by a health care provider as part of the treatment and for the purpose of furthering the treatment of that individual. This means that health care providers are free to use or disclose PHI as part of a discussion of its products and services, or the products and services of others, and to prescribe, recommend or sell products and services as part of the treatment. This includes referrals, prescriptions, recommendations and other communications that describe how a product or service may relate to the health of the individual; and (3) Communications tailored to an individual made by a health plan or health care provider to an individual in the course of managing treatment, including recommending alternative treatments, therapies, providers, or settings of care.

Psychotherapy Notes: Must be separated from the rest of the individual's medical record to qualify as psychotherapy notes. Health plans may not request authorization to use or disclose psychotherapy notes for determination of benefits, underwriting, issuing insurance or payment of claims. Authorizations for psychotherapy notes may not be combined with any other authorization or consent.

Revocation: Covered entities will only be responsible for implementing a revocation if they have direct knowledge of the revocation. For example, a government agency may obtain an authorization for all providers who have seen the individual in the past year. If the individual sends a written revocation to the agency, the rule cannot control the agency and they cannot be required to inform all of the providers that there has been a revocation. Therefore, if a covered entity does not know about a revocation, they are not violating the rule by acting on the authorization.

Fund Raising: Fund raising is a named health care operation and for the purposes listed in the health care operation definition, no authorization is required, even to release demographic information to a third party institution raising funds on behalf of the covered entity.

Disaster Relief: There is no requirement to obtain authorization for the purpose of disclosing PHI to federal, state, local or private agencies engaged in disaster relief activities.

Uses & Disclosures Requiring an Opportunity for the Individual to Agree or Object:

These are circumstances where the environment is informal and agreements are made orally, without written authorizations. Essentially, the final rule details purposes for which an individual must be informed in advance of the use or disclosure of their PHI, the purpose and be given a meaningful opportunity to prevent or object to the use or disclosure. The circumstances and situations are as follows:

1. Facility Directories: Allows health care providers (typically facilities) to include patient information in their directory only if they inform incoming patients of their directory policies, the patient doesn't object and give patients an opportunity to opt out of the directory listing or restrict some of the information to be included. In the event the patient is incapacitated or in emergency treatment circumstances, the health care provider can use their professional judgment whether to include the individual's information and what information to include in the facility directory. However, the individual must be given the opportunity to object as soon as practical after the individual is capable of making a decision. Additionally, if the provider learns of an incapacitated individual's prior wish not to be included in the directory, the facility must not include the individual's information in the directory.
2. Disclosure to Clergy: Subject to the individual objecting, a covered entity may disclose to clergy, the individual's name, general condition (in terms that do not communicate specific medical information, individual's location, and religious affiliation. This disclosure can be made without the clergy inquiring by patient name.
3. Individual Care and Notification: Covered entities may disclose to a person involved in the current health care of an individual PHI that is directly related to the person's involvement. This would include family member, relatives, close friends, boy/girl friends, roommates, neighbors, colleagues, or any other person named by the individual. This is intended to maintain current practices with respect to involvement of other persons in an individual's care, and sharing of PHI to contact person during a disaster. This is intended to give the health care provider latitude to involve other persons that in their professional judgment are appropriate and may be needed to participate in the individual's care. If the individual has the capacity to make their own decisions, then they must be consulted and given an opportunity to

agree or object to disclosure of PHI to third parties. In the event the individual is incapacitated, the provider is use their best professional judgment and are cautioned to take circumstances into consideration that may put the individual at risk if they were to involve third parties that were the perpetrators of abuse to the individual. Generally, the provider is to exercise their professional judgment to determine whether disclosures are in the individual's best interest. They can make reasonable inferences, such as when a friend shows up at the pharmacy to pick up a prescription or sharing information with the person showing up to drive the individual home from the hospital, inform relatives of the condition of the individual.

4. Notification of Relatives: While the rule give the health care provider latitude to disclose PHI to an individuals relatives and other persons providing care, there is no requirement to verify the identify of those relatives or other persons involved in the patient's care.
5. Agreement to Disclosure Does Not Persist: Agreement by the individual to disclosure of PHI at one point in time does not imply disclosure indefinitely.

Individual Right to Request Restrictions

Generally, an individual has the right to request from any covered entity, other than a business associate of another covered entity, specific restriction on the use or disclosure of PHI covered under consent or the right of the individual to agree or object. The covered entity may refuse to agree to the restrictions. Restrictions must be documented and any documentation regarding restrictions must be retained for six years. With the exception of provision of restricted PHI to providers in an emergency treatment situation, there is no requirement to notify other entities to which they disclose PHI of the existence of any restrictions.

A covered entity may override any agreed upon restrictions in the event of an emergency treatment situation. If the information is disclosed to a provider for emergency treatment purposes, the covered entity must request the provider not further use or disclose the information.

A covered entity may terminate an agreed upon restriction by written or oral agreement that is documented. In the event the entity terminates the agreement unilaterally, the removal of restrictions only applies to information received after the termination.

Confidential Communication Requirements:

Individuals may request covered entities to provide confidential communication of PHI from the covered entity to the individual, even that information a dependent that would ordinarily be send to the member (named insured).

A patient that did not want their family members to know about a certain treatment could request that the covered entity communicate with them at their place of employment, by mail to designated address (e.g. EOB), or by phone to a designated number. An individual could also request that mail be sent in a closed envelope and not by post card.

Covered health plans and health care providers must accept any reasonable request, with the proviso that for a health plan the individual must clearly state that the disclosure of all or part of the PHI could endanger the individual. The reasonable of any request is to be determined only on the basis of administrative difficulty and not on the perceived merits of the request. However, as applicable, a request may be refused if the individual does not provide information as to how payment will be made or has not specified an alternative address or method of contact.

Right of Access and Amendment of Records:

Individuals have a right to access and amend any of their PHI maintained in a “designated record set”. A designated record set is defined as the PHI maintained by either the covered entity or their business associates, and used in whole or in part to make a decision on an individual. For health plans, the designated record set includes at a minimum; enrollment, payment, claims adjudication and case or medical records maintained by the plan. For providers, designated record set includes at a minimum the medical and billing records. However it may not include, for example, administrative notes, peer review data, quality control, morbidity & mortality data, etc. This applies to all health plans, covered providers and clearinghouses that are not acting as business associates of another covered entity.

The individual has the right to access and amend PHI for as long as it is maintained by the covered entity. The covered entity may require that any request be in writing. However, it must respond to requests in no later than 60 days. In the event they cannot respond in 60 days, one time only, they may extend the deadline by 30 days with a written statement describing the reasons for the delay and stating the date of completion.

Access:

If able, the covered entity must provide the information in the format requested by the individual and the individual may choose whether to inspect, copy or inspect and copy the information. If unable to produce the information in the format requested, then the covered entity must produce it in a form and format to which the covered entity and the individual can agree. If the individual agrees to a summary of the record, rather than the entire record, the entity may charge an agreed upon fee for producing the summary record.

The covered entity may charge reasonable cost based fees for copying the record – but the cost is not to include a fee for retrieving the record. If any state law allows a fee for record retrieval, then this rule supercedes any such state law. Or cost of (including any associated fees).

There are exceptions for psychotherapy notes, information compiled in reasonable anticipation of or use in a civil, criminal, or administrative action, and certain PHI maintained by entities subject to or exempted (including research laboratories that test human specimens but do not report patient specific results) from CLIA (Clinical Laboratory Improvement s Amendments of 1988.

Covered entities may individual deny access to their PHI for: (1) PHI excepted above, (2) inmates request of a copy of their record from a correctional institution where obtaining the copy would jeopardize the health, safety, security, custody, rehabilitation of inmates, or safety of any officer or employee or other person (this applies to copy only – inmates still have the right to access and view their PHI), (3) PHI obtained in the course of research while the research is in progress (the individual must have agreed to the denial of access in the authorization), (4) any PHI also covered under the Privacy Act, if that denial is permitted by the Privacy Act, (5) PHI that the covered entity obtained from someone other than a health care provider on the contingency of confidentiality, if the access were likely to reveal the source.

Denial may also be made for reasons that disclosure may harm the individual or others under the following specific circumstances: (1) If a licensed health care professional makes a determination that the access is reasonably likely to endanger the life or physical safety of the individual or other person. This denial may not be based on the sensitivity of the information or the potential for causing emotional or psychological harm; (2) If the information requested makes reference to another individual, other than a health care provider, and a licensed health care professional makes a determination that access is reasonably likely to cause serious harm to that other person; (3) May refuse to act upon the request of a personal representative if the covered entity has a reasonable belief that the individual has been or will be subjected to domestic violence, abuse or neglect by the personal representative, or that treating the personal representative as the individual would endanger the individual, and (4) May refuse to act upon the request of a personal representative if a licensed health care professional has determined that the information requested by the personal representative is reasonably likely to cause substantial harm to the individual or to another person. In the event a request is denied for any of the above reasons, the entity must provide a right of review and a process to have the decision reviewed by a licensed health care professional that was not involved in the original decision to deny access.

For any denials, the covered entity must provide a written explanation in plain language that explains why the request was denied. The denial must also describe how an individual may complain to both the covered entity and the Secretary, including providing the name or title and phone number of the covered entity's contact person or office that receives complaints.

A covered entity may only refuse access to information specified in the reason for denial. They must provide access to all other information in the designated record set.

Amendment:

A covered entity may deny a request for amendment if: (1) the entity did not create the PHI or record. However, if the individual provides a reasonable basis to believe that the creator of the PHI or record is not longer available to act on the request, then the covered entity must address the request as though they were the creator; (2) If the PHI is not part of the designated record set; and (3) if the information is determined to be accurate and complete.

In the event the covered entity denies a request for amendment, the denial must be in writing and include the basis of the denial, how the individual may file a written statement disagreeing with the denial, and how the individual may file a complaint with the entity and the Secretary. It must also state that if the individual chooses not to file a statement of disagreement, the individual may request that the covered entity include the request for amendment and denial of request with any future disclosures of the PHI that is the subject of the request. In the event the individual does file a disagreement, it may be reasonably limited in length and the entity may prepare a rebuttal with a copy to the individual.

If there is a written disagreement, the covered entity must identify the record or PHI that is the subject of the disputed amendment and append or link the following information to the designated record set: (1) Request for amendment, (2) denial of the request, (3) Individual's statement of disagreement and the covered entity's rebuttal. All of the appended or linked information, or an accurate summary, must be included with any subsequent disclosure of the PHI to which the disagreement relates. If the subsequent disclosure is a standard transaction that cannot accommodate the materials above, then they may be separately disclosed to the recipient of the transaction. If there is no written disagreement, then only if the individual requests it, must the entity include the appended or linked information.

If a covered entity accepts a request for amendment, they are required to identify the records in the designated record set that are affected and must append or otherwise provide a link to the location of the amendment. In addition the covered entity must obtain authorization to share the amended information. If the individual agrees, they must make reasonable efforts to provide a copy of the amendments to: (1) Persons or entities the individual names as needing the amendment; (2) Persons, including business associates that the covered entity knows may have relied on or could rely on the information to the detriment of the individual.

If a covered entity receives an amendment from another covered entity, then the covered entity must make the necessary amendment to PHI in the designated record set that it maintains. Covered entities must also require their business associates who receive amendments to incorporate those amendments to the designated record sets maintained on the covered entity's behalf.

Right to an Accounting of Disclosures:

Individuals have the right to request and receive an accounting of any disclosures made for purposes other than treatment, payment and health care operations for up to six years prior to the request for an accounting. Requests must be responded to within 60 days from receipt. If the covered entity is unable to respond in 60 days, they may one time only, extend the period by 30 days by providing a written explanation of the reasons for delay and stating the date in which the request will be fulfilled.

Individuals may receive one free accounting every 12-month period. Additional requests may be charged a reasonable, cost based fee. In the event a fee is charged, the individual must be given an opportunity to withdraw or revise their request.

For disclosures that are required to be in the accounting, the covered entity must retain documentation of the PHI required in the accounting and retain a copy of any accounting provided and document the titles of persons or offices responsible for receiving and processing requests for an accounting.

The accounting must contain:

1. Date of each disclosure.
2. Name and address, if known, of the person or organization receiving the PHI.
3. Brief description of the information disclosed.
4. The purpose for the disclosure – or a copy of the individual’s authorization or request for disclosure.

Note: Multiple disclosures of the same information, under the same authorization (or required by law) for the same purpose may be summarized.

Covered entities are not required to provide an accounting for:

1. Facility directories.
2. Persons involved in the individual’s care.
3. Disclosures allowed in the right to object or agree section.
4. National security or intelligence.
5. Correctional institutions or law enforcement officials.
6. Any disclosures made prior to the compliance date of the Privacy rule.

Covered entities must not provide an accounting for those to a health oversight agency or law enforcement official for the time period specified in the agency or law enforcement officials request for non-disclosure which states that an inclusion in the disclosures would reasonably be likely to impede the agency or official’s activities. The statement must state how long the information must be excluded. Oral statements are limited to a 30-day exclusion.

Public Responsibility – Use & Disclosure Not Requiring Consent, Authorization or Agreement

Individual authorization is not required to release PHI for disclosures mandated by law; public health activities; about victims of abuse, neglect or domestic violence; uses and disclosures for health oversight activities; disclosures for judicial and administrative proceedings; disclosures for law enforcement purposes; uses and disclosures about decedents; uses and disclosures for cadaveric donation of organs, eyes, or tissues; uses and disclosures for research purposes; uses and disclosures to avert a serious threat to health and safety; uses and disclosures for specialized government functions; and disclosures to comply with workers compensation; and disclosure for research purposes. Specific details of disclosures are as follows:

1. Summary Reports to Plan Sponsors: Health plans may provide summary reporting to their plan sponsors, even if it does not meet the definition of de-identified. However, such usage must be included in the covered entity’s notice of privacy practices.
2. Disclosures mandated by law: All covered entities may respond to disclosure requirements required by any law, provided the use or disclosure meets and is limited to the relevant requirements of such laws.

3. Public Health Activities: Allows disclosures to U.S. public health authorities and, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration. In addition, disclosures to FDA to report adverse events, product defects or problems, or biologic product deviations to enable recalls, repairs, or replacement, including locating and notifying individuals who have received those products, or to conduct post marketing surveillance.

Note 1: This is only if directed by the FDA or required by statute. Other agencies covered under this provision are OSHA, Federal Mine Safety and Health Act, Centers for Disease Control and Prevention, state and local public health departments for public health purposes. This may also include disclosure of PHI to persons who may have been exposed to communicable disease when the entity or public health authority is authorized by law to notify these individuals.

Note 2: Any health care providers who make disclosures to employers under this provision must provide notice to the individuals that it discloses PHI to employers related to the medical surveillance of the workplace and work-related illnesses and injuries. This notice is a separate from the notice of privacy practices as discussed above.

4. Communicable Disease: Allows disclosure to a person who may have been exposed to a communicable disease or may be at risk of contracting or spreading a disease or condition – provided that covered entity or public health authority is authorized by law to notify such person.
5. Employer: Allows disclosure to an employer about an individual who is a member of the workforce of the employer, if:
(1) The covered entity is a health care provider who is member of the workforce of such employer or who provides the health care at the request of the employer; to conduct an evaluation relating to medical surveillance or to evaluate whether the individual has a work-related illness or injury; (2) The PHI that is disclosed consists of findings concerning a work-related illness or injury or medical surveillance; (3) The employer needs such findings in order to comply with law requiring recording illness or injury or workplace medical surveillance; (4) The covered health care provider provides a written notice to the individual that PHI relating to the medical surveillance or work-related illness and injuries is disclosed to the employer.
6. Victims of Abuse, Neglect or Domestic Violence: Allows disclosure to public health authorities authorized to receive reports of child abuse or neglect.

In addition it allows - if expressly authorized by statute or law - disclosure to any governmental authority authorized by law to receive reports of abuse, neglect or domestic violence if required by law, and limited to the requirements of the law. Additionally, if the individual agrees to such disclosure, or the covered entity believes in its best judgment that disclosure is necessary to prevent serious harm - or – if the victim is incapacitated, if the law enforcement or other public official represents that the PHI disclosed is not intended to be used against the individual and that an immediate enforcement activity would be materially and adversely affected by waiting until the individual is able to agree.

Note: The covered entity must inform the individual of all disclosures to report abuse, neglect or domestic violence. Except – (1) If the covered entity believes that informing the individual would place them at risk of serious harm or (2) if the covered entity would be informing a personal representative and the covered entity reasonably believes that informing that person would not be in the individual's best interest.

7. Uses and Disclosures for Health Oversight Activities: This allows disclosure to an agency or authority of US, state, territory, political subdivision of state or territory, or Indian Tribe, that is authorized by law to oversee the health care system or government programs in which PHI is necessary to determine eligibility, compliance or to enforce civil rights laws for which health information is relevant. This includes agencies such as ADA, Civil Rights of Institutional Persons Act, EEOC civil rights enforcement, FDA, Public Health Service, US Dept. of Labor's Pension and Welfare Benefits Administration, etc. This includes disclosures for health care fraud investigations.

Note 1: This provision does not include private sector organizations such as accrediting organizations or coding committees that help government agencies.

Note 2: An investigation or activity is not considered oversight and is considered law enforcement if; (1) The individual is the subject of the investigation; (2) The investigation does not directly related to the receipt of health care or a claim/qualification for public benefits.

8. Judicial and Administrative Proceedings: PHI may be disclosed if the request is made pursuant to a court order, response to subpoena or discovery request from a party to the proceeding. If there is no subpoena or order from the court, the covered entity can only disclose if there are satisfactory assurances that reasonable efforts have been make to notify the individual OR the parties have made reasonable efforts to secure a protective order to guard the confidentiality.

Note: The minimum necessary requirements do not apply in the case of court order or order from administrative tribunal.

9. Law Enforcement Purposes: Covered entities may disclose PHI as limited by the relevant requirements of legal process or other law. This means responding to a warrant, subpoena or other order issued by a judicial officer; State, federal or grand jury subpoena; administrative request such as subpoena, summons civil investigative demand or similar process only if the information sought is relevant; the request is narrowly drawn and specific as reasonably practical; and de-identified information could not reasonably have been used.

Note 1: Information about suspects, fugitives, material witnesses, and missing persons may be disclosed for both cases in which law enforcement officials are seeking to identify and those cases in which they are trying to locate the individual. Only the following information may be disclosed; ABO blood type and Rh factor; date and time of death; scars, tattoos, height, weight, gender, race, hair, eye color and presence or absence of facial hair.

Note 2: Cannot disclose DNA data, dental records, or typing, samples or analyses of tissues or body fluids other than blood.

Note 3: Under this provision, a covered entity can only respond to a law enforcement request, which may be made orally

Note 4: Covered entities are allowed to initiate disclosure with law enforcement in the event the covered entity believes that it constitutes evidence of a crime committed on the premises.

Note 5: In the case of a medical emergency on the premises of the covered entity, the entity may disclose PHI if such disclosure is necessary to alert law enforcement to; (1) the commission of a crime and its nature, (2) the locations of the crime or victims, (3) identify description and location of the perpetrator.

Note 6: In the event the individual is a victim of a crime a covered entity may disclose PHI if; (1) the individual agrees to the disclosure or the covered entity is unable to obtain the individual's agreement due to an emergency circumstance. The law enforcement official must represent that such information is needed to determine whether a violation of law has occurred by someone other than the victim and such information is not intended to be used against the victim and that immediate law enforcement activity would be materially and adversely affected by a delay in receiving PHI.

Note 7: A covered entity may disclose PHI about an individual to a law enforcement official for the purpose of alerting law enforcement officials to the death of the individual - if the covered entity has a suspicion that the death may have resulted from criminal conduct.

Note 8: A covered entity may release PHI that a covered entity believes in good faith provides evidence of criminal conduct on the premises of the covered entity.

Note 9: If a covered health care provider giving emergency health care in a medical emergency, other than an emergency on the premises of the provider, may disclose PHI to a law enforcement official if such disclosure appears necessary to alert law enforcement to: (1) The commission and nature of a crime; (2) The location of the crime and the victims; and (3) The identity, description, and location of the perpetrator. In the event the covered entity believes the emergency is the result of abuse, neglect or domestic violence, then the disclosure falls under the control of 6 above – "Victims of Abuse, Neglect or Domestic Violence"

Note 10: For all actions taken in accordance with Notes 1 through 8, the covered health care provider must be responding to request from law enforcement officials, the provider cannot initiate the disclosure on their own initiative.

10. Disclosures About Decedents: Essentially, allows covered entities to disclose PHI information to funeral directors, consistent with applicable law, as necessary to carry out their duties, this include psychotherapy notes. This includes a public hospital with on-staff medical examiner functions.
11. Disclosures For Cadaveric Donation of Organs, Eyes, or Tissues: A covered entity may use or disclose PHI to organ procurement organizations or other entities engaged in the procurement of banking or transplantation of cadaveric organs, eyes, or tissue for the purpose of eye or tissue donation and transplantation.
12. Uses and Disclosures for Research Purposes: A covered entity may use or disclose PHI for research that an alteration to or waiver, in whole or in part, of the individual authorization has been approved by either; (1) an Institutional Review Board (IRB) established under the Common Rule or (2) A privacy board that has members with various backgrounds and professional competency necessary to review the effect of the research protocol on the individual's rights. In addition, the privacy board must include at least one member who is not affiliated with the covered entity or other interested entity and does not have any member participating in the review of any project in which the member has a conflict of interest. There are a number of other qualifications for the IRB and/or privacy board contained in the rule at 164.512(iii) – (iv) and (v).
13. Uses and Disclosures to Avert a Serious Threat to Health and Safety: A covered entity may, consistent with applicable law and standards of ethical conduct, use or disclose PHI, if the covered entity in good faith believe the use or disclosure: (1) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is to a person reasonably able to prevent or lessen the threat, including the target of the threat; or (2) is

necessary for law enforcement authorities to identify or apprehend an individual: (a) Because of a statement by and individual admitting participation in a violent crime that the covered entity believes may have caused serious physical harm to the victim; or (b) Where it appears that the individual has escaped from a correctional institution or from lawful custody.

Note 1: A use or disclosure is not permitted if information is learned by the covered entity is gained: (1) In the course of treatment to affect the propensity to commit the criminal conduct that would be the base for disclosure above, or from counseling or therapy; or (2) Through a request by the individual to initiate or be referred for the treatment, counseling or therapy.

Note 2: A disclosure made for this purpose shall contain only; ABO blood type and Rh factor; date and time of death; scars, tattoos, height, weight, gender, race, hair, eye color and presence or absence of facial hair.

14. US and Foreign Military Authorities: A covered entity may disclose the PHI of individuals who are US Armed Forces personnel or foreign military personnel for activities deemed necessary by the appropriate US or foreign military command authorities, if such US or foreign military authority has published notice in the Federal Register containing the appropriate command authorities and the purposes for which the protected health information may be used or disclosed.
15. Department of Veterans Affairs: A component of the Department of Veterans Affairs that is a covered entity may use or disclose PHI to components of the Department that determines eligibility benefits under the secretary of foreign affairs.
16. Protective Services for the President and Others: Covered entities may disclose PHI to authorized federal officials for the provision of protective services to the President and other persons, or to foreign heads of state or for the conduct of investigations.
17. National Security and Intelligence Activities. A covered entity may disclose protected health information to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act.
18. Medical Suitability Determinations: Covered entities that are components of the Department of State may use PHI to make medical suitability determinations and may disclose whether the individual was medically suitable to the officials of the Department of State for: (1) Conducting required security clearances, to determine worldwide availability for mandatory service abroad; or (3) for a family to accompany a Foreign Service member abroad.
19. Correctional Institutions and other Law Enforcement Custodial Situations: A covered entity may disclose to a correctional institution, correctional psychiatric institution or a law enforcement official having custody of an inmate or other individual if the law enforcement official represents that the PHI necessary for: (1) The provision of health care to such individuals; (2) The health and safety of such individual or other inmates; (3) The health and safety of the officers or employees of the correctional institution; (4) Law enforcement on the premises of the correctional institution; and (5) administration and maintenance of the safety, security, and good order of the correctional institution.
20. Government Programs Providing Public Benefits: A health plan that is a government program providing public benefits may disclose PHI relating to eligibility for enrollment in the health plan to another agency providing public

benefits if the sharing of eligibility or enrollment information in a single or combined data system is accessible to all such government entities is required or expressly authorized by statute or regulation.

21. Disclosures for Workers' Compensation: A covered entity may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs established by law, that provide benefits for work-related injuries or illness without regard to fault.

Administrative Requirements:

Privacy Officer: Covered entities must appoint a privacy official and privacy contract person for individuals to contact in regards to privacy practices, complaints and other issues. An organized health care arrangement or covered entities under common ownership and control who have designated themselves as a single affiliated entity and have agreed to produce a single notice, then together they may also have a single privacy official and/or privacy contact person.

Training: By the compliance date of the Privacy rule, each covered entity must provide privacy training to their entire workforce on the policies and procedures used to protect PHI as required by the rule. Training must be appropriate for the workforce members to which it is conducted. After the compliance date, all new members of the workforce must have this training. In the event a covered entity materially changes its privacy policies or procedures, then, within a reasonable time, all members of the workforce affected by those changes must be retrained. Policies and procedures must be implemented to both provide the training and document that the training has taken place. A formal education process and training in the organization's privacy policy and procedures must be provided for all members of the workforce and Business associates who have access to patient information.

Privacy Policy & Procedures: Privacy policies and procedures must be reasonably designed, developed and documented in writing to comply with requirements in the rule. This portion of the rule is also designed to be scalable and the policies and procedures should take into account the size and nature of the activities undertaken by the covered entity. All documentation must be retained for six years from the date the document was last in effect

There must be a process in place to accommodate revision of privacy policy and procedure, (promptly made to accommodate changes applicable laws or regulations), that ensure that any revisions of a covered entity's privacy practices are reflected in the revisions and that they comply with the rule and any applicable law, including revision of notices.

Internal Complaint Process: A covered entity must have a process for receiving individual complaints concerning violations of the covered entities privacy practices. While there is no requirement for responding to complaints, they must be documented and as a practical matter, covered entities would want to respond in order to resolve complaints before the individual complained to HHS.

Sanctions: There must be a method to measure workforce compliance to privacy policies and procedures and there must be written policy and procedures to apply appropriate sanctions for violation of those policies and procedures to the covered

entities workforce. The exception is that there can be no sanctions or retribution applied to a member of the work force for whistleblower activities or work force opposition to practices at the covered entity that may violate the rule.

Mitigation: There must be procedures in place to mitigate any harmful effect of use or disclosure of PHI that was a violation of the covered entities privacy practices, policies or procedures. This includes violations by both members of the workforce and business associates.

Whistleblower Provision: Covered entities are prohibited from taking any retaliation against any person who files a complaint, including individuals, members of the workforce or business associates. This provision also applies to persons who reasonably oppose a practice of the covered entity that they have a good faith belief that the practice is unlawful.

No Waiver of Rights: As a condition of treatment, payment, enrollment or eligibility, individuals may not be required to waive any of their rights pursuant to filing complaints with Secretary, or any other rights under this rule.

HIPAA SECURITY NPRM APPLICABILITY

The original DHHS Security NPRM covered only all electronic, patient-identifiable health data and called for a business process to protect source records. However, this will be clarified to expand this coverage to paper and oral records that are the source or progeny of electronic records. Like the Privacy rule, the Security NPRM is limited to any health care provider who transmits electronic data in any of the nine covered formats, payers and clearinghouses. However, as we discussed earlier, the Privacy rule's inclusion of the Business associate Agreement serves to expand the inclusion of the Security NPRM since security is mandated in the Privacy rule.

Certain Group Health Plans: Any group health plan that provides benefits only through an issuer of insurance or HMO and does not create, receive or maintain PHI (except summary information, enrollment and disenrollment information) is only subject to the requirements regarding documentation with respect to plan documents. They are exempt from the following administrative requirements: (1) Designation of a privacy official and contact person, (2) Workforce training, (3) Safeguards, (4) Complaints, (5) Mitigation and (6) Policies and procedures.

Transition Requirements: A covered entity may rely on a consent, authorization or other express legal document obtained from an individual prior to the compliance date that does not meet the requirements of consent or authorization provided the entity complies with all the limitations in such a document and it is consistent with the requirements in the rule. After the compliance date, consent and/or authorization must be obtained.

HIPAA SECURITY REGULATIONS

There are five major sections of the Security Regulations: Administrative Procedures; Physical Safeguards; Technical Security Services; Technical Security Mechanisms (for secure transmission over network); and Electronic Signature Standard.

1. *Administrative Procedures*

Over 75% of HIPAA Security compliance is operational in nature. The Security NPRM requires a security audit/assessment and risk analysis. Policy and procedure requirements include audit trail policy, certification, change control process, contract approval to include chain of trust language in trading partner agreements, human resources orientation and termination, information access privileges, workstation location, password and authentication policies and security incident procedures. Other administrative controls include contingency planning/disaster recovery (must be tested), a formal business process control, formal record processing, security configuration documentation and appointment of a security officer.

Employee and vendor education and training of security policy and procedures is also a requirement of the Security NPRM.

A few examples of policy and procedural issues that must be addressed are: (1) Policy assigning authorities to individuals assigned to authorize various levels of physical and access, (2) policy defining physical and data access levels based on roles, (3) formal employee security orientation, (4) Procedure for identifying and tracking employee access to applications, systems, data and physical areas and (5) Termination procedures that ensure recovery of tokens/card access, keys, changing of locks/combinations, removal of access to applications, data and systems.

2. *Physical Safeguards*

The issue with physical safeguards is the ability to protect the computers and the physical records. Each physical safeguard must be documented. Examples of physical safeguard requirements include: Facility management, physical access controls, computer room access, medical record access/tracking, shredding policy/procedure, card access systems, and a workstation location policy.

3. *Technical Security Services*

The technical component of the Security NPRM is designed to support or enforce the administrative policy and procedures. These methodologies should ensure the authentication of the user and restrict the user to only the systems, applications and data for which the user is authorized. Applying technical solutions without the policy and procedures provides little, if any, real protection. Technical security services deal with deployment of appropriate authentication methodologies supporting the authentication and access policies. This may be as simple as user id and password or include complex devices such as tokens, digital certificates, biometrics (e.g., fingerprint scanning), and proximity sensing devices. It may also include the integration of single-sign-on technology to help improve the productivity. Inappropriate access policy has the potential of creating negative patient outcomes if clinical personnel are inadvertently restricted from access patient records. An organization may want to deploy a “break the glass” type of access control that would give clinicians a special password, token or other device that would give them access to patient records in case of emergency while identifying the user, forcing an alarm and audit trail reporting.

Audit trails implemented in accordance with the audit trail policy to track user access is also part of the requirements. The granularity of the audit trails is established through policy and the enforcement and monitoring is established through implementation of system and/or application level audit trails and procedures for monitoring. It should also include automated exception reporting that complies with the established audit trail policies.

4. *Technical Security Mechanisms*

The Technical Security Mechanisms provision addresses protection of patient data from public networks. This typically deals with wide area network, remote access (dial-up), Intranet, Extranet and Internet access. Due to the proliferation of Internet security software and devices, this area, albeit complex, is probably the most straight forward to deploy technical defenses. This provision requires the appropriate deployment of communications/network controls, including Internet use monitoring, encryption, digital certificates, Virtual Private Networks (VPN), firewalls and virus protection.

Since encryption of dial-up remote access lines is included in the Security NPRM, it would behoove a covered entity to investigate replacing their dial-up lines with a VPN. Quite a bit of care needs to be taken in selection of the VPN. For example, if the remote access requirements include restricting a user to a particular application or server or the need to access through another site's firewall (user to firewall to firewall to application), most VPN software (including most VPN software that comes with popular firewalls) and public VPN services will not accommodate such uses.

This provision also mandates on-going threat, penetration and vulnerability audits. This may be accomplished through contracted third party ethical hackers or scanning software such as SATAN which automatically tries to penetrate firewalls and router protections.

HCFA has released an Internet Security Policy that details the level of encryption required and other authentication mechanisms needed to protect patient information when transmitted on the Internet. This essentially requires 112-bit asymmetric minimum. The complete policy is available from the HCFA web site at <http://www.hcfa.gov>. 128-bit SSL encryption is readily available from both Microsoft and Netscape as browser upgrades. PGP (Pretty Good Privacy) also makes an excellent encryption tool for encrypting both email and files for FTP transfers and is free for non-commercial use.

Entities must be very careful when deploying automated email patient appointment reminders and/or notification systems. Most of these applications come with 40-bit encryption as their default and must be specifically configured to test for and support the 128 bit browsers. Policies and procedures are of special concern with these systems as there must be methodology available to ensure authentication of the recipient. An email containing appointment or other health care information sent to a patient's email address is probably not secure enough since it could be anticipated that a patient could be sharing their computer with other family members who could have access to their email messages.

Additionally, systems that dial-up and leave messages for patients are also highly suspect and probably not compliant, since there is no methodology available to authenticate the recipient.

5. *Electronic Signatures*

As it currently stands in the NPRM, Electronic signatures are not required, however if an electronic signature is used (or required by DHHS in future), the electronic signature used must be a true digital signature (as opposed to a scanned signature) with properties that ensure message integrity, non-repudiation, and user authentication. However, it is reasonably clear that Electronic signatures are being removed from the final Security rule and may reappear in a later final rule. We do not expect digital signatures to be a requirement, especially since the final Privacy rule indicated that HHS did not intend to do anything contrary to the E-Sign law, which does not require digital signatures.

COMMON HEALTH CARE SECURITY ENVIRONMENT

Today's health care environment is typically 10-20 years behind other industries in regards to security. During the assessment process we typically find absent, weak, or outdated policies, lack of policy enforcement, procedures not documented/audited, insufficient education, inadequate disaster recovery (or more commonly not tested), servers and/or workstations lacking virus protection, weak audit trails and audit trail monitoring and Internet connections (telnet, ftp, http) lacking encryption, authentication and even firewalls. Even more common are shared IDs and/or passwords; weak passwords (length, aging, format); accounts not deleted, systems installed with vulnerabilities, access given to expedite business (inappropriate persons and inappropriate data).

The bottom line is that the vast majority of health care entities are going to have to make some changes to become compliant. Interestingly, as you will see, these changes may induce culture shock in most health care organizations. Largely, what is going to determine the success of any HIPAA compliance project is the ability of the organization to drive and control cultural changes through awareness and educations.

HIPAA SECURITY AND PRIVACY COMPLIANCE PROGRAM

Ok, where do we go from here? We know the impact and understand we probably have to do something. What is it we need to do? There are two basic categories of solutions: Organizational and/or operational approaches for security (75% of HIPAA Security compliance and 99% of HIPAA Privacy compliance is organizational in nature) and infrastructure and technical controls for security. What is important to understand now is that implementation of technical controls (e.g. encryption, VPN, audit trails, biometrics, firewalls, single sign-on, digital certificates, PKI, etc.) does not make an organization HIPAA Security Compliant. **Contrary to some vendor ads and promotions, there is no such thing as HIPAA Security compliant hardware or software. Technical controls and infrastructure are implemented only to enforce or support organizational policies and procedures.** Whether software or hardware is compliant to HIPAA Security regulations is completely dependent on how it is configured and implemented to support senior management policy decisions. It is common to find vendor software or hardware that could be successfully implemented to enforce and support Organization A's policies could not be used to enforce and support Organization B's policies.

The first step is to conduct a thorough security and privacy readiness assessment that examines all current policies and procedures and develops the current state of the organization. During this process, we must analyze affected business processes and understand senior management's goals and objectives. It is important to conduct key staff interviews to determine adherence to current policy. We have found that most policy and procedures that are ignored by staff are ignored because they are at cross purposes with the staff functions or are unworkable, impractical, or just do not have the funding to support their administration. A third party that is empowered to hold the staff responses confidential should ideally do these key staff interviews. Unfortunately, if the staff perceives that their responses will be used against them at some point; or think that their responses may offend someone the results will be invalid.

Secondly, we examine system and application security mechanisms to determine the current state of policy support and the technical controls available for each system and application. Once we know the current state of the organizational and technical components we can compare it on a detail basis to where we should be according to HIPAA. Then we can prepare a gap analysis that identifies and quantifies the deficiencies. Once the deficiencies are understood, we can develop a risk analysis that quantifies the risk associated with each deficiency and the costs and options associated with mitigating those risks.

We have included a detailed model of a HIPAA Security and Privacy project that is included as Exhibit A.

ORGANIZATIONAL APPROACH TO HIPAA SECURITY COMPLIANCE

After your organization has assessed its security risks and has developed the costs and options, you now have the information that senior management needs to make intelligent, informed decisions about the organization's level of security risk tolerance/acceptance. This should also be an educational process since senior management may not understand that the only secure data is data that cannot be accessed. Any access to data is accompanied by associated risk. In addition, since the investment to secure information is not linear, I would venture to say that most organizations do not have the funding to completely secure data and must make decisions on what is reasonable for their organization. For example, an organization may determine that it is not reasonable for them to spend \$1.5M to shield their building in order to defend against someone parking a van full of high tech electronics in front of their building, capturing all of their keystrokes and through the use of sophisticated software assembling the keystrokes into meaningful data. On the other hand, they may determine that it is reasonable to invest \$200,000 implementing a single sign-on solution with proximity devices that increases the security of the nurses and other clinical workstations without affecting their productivity. One of the good things about HIPAA is that it allows an organization to make risk decisions and set its own level of remediation, as long as those decisions are reasonable and well documented. Therefore, these decisions must be made on an informed basis and must be documented.

For the changes that will be required to comply with HIPAA Security and Privacy regulations to be successful, most organization will need to induce a change in the organizational culture. In order for security and privacy policies and procedures to take hold and become part of the organizational culture, they must be totally integrated into the organization,

starting from the senior management. Developing and deploying great policies and procedures that are subsequently ignored does not accomplish the goal. Since HIPAA Security and Privacy rules reach out to every nook and cranny of every department in the organization, each department must participate in the development, education and deployment. This would normally include establishing a Security Committee, with organization-wide representation (Senior Management, clinical, legal, IT/IS, HR, audit and records staff). Ideally, the Committee should report directly to the board, and should be given policy authority. The first item on the agenda of the Security Committee is to work with senior management to develop an overall corporate security strategy and privacy policy.

It is important that once the corporate security strategy has been decided, that adequate budget be approved for the remediation and implementation phases.

Next, a security and privacy awareness education and training program needs to be developed and implemented. This formal training program is for all staff members, and should be consistent, measurable and continued on an ongoing basis to keep awareness heightened, (e.g., monthly newsletters via memo or e-mail).

Interestingly, since compliance to HIPAA Security and Privacy regulations impacts business process, we have an opportunity for the changes that will be invoked to be a catalyst to also improve our business processes and yield an overall improvement in efficiency. Unlike the money we spent on Y2K, the investment in complying with HIPAA Security and Privacy rules can yield a return on our investment.

DEVELOPING HIPAA COMPLIANT POLICIES AND PROCEDURES

Once senior management has made the tough risk decisions and approved an overall corporate security and privacy policy the work begins on development of specific policies and procedures that must remediate the weaknesses found in the assessment and represent Senior Management's goals and reflect associated acceptance of risk. They must be clear and consistent throughout the organization. There needs to be a feedback process in place to measure their effectiveness and employee compliance. Enforcement must be consistent and equal, and they must integrate with OIG compliance policies.

HIPAA SECURITY COMPLIANCE CERTIFICATION

HIPAA Security NPRM mandates that a covered entity be certified as compliant. Third-party certification is not required, but is highly recommended. Organizations can self-certify, or can utilize associations such as EHNAC (clearinghouse, provider and hospital organizations) or NCQA (payer organizations) that are currently in the process of developing certification programs. Unfortunately, JCAHO has stated that they will note any security deficiencies that they find during an audit, but passing a JCAHO audit will not certify compliance to HIPAA Security rules.

If an entity determines that it will self certify, the process that they developed for Y2K certification can probably be modified to fit a HIPAA Security self-certification. However, it will probably not hold the same weight in a courtroom as a third party certification. There has been legal opinion that certification of compliance to HIPAA security will go a long

way to help an organization prove that it was reasonably and diligently applying security protections that are consistent with those found in the industry. Having a HIPAA Security certification is a lot better than having a jury that has been raised on X-Files and Star Wars applying what they may believe are reasonable and diligent protections. Without this certification, one could imagine a jury finding that it is reasonable for a hospital to provide the same level of security protections for patient data as a government defense contractor would apply to the secrets associated with a missile contract.

Since covered entities will be held responsible for their business associates' actions, it is important that we ensure that our business associates also comply with HIPAA Security rules through either third parties or self-certification. Again, this process can follow the same methodology that we used to ensure our business associates Y2K compliance.

RESOURCES

For additional information on HIPAA, visit the following Web sites:

- HIPAAComply.com - www.hipaacomply.com
- WEDI (Work Group for Electronic Data Interchange) - www.wedi.org
- AFEHCT (Association For Electronic Health Transactions) - www.afehct.org
- EHNAC (Electronic Health Network Accreditation Commission) - www.ehnac.org
- For the record, national research council (chapter 6) www.Nap.Edu/readingroom
- DHHS Administrative Simplification - aspe.os.dhhs.gov/admsimp/index.htm
- DHHS Data Council - aspe.os.dhhs.gov/datacncl/
- NCVHS - aspe.os.dhhs.gov/ncvhs

AUTHOR BIO

Tom Hanks has 20 years of information systems, management consulting and network experience with the last eight years focusing on health care, including co-founding a successful EDI clearinghouse. He is recognized as an authority on HIPAA security and standards legislation, has contributed to the development of HIPAA security and standards regulations and is active on several industry security and standards workgroups. Mr. Hanks is currently a board member of WEDI (Workgroup on Electronic Data Interchange), Co-chair of the WEDI Privacy Policy Action Group, VPN Group Leader for WEDI/AFEHCT/HCFA Internet Interoperability Pilot and co-chair of the HIPAA Summit Monitoring Committee. Mr. Hanks is also a Commissioner for the Electronic Health Network Accreditation Commission (EHNAC) and he is chair of the HIPAA Security Certification Criteria Committee. He also has served as a board member of the Association for Electronic Health Care Transactions (AFEHCT) and is currently active in AFHECT Security, Privacy and Administrative Simplification Workgroups.