AmeriCares

NAFC The National Association of Free & Charitable Clinics

Guide to HIPAA for Covered Entities

Free & Charitable Clinic HIPAA Toolbox

May 2014

Following is a HIPPA Guide prepared by Ropes & Gray, a law firm focusing on healthcare, on behalf of AmeriCares and the National Association of Free and Charitable Clinics. The HIPAA Guide summarizes current HIPAA Privacy, Security, Data Breach Notification, and Enforcement Rule requirements regarding common situations relevant to Covered Entities. The Guide is intended to provide an overview of a Covered Entity's obligations; however, it is not a substitute for the development and implementation of Covered Entity-specific policies and procedures.

The Toolbox is directly applicable to healthcare providers that are considered "Covered Entities" under HIPAA; however other providers may choose to comply with certain HIPAA principles in order to meet patients' general expectations about the privacy of their health information. The Toolbox does not address any privacy or security obligations imposed by state law or by payors. Particular provider-specific questions or situations (such as a potential "breach" of health information) should be addressed with counsel.

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") regulates how certain healthcare providers, health insurers, and other entities, collectively known as "Covered Entities," and certain of their subcontractors, referred to as "Business Associates," use, disclose, and protect patients' healthcare information. HIPAA is designed to enhance and standardize the patient privacy protections afforded by many existing state laws.

With respect to privacy and security, HIPAA regulations are divided into four "Rules" – the Privacy Rule, the Security Rule, the Breach Notification Rule, and the Enforcement Rule. The Privacy Rule describes individuals' rights to their health information and under what circumstances health information may be used or disclosed by a "Covered Entity." The Security Rule describes the policies and procedures that Covered Entities and their Business Associates must have in place in order to safeguard electronic protected health information. Rather than prescribing the exact type of electronic systems required, the Security Rule gives Covered Entities and Business Associates guidelines for developing scalable, appropriate data security measures. The Breach Notification Rule creates procedures and timelines for the notification of individuals whose health information may have been compromised. Finally, the Enforcement Rule sets forth penalties for non-compliance with HIPAA regulations, as administered by the Department of Health and Human Services Office for Civil Rights ("HHS OCR" or "OCR") and the Department of Justice ("DOJ").

This Guide is intended to describe and summarize the basic requirements of each of the HIPAA Rules, but is not intended to be a substitute for informed legal advice. This Guide also does not cover state or local laws or regulations that may have an impact on a Covered Entity's implementation of its HIPAA policies and procedures.

II. APPLICABILITY

HIPAA's regulations apply to the subset of health information defined as "protected health information" or PHI. PHI is information created or received by a Covered Entity that relates to the past, present, or future physical or mental health of the individual, the provision of healthcare to an individual, or the past, present or future payment for healthcare provided to the individual that either identifies the individual or could identify the individual. Education records, certain student health records, employment records, and information regarding an individual that has been deceased for more than fifty years are excluded from the definition of PHI.

HIPAA's restrictions on the uses and disclosures of PHI apply to Covered Entities and their Business Associates. A Covered Entity is a healthcare provider, health plan, or a provider of data processing services (also known as a healthcare clearinghouse) that transmits any health information in electronic form for the following purposes: claims and encounter information, payment and remittance advices, claims status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits, and premium payment. Covered Entities must comply with all of HIPAA's regulations. This Guide focuses on the provisions of HIPAA that apply to most Covered Entities that are healthcare providers, and not on provisions that solely relate to health insurers or healthcare clearinghouses. Please see Exhibit A for a flowchart for determining whether an individual or entity is a Covered Entity healthcare provider.

By contrast, a Business Associate is an entity that creates, receives, maintains, or transmits PHI for a function or activity by the Covered Entity. Examples of Business Associate activities include claims processing, data analysis, utilization review, quality assurance, patient safety activities, billing, benefit management, and repricing, or the performance of legal, actuarial, consulting, data aggregation, management, administrative, accreditation, or financial services to or for a Covered Entity, if the activity involves the disclosure of PHI. Business Associates must comply with all of the Security and Breach Notification Rules, as well as a limited portion of the Privacy Rule. They are also subject to the Enforcement Rule. A Covered Entity must have a written agreement, as discussed below, that describes the services that the Business Associate will perform on behalf of the Covered Entity, as well as the Business Associate's duties to protect the PHI and report breaches. In some instances, a Covered Entity may act as a Business Associate on behalf of another Covered Entity.

III. THE PRIVACY RULE

The HIPAA Privacy Rule establishes national standards for patients' rights to understand, access, and control the use of their health information as well as administrative requirements for Covered Entities to use and disclose their patients' PHI. The Privacy Rule attempts to balance the need for health information to flow through the healthcare system with patients' privacy expectations.

a. Patient Rights

The HIPAA Privacy Rule creates a uniform set of patients' rights to access, restrict, and amend their PHI. Covered Entities must have policies and procedures in place to facilitate patients' exercise of their rights under HIPAA. Non-compliance with HIPAA's patient rights provisions – such as a refusal to allow a patient with an unpaid bill access to their medical records – is considered a violation of HIPAA and is subject to the same types of enforcement actions and penalties as an unauthorized use or disclosure of PHI.

i. Notice of Privacy Practices

As part of HIPAA's patient rights provisions, a Covered Entity must provide each patient with a Notice of Privacy Practices ("NPP") that describes the uses and disclosures of PHI that may be made by the Covered Entity, as well as the Covered Entity's legal duties, such as the duty to protect PHI.[1] A Covered Entity must revise and distribute its NPP whenever there is a material change to its uses and disclosures, the individual's rights, the Covered Entity's legal duties, or other privacy practices stated in the notice.

A Covered Entity must provide the NPP no later than the date of the first service delivery, including service delivered electronically, or as soon as possible after an emergency treatment situation. A Covered Entity must make a good faith effort to obtain a written acknowledgement of receipt of the NPP, and if not obtained, the Covered Entity must document its efforts to obtain the acknowledgement and the reason why the acknowledgement was not obtained. The Privacy Rule sets forth the following parameters for the provision of NPPs to patients:

- An NPP may be provided by e-mail if the individual agrees to electronic notice and the notice has not been withdrawn. The individual will retain the right to obtain a paper copy upon request.

- The NPP must be provided to individuals upon request at the locations where the Covered Entity provides healthcare services. The NPP must also be posted in a clear and prominent location – such as a waiting room – where it is reasonable to expect individuals seeking service from the Covered Entity to be able to read the notice.

[1] The specific elements that must be set forth in the NPP are provided in the HIPAA Privacy Rule at 45 C.F.R. § 164.520.

- If the Covered Entity maintains a website, it must prominently post a link to the NPP on the web site and make the notice available for download through the web site.

ii. Authorizations

A Covered Entity must obtain a signed authorization from the individual for any use or disclosure of PHI that is not described in the NPP or otherwise permitted under HIPAA. The authorization must be written in plain language and include a meaningful and useful description of the PHI to be used or disclosed. The authorization must also specifically identify the person or class of person(s) authorized to make the disclosure; describe each purpose of the use or disclosure; and provide an expiration date for the authorization.

The authorization must include a statement regarding the individual's right to revoke in writing and contain a notice that the Covered Entity may not condition treatment on the authorization. However, treatment pursuant to a research protocol may be conditioned on receipt of an authorization to use or disclose the PHI for purposes of the research study. If the Covered Entity is seeking an authorization to use or disclose PHI for marketing purposes, the authorization must state that the Covered Entity will receive remuneration, if applicable. For all authorizations, an individual has the right to receive a signed copy from the Covered Entity. If an individual notifies a Covered Entity that the individual is revoking their authorization, the Covered Entity must cease using or disclosing the PHI for the purpose described in the authorization.

iii. Access to Protected Health Information

An individual also has the right to inspect, review and obtain a copy of the PHI that is maintained by the Covered Entity and used, in whole or in part, to make decisions about the care of an individual, and medical and billing records about the individual, which is known as the "Designated Record Set." However, psychotherapy notes and information compiled in reasonable anticipation of litigation are exempt from this requirement.[2]

A Covered Entity may deny access to PHI in the Designated Record Set that would otherwise be required under the Privacy Rule if a Covered Entity believes that access could cause harm to the individual or to another person. The Covered Entity must permit the denial to be reviewed by a licensed healthcare professional designated by the Covered Entity who did not participate in the original decision to deny access. A Covered Entity may also deny access to PHI related to ongoing research to which the individual previously consented or if the PHI was obtained by the Covered Entity from someone other than a healthcare provider under a promise of confidentiality. These types of denials are not reviewable. For all denials, the

[2] Under HIPAA's current regulations, individuals do not have the right to access their PHI directly from CLIA and some CLIA-exempt laboratories, but may access their laboratory results through the ordering provider. In 2011, HHS proposed ending this exemption in order to facilitate the implementation of personalized medicine and personal health records. See 78 Fed. Reg. 56712 (Sept. 14, 2011). Final regulations on this proposal are expected in the near future.

Covered Entity must provide a written statement of the denial, the reasons for the denial, and the individual's right to have the denial reviewed, if applicable.

An individual may direct a Covered Entity to transmit the PHI requested directly to another person designated by the individual. A request to transmit information to another individual must be made in writing, signed by the individual, and clearly identify the designated person to receive the PHI.

A Covered Entity must act on a request for access no later than thirty days after the request is received, unless the information is not readily accessible, in which case the Covered Entity has sixty days to respond. In certain circumstances, a Covered Entity may receive a one-time, thirty day extension.

If the individual is granted access, the Covered Entity may impose a reasonable, cost-based fee for labor, supplies, postage, or for preparing a summary of the PHI, if agreed to by the individual.

iv. Accounting of Disclosures

An individual has the right to receive an accounting of disclosures of PHI made by the Covered Entity for the six years prior to the date of the request for an accounting.

The accounting is <u>not</u> required to include disclosures:

- To carry out treatment, payment, or healthcare operations;
- To individuals pursuant to a request for access;
- For inclusion in the Covered Entity's patient directory;
- To persons involved with the individual's care or for other notification purposes;
- For national security or intelligence purposes; or
- To correctional institutions or law enforcement officials.

A Covered Entity must act on a request for an accounting within sixty days, but may receive a one-time, thirty-day extension of time to provide the accounting so long as the Covered Entity provides the individual with an explanation of the delay within sixty days of the request.

The written accounting must include all disclosures for the six year period, including disclosures by any Business Associate of the Covered Entity. For each disclosure, the Covered Entity must provide the date of disclosure, the name of the entity or person who received the PHI, and if known, the address of such entity or person, a brief description of the PHI disclosed, and a brief statement of the purpose of the disclosure. In some instances a Covered Entity may

consolidate information about multiple disclosures made to the same individual or entity for the same purpose.

An individual is entitled to one free accounting in any 12-month period. A Covered Entity may charge a reasonable, cost-based fee for subsequent requests during any 12-month period.

v. Correction or Amendment of PHI

An individual has the right to request that the Covered Entity amend PHI contained in the Designated Record Set. A Covered Entity may require individuals to request an amendment in writing and to provide a reason to support a requested amendment, provided that the individual is informed in advance of such requirements.

A Covered Entity must act upon a request for amendment no later than sixty days after receipt of such a request. If the Covered Entity is unable to act on the amendment within the sixty day requirement, the Covered Entity may have a one-time, thirty-day extension of time to respond, provided that the Covered Entity notifies the individual of the reason for the delay within the initial sixty-day window.

If the Covered Entity agrees to the amendment, the Covered Entity must make the appropriate amendment by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and appending or otherwise providing a link to the location of the amendment. The Covered Entity must inform the individual within the appropriate timeframe that the amendment is accepted and receive information from the individual regarding appropriate persons with whom the amendment should be shared.

A Covered Entity may deny a request for an amendment in certain circumstances specified in the Privacy Rule. If a Covered Entity denies a request for an amendment, it must provide the individual with a timely written denial that uses plain language and contains the basis for the denial, the individual's right to submit a written statement disagreeing with the denial, and information regarding the individual's ability to appeal the denial or complain to the Covered Entity about the denial.

If the individual disagrees with the Covered Entity's denial, the Covered Entity must permit the individual to submit a written statement disagreeing with the denial. The Covered Entity must include: 1) the individual's request for an amendment, 2) the Covered Entity's denial of the request, 3) the individual's statement of disagreement, if any, and 4) the Covered Entity's rebuttal statement, if any, in the Designated Record Set. The statement of disagreement must be appended to any subsequent disclosures of the PHI at issue.

vi. Additional Individual Rights

A Covered Entity may not disclose patient PHI to the patient's health insurer for purposes of seeking payment or for healthcare operations if the patient, or someone else on

behalf of the patient (other than the patient's health insurer), pays in full for the healthcare item or service. If a Covered Entity is required to submit claims, and payment for services out of pocket is not possible, the Covered Entity must deny the request. A Covered Entity must also counsel an individual requesting such a restriction on the need to restrict additional restrictions on disclosures for follow up services and on the possibility of automated disclosures, such as e-prescribing and laboratory services. However, the individual bears the burden of paying in full and requesting restrictions from other ancillary providers.

A Covered Entity may, but is not required to, agree to comply with additional reasonable requests for restrictions on uses and disclosures of an individual's PHI. If a Covered Entity agrees to an additional restriction, the Covered Entity may not use or disclose PHI in violation of the restriction except in an emergency situation. If a Covered Entity agrees to a restriction, the restriction must be documented. A restriction, except for information regarding healthcare items or services paid in full by the individual, may later be terminated if the individual agrees to the termination in writing, or if the individual agrees orally and the oral agreement is documented. A Covered Entity may also unilaterally terminate a restriction, but only with regard to PHI obtained by the covered entity after the termination of the restriction.

b. Administrative Requirements

A Covered Entity must develop reasonable written policies and procedures that are designed to comply with HIPAA. A Covered Entity must promptly change its policies and procedures as necessary and appropriate to comply with changes in state and federal law and regulations. If a change to a policy or procedure will materially impact the Covered Entity's NPP, the Covered Entity must revise the NPP and distribute the revised NPP to its patients. Policies and procedures required under HIPAA must be maintained by the Covered Entity in written or electronic form for at least six years.

For accountings of disclosures, requests for access, and requests for amendment of PHI, a Covered Entity must retain the documentation of the request and the Covered Entity's response for six years. The Covered Entity must also document the person or office to whom such requests should be directed. A Covered Entity must also retain copies of its NPP, acknowledgements of receipt of the NPP, or documentation of attempts to obtain such an acknowledgement, for six years.

A Covered Entity must also designate a Privacy Official who is responsible for the development of the Covered Entity's HIPAA policies and procedure. The Privacy Official should be well versed in applicable federal and state privacy laws and have sufficient standing within the Covered Entity's organizational structure to ensure that policies and procedures are implemented appropriately. The Privacy Official's chief responsibilities should include the development of policies and procedures necessary for HIPAA compliance, in coordination with the Covered Entity's management and administration, privacy committee, and legal counsel. The Privacy Official should perform initial and periodic privacy risk assessments. The Privacy Official should also implement mechanisms to track access to PHI, and ensure the Covered Entity allows patients to inspect, amend, and restrict access to PHI when appropriate.

i. Compliance with the Minimum Necessary Standard

HIPAA requires Covered Entities to make reasonable efforts to limit uses, disclosures or requests for PHI to that which are reasonably necessary to accomplish the purpose for which the requests or disclosures are being made. The minimum necessary requirement does not apply to requests or disclosures to or from a provider for treatment purposes, to the individual, or to HHS in response to a request for information.

In order to comply with the minimum necessary standard, a Covered Entity must identify the persons or classes of persons in its workforce that need access PHI to carry out their duties. For each person or class of persons, a Covered Entity should identify the category or categories of PHI to which access is needed and any conditions appropriate to such access.

For routine or recurring disclosures, a Covered Entity must implement policies and procedures that limit the PHI disclosed to the amount necessary to accomplish the purpose of the disclosure. For non-routine disclosures, a Covered Entity must develop criteria designed to limit the PHI disclosed to the information reasonably necessary and review requests for disclosure on an individual basis to ensure compliance with HIPAA. A Covered Entity is entitled to rely on reasonable requests from public officials, other Covered Entities, workforce members of the Covered Entity, and the Covered Entity's Business Associates for PHI as satisfying the "minimum necessary" standard.

A Covered Entity may not use or disclose an individual's entire medical record, except when the entire record is specifically justified as the amount needed to accomplish the use, disclosure or request.

ii. De-identified Data Sets

A Covered Entity may disclose data if there is no reasonable basis to believe that it can be used to identify an individual. A Covered Entity may only determine that data is no longer individually identifiable (and thus not PHI subject to HIPAA) if:

1. A statistician determines that the risk of re-identification is very small, or

2. The following identifiers of the individual, or of relatives, employers or household members of the individual, are removed:

   a) Names

   b) All geographic subdivisions smaller than a State, except for the three initial digits of a zip code if the combination of all zip codes with the same three digits results in more than 20,000 people

   c) All elements of dates related to the individual, including birth date, admission date, discharge date, date of death, and all ages

over 89 and all elements of dates including year indicative of such date

d) Telephone numbers

e) Fax numbers

f) Email addresses

g) Social security numbers

h) Medical record numbers

i) Health plan beneficiary numbers

j) Account numbers

k) Certificate/license numbers

l) Vehicle identifiers and serial numbers, including license plate numbers

m) Device identifiers and serial numbers

n) Web Universal Resource Locators (URLs)

o) Internet Protocol (IP) address numbers

p) Biometric identifiers, including finger and voice prints

q) Full face photographic images and any comparable images, and

r) Any other unique identifying number, characteristic, or code, except for a record identification code that is not derived from or related to information about the individual, and the code is not disclosed

iii. Limited Data Sets

A Limited Data Set is still PHI, but it must exclude all of the elements listed above <u>other than</u> town or city, state, and zip code; elements of dates; and other unique identifying numbers, characteristics, and codes. A Limited Data Set may be disclosed only for research, public health, or healthcare operations purposes, and only pursuant to a written Data Use Agreement with the recipient. The Data Use Agreement must establish the permitted uses and users of the Limited Data Set and require the recipient to safeguard the PHI, report unauthorized uses or disclosures to the Covered Entity, and not attempt to identify the PHI or contact the individuals described in the Limited Data Set.

iv. Disclosures to Business Associates

Covered Entities often contract with Business Associates in order to perform healthcare activities and functions involving PHI held by a Covered Entity. Examples of Business Associates include a CPA firm that provides the Covered Entity with accounting services, an attorney that requires access to PHI to provide legal services, a consultant performing utilization reviews, or an independent medical transcriptionist providing transcription services to a physician.

A Covered Entity must obtain assurances that a Business Associate will safeguard the PHI from misuse, and will assist the Covered Entity with the Covered Entity's duties to provide individuals with access to their PHI, amendment of their PHI (to the extent the Business Associate possesses an individual's designated record set) and an accounting of disclosures of their PHI. These assurances must be documented in a Business Associate Agreement ("BAA"), with terms specified in the Privacy Rule and signed by both parties. A Covered Entity's legal counsel should determine whether a BAA is required for a specific relationship between a Covered Entity and a third party.

Additionally, the Covered Entity's Privacy Official, or designated legal counsel, should review all agreements with Business Associates to ensure that the BAA meets HIPAA's requirements before PHI is disclosed to a Business Associate. Business Associates are subject to the Security, Enforcement, and Breach Notification Rules of HIPAA, as well as a limited portion of the Privacy Rule.

v. Workforce Training and Sanctions

A Covered Entity must train all of its workforce members on its HIPAA policies and procedures as necessary and appropriate for each workforce member to carry out their responsibilities. The Privacy Official should ensure that workforce members receive initial HIPAA training upon starting and periodic refresher training thereafter. Covered Entities must document the training provided to workforce members, which must occur within a reasonable period of time after the person joins the Covered Entity's workforce and upon significant changes in either the Covered Entity's policies or procedures or in the HIPAA regulations. A Covered Entity must have and initiate appropriate sanctions against workforce members that violate the Covered Entity's HIPAA policies and procedures.

c. <u>Uses or Disclosures of PHI</u>

A Covered Entity may only use or disclose PHI as expressly permitted by the Privacy Rule, with an individual's prior written authorization, or, in some circumstances, without authorization so long as the individual has an opportunity to agree or object.

i. Uses or Disclosures for Treatment, Payment, or Healthcare Operations

Disclosures of PHI to an individual, for purposes of Treatment, Payment, or Healthcare Operations of the Covered Entity do not require prior authorization. All uses or disclosures of

PHI for Treatment, Payment, and Healthcare Operations must comply with the Covered Entity's NPP and the Minimum Necessary requirement.

"Treatment" is the provision, coordination, or management of healthcare and related services by one or more healthcare provider, including the coordination or management of healthcare by a healthcare provider with a third party, consultations between healthcare providers, and referrals from one healthcare provider to another.

"Payment" is obtaining reimbursement for the provision of healthcare, including billing, claims management, and collection activities, precertification and preauthorization of services, and disclosures of personal information (name, address, DOB, SSN, payment history, account number, and provider address) to consumer protection agencies.

"Healthcare Operations" includes quality assessment and improvement activities, patient safety activities, population-based activities relating to improving health or reducing healthcare costs, protocol development, case management and care coordination, contacting patients with information about treatment alternatives, reviewing competence or qualifications of healthcare professionals, evaluating provider performance, conducting training programs, accreditation/certification/licensing/credentialing, medical review, legal services, auditing (including compliance programs), cost management, and business management.

In addition to disclosures for Treatment, Payment, and Healthcare Operations purposes of the Covered Entity, a Covered Entity may disclose PHI to another healthcare provider for treatment purposes of the healthcare provider (such as a referral to a specialist), to another healthcare provider or Covered Entity for payment activities of the other entity, and to another Covered Entity for that Covered Entity's Healthcare Operations, but only to the extent that each Covered Entity has or has had a relationship with the individual, the PHI pertains to such relationship, and the purpose of the disclosure is to engage in risk management or quality improvement activities, or for the purpose of healthcare fraud and abuse detection or compliance.

ii. Uses or Disclosures Required by Law, for Public Health Purposes, or for Research Purposes

A Covered Entity may disclose PHI for purposes required by law, such as disclosures regarding victims of abuse, disclosures for judicial and administrative proceedings, and disclosure for law enforcement purposes. For example, a Covered Entity may disclose PHI in order to avert a serious threat to public safety, to allow law enforcement officials to apprehend a criminal suspect or escaped convict, or to federal officials for intelligence purposes or to the Secret Service to investigate threats to the president, vice-president, or their immediate family members. All such uses and disclosures must be consistent with the Covered Entity's NPP and are subject to restrictions on the amount of PHI disclosed and the circumstances under which a disclosure would be appropriate.

A Covered Entity may also disclose PHI without prior authorization to (1) a public health authority for the conduct of public health surveillance, public health investigations, and public health interventions; (2) a person who may have been exposed to a communicable disease or who is at risk of contracting or spreading a disease or condition, if the Covered Entity or public health authority is authorized by law to notify the individual; and (3) for research purposes where a researcher has received a valid, documented waiver of authorization from an Institutional Review Board or a Privacy Board, if the PHI is necessary for a review preparatory to research and no PHI will be removed from the Covered Entity, or if a researcher demonstrates that the research will solely be performed on the PHI of decedents and that access to the PHI is necessary to perform the research.

iii. Incidental Uses and Disclosures

Incidental uses and disclosures are secondary uses or disclosures of PHI that cannot reasonably be prevented, are limited in scope, and that occur as a result of another use or disclosure that is permitted under HIPAA. For example, an incidental disclosure could occur when a hospital visitor overhears a patient's name being called in a waiting area, or sees a patient's name may be displayed on a whiteboard at a nursing station.

A Covered Entity must have reasonable safeguards in place to minimize the potential for incidental uses or disclosures to occur. Examples of reasonable safeguards include avoiding discussing patient information in public spaces, posting signs to remind workforce members of the need to protect patient confidentiality, or isolating or locking file cabinets or records rooms.

iv. Disclosures Requiring an Opportunity to Agree or Object

A Covered Entity may use or disclose an individual's PHI for healthcare facility directories, for the involvement of another person in the individual's healthcare, for disaster relief purposes, or for fundraising purposes without prior authorization so long as the individual is given an opportunity to agree or object.

1. Facility Directories

For a facility directory, a Covered Entity may use the individual's name, location within the facility, a general description of the individual's condition, and the individual's religious affiliation to communicate with members of the clergy and with other persons who ask for the individual by name as long as the individual is notified and provided with the opportunity to opt out. If the individual is unavailable, the Covered Entity may disclose some or all of the permitted information so long as such disclosure is consistent with the individual's prior expressed preference, if any, and with the individual's best interest.

2. Involvement in Care and Notification Purposes

A Covered Entity may disclose PHI to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, as long as the PHI disclosed is relevant to the recipient's involvement in the care or in the payment for the care.

If the individual is present and has the capacity to make healthcare decisions, the Covered Entity must either obtain the individual's agreement to disclose the PHI, and provide the individual with an opportunity to object to the disclosure, or reasonably infer from the circumstances that the individual would not object to the disclosure. If the individual is not present, or is not otherwise able to agree or object, the Covered Entity should disclose only the PHI that is directly relevant to the person's involvement with the individual's care or for payment related to the individual's healthcare or needed for notification purposes.

A Covered Entity may also disclose PHI to notify, or to assist in the notification of a family member, a personal representative of the individual, or another person responsible for the individual the individual's location, general condition, or death. If the individual is deceased, a Covered Entity may disclose to a family member, or other person listed above who were involved in the individual's care or payments for healthcare prior to the individual's death, PHI of the individual that is relevant to the person's involvement, except if doing so would be inconsistent with any prior expressed preference of the decedent known to the Covered Entity.

3. Disaster Relief Purposes

A Covered Entity may disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating permitted notifications. A Covered Entity should exercise its professional judgment in determining whether attempting to obtain authorization from the individual would interfere with the ability to respond to the emergency circumstances.

4. Fundraising Communications

A Covered Entity may use or disclose an individual's PHI to a Business Associate or to the Covered Entity's institutionally-related foundation if the Covered Entity describes its fundraising practices in the NPP and the individual is provided a clear and conspicuous opportunity in the fundraising communication to opt out at no additional cost to the individual. Examples of acceptable opt-out methods include a toll-free number, a prepaid postcard, or an email address. A Covered Entity may not condition treatment on an individual's decision to receive fundraising communications.

v. Required Disclosures

A Covered Entity is <u>required</u> to disclose PHI to individuals at their request. A Covered Entity is also required to disclose PHI to the Secretary of HHS upon request.

vi. Disclosures Requiring Prior Authorization

Unless a use or disclosure is otherwise permitted under HIPAA, a Covered Entity may not use or disclose PHI without a valid authorization. In particular, a Covered Entity must obtain a valid authorization for any use or disclosure of psychotherapy notes (except for disclosures for treatment, payment, or healthcare operations), for marketing purposes (except for face-to-face communications by the Covered Entity to the individual or promotional gifts of nominal value provided by the Covered Entity to the individual), and for the sale of PHI. For marketing purposes and for the sale of PHI, the authorization must state that the disclosure will result in remuneration to the Covered Entity, if applicable.

IV. THE SECURITY RULE

The Security Rule provides guidelines for Covered Entities and their Business Associates to develop and implement policies and procedures to protect PHI that is transmitted or maintained in electronic media, known as "ePHI." The Security Rule describes requirements for appropriate administrative, technical, and physical safeguards to protect the privacy of ePHI, but does not mandate specific technologies, infrastructures, or platforms necessary for compliance. Instead, it allows Covered Entities to implement data protection measures that are reasonable and appropriate to the size, complexity and resources of each Covered Entity.

Electronic media subject to the Security Rule includes electronic storage material on which data is or may recorded electronically (such as hard drives, optical disks, and digital memory cards) or transmitted through the Internet, extranet, or intranet, dial-up connections, private networks, and the physical movement of removable electronic storage media. Transmissions of paper via facsimile and voice via telephone are not considered to be transmissions via electronic media if the information transmitted did not exist in electronic form immediately prior to transmission.

A Covered Entity must protect ePHI created, received, maintained, or transmitted by a Covered Entity from reasonably anticipated threats, hazards and impermissible uses or disclosures through the use of administrative safeguards, physical safeguards, and technical safeguards. In addition, the Security Rule describes policies and procedures and documentation requirements for Covered Entities. Policies should implement recommendations of the risk management program, with clearly established roles and responsibilities for each control. A Covered Entity must document its reasonable and appropriate security policies and procedures, and document any amendments necessary to meet the changing needs of the organization. Documentation of security policies and procedures must be retained for at least six years.

a. <u>Administrative Safeguards</u>

Administrative Safeguards comprise the majority of the HIPAA Security Rule's requirements and must be implemented in order for a Covered Entity to comply with the Security Rule. The Administrative Safeguards include a risk analysis, risk mitigation, assigned security responsibility, limitations on workforce access to ePHI, security training, security incident procedures, contingency planning, and business associate agreements.

i. Risk Analysis and Risk Management

A Covered Entity must perform and document an accurate and thorough risk analysis in which all of the systems that house ePHI are identified and assessed for vulnerabilities and threats. Vulnerabilities are flaws or weaknesses in system security procedures, design, or implementation that could be exploited and result in a security breach. Threats are reasonably anticipated natural, human, or environmental factors that could exploit a vulnerability identified by a Covered Entity. For example, a Covered Entity could identify a lack of redundant data backups as a vulnerability, with a natural disaster, such as a flood or hurricane, as an environmental threat. In order to complete a risk analysis, a Covered Entity should evaluate the potential of each vulnerability and threat combination to impact the confidentiality, integrity, or availability of ePHI, and identify actions to mitigate each identified risk.

Based on the results of its risk analysis, a Covered Entity must implement a risk management program that will reduce risks and vulnerabilities to an appropriate level. Following implementation, a Covered Entity must periodically evaluate its risk analysis in order to respond to new threats to ePHI, changes in the Covered Entity's policies and procedures, or the implementation of new technologies. Ongoing evaluations should be performed on a periodic basis and assess technical and non-technical aspects of a security program. As with the initial risk analysis, a Covered Entity must document subsequent analyses and risk mitigation measures.

ii. Assigned Security Responsibility

A Covered Entity must identify an individual who has final responsibility for the security of ePHI (the "Security Official"). The Security Official should be knowledgeable about electronic systems and able to assess an effective security plan and implement policies, procedures and workforce training. The Security Official can be, but is not required to be, the same person as the Privacy Official.

iii. Workforce Access to ePHI

A Covered Entity must develop procedures for authorization and supervision of workforce members with access to ePHI. Workforce members' business needs to access, view, modify, retrieve, or store ePHI should be documented. Covered Entities should limit access to ePHI to workforce members that require access to ePHI as a necessary component of their job. A Covered Entity must also establish policies and procedures to prevent workforce members who are not authorized to receive ePHI from obtaining access to ePHI. A Covered Entity must

establish and apply an appropriate workforce sanctions policy in the event that workforce members fail to comply with the Covered Entity's security policies and procedures.

iv. Security Training

A Covered Entity must develop and implement an appropriate security awareness and training program for all members of its workforce, including managers. Security awareness includes workforce understanding of the threats posed by malicious software, invalid log-in attempts, and creating and safeguarding passwords. Workforce training should be monitored and updated to address new and emerging security risks.

v. Security Incident Procedures

A Covered Entity must develop policies and procedures to address security incidents. Security incidents are attempted or successful access, use, disclosure, modification or destruction of ePHI or interference with normal systems operations. In developing policies and procedures, a Covered Entity must identify and respond to suspected or known security incidents, mitigate the effects of security incidents, and document the incidents and outcomes.

vi. Contingency Planning

In order to ensure the availability of ePHI, a Covered Entity must develop policies and procedures for responding to an emergency (such as a fire or natural disaster) that threatens information technology systems containing ePHI. Such a policy may include redundant backups and distributed offsite storage, with additional protection given to ePHI necessary for daily operations. As part of these policies and procedures, a Covered Entity must develop a data backup plan and disaster recovery plan and develop and implement an emergency operations plan. These contingency plans must undergo routine testing and re-evaluation to ensure that they are consistent with the Covered Entity's organizational needs.

vii. Business Associate Agreements

A Business Associate Agreement ("BAA") is required when a Covered Entity seeks to disclose ePHI to a party that will perform Business Associate services on behalf of the Covered Entity. In addition to the general requirements for BAAs that involve the transmission of PHI, BAAs involving ePHI must also require that a Business Associate implements the administrative, physical, and technical safeguards required under the HIPAA Security Rule. The BAA must also require a Business Associate's agents adequately protect ePHI by implementing reasonable and appropriate safeguards. The BAA must also require that a Business Associate report any security incident of which the Business Associate becomes aware. The BAA must allow the Covered Entity to terminate the contract due to material breach.

b. <u>Physical Safeguards</u>

Physical safeguards are the mechanisms, such as door locks and passcodes, used to protect electronic systems, such as server rooms and data storage facilities, equipment, and the

data stored therein, from threats, environmental hazards, and unauthorized intrusion. Physical safeguards also include workstation use and security and device and media controls.

i. Facility Access Controls

A Covered Entity must limit physical access to electronic information systems. These policies and procedures must include a facility security plan to prevent unauthorized physical access, tampering, and theft. Access to a facility should be limited based on a workforce member's or visitor's role or function. Policies and procedures must be implemented to document repairs and modifications to the facilities. In addition, a Covered Entity must develop plans to allow continuity of access in the event of an emergency.

ii. Workstation Use and Security

A Covered Entity must also develop policies and procedures that limit the use of workstations accessing ePHI to appropriate workforce members, such as individual passwords and automatic log-offs due to inactivity. Workstations should be assessed for whether physical position could lead to unauthorized access or viewing of ePHI. This requirement is different from but related to the administrative safeguard of limiting workforce access to ePHI based on each workforce member's need to access ePHI.

iii. Device and Media Controls

A Covered Entity must develop policies and procedures regarding the use and removal of electronic media. A Covered Entity should consider the feasibility of a global device encryption policy in order to limit potential breaches of ePHI due to lost laptops, smartphones, tablets, or other electronic media. The Covered Entity's policy must implement policies of the removal of ePHI from devices prior to reuse or disposal, including a policy to account for the movement of hardware and electronic media. Portable devices and media, in addition to remote access to information systems using such devices and media, tend to be significant risk areas for Covered Entities and their Business Associates and, therefore, should be issues of focus in the development of security policies and procedures.

c. <u>Technical Safeguards</u>

The Security Rule requires Covered Entities to evaluate and implement automated processes, such as authentication controls, to verify that the person accessing data is authorized to access the ePHI and methods, such as encryption, to protect data. The Security Rule also requires Covered Entities to implement audit controls and ensure the integrity of ePHI.

i. Transmission Security

A Covered Entity must implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network, such as encryption whenever appropriate and the implementation of physical and software-based firewalls. Security measures should protect ePHI in transmission from improper modification without detection.

ii. Access Controls and Authentication

A Covered Entity must implement access controls that allow only authorized workforce members or software to access systems containing ePHI. All system users must be assigned a unique identifier, such as a computer name or log-in credentials, that can be traced to a specific user. A Covered Entity must also establish a procedure for access to ePHI during an emergency.

iii. Audit Controls and Data Integrity

In order to determine whether ePHI is being appropriately used and disclosed, a Covered Entity must implement procedures to regularly review reports of information system activity. These reports can be generated as audit logs, access reports, or security incident tracking reports.

To protect ePHI from improper alteration or destruction, a Covered Entity must identify all users who have been authorized to access ePHI. In the course of monitoring user access to ePHI, a Covered Entity must also implement electronic mechanisms to verify and validate the integrity of ePHI stored on the Covered Entity's information systems.

V. THE BREACH NOTIFICATION RULE

A "Breach" is an impermissible use or disclosure of unsecured PHI that compromises the security or privacy of PHI and poses a significant risk of financial, reputational or other harm to the individual. The Breach Notification Rule provides for certain exceptions to be determined when the risk of harm to the individual is generally very low. The exceptions are as follows:

- Unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a Covered Entity.

- Inadvertent disclosure of PHI from a person authorized to access PHI at a Covered Entity to another person authorized to access PHI at the same Covered Entity. PHI unintentionally or inadvertently disclosed may not be further used or disclosed in a manner not permitted under the Privacy Rule.

- Finally, disclosures to unauthorized individuals where the Covered Entity has a good faith belief that the individual would not be able to retain the information do not constitute a breach.

Any potential breach should be evaluated by the Covered Entity with the advice and assistance of counsel. If the Covered Entity determines that no exception applies, any impermissible use or disclosure of PHI is presumed to be a Breach unless the Covered Entity demonstrates that there is a low probability that the data has been compromised, based on a risk assessment. The risk assessment must, at a minimum, examine:

- The nature and extent of the PHI involved;
- The identity of the unauthorized person who used or received the PHI;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

If a risk assessment does not demonstrate a low probability that the data have been compromised, a Covered Entity must notify the affected individual(s) without unreasonable delay and within sixty days of discovery of the Breach. Notification can be made by first-class mail or email, or, if the Covered Entity's contact information is out of date for ten or more individuals, via posting on the Covered Entity's website or in major print or broadcast media. If the Breach affects five hundred or more individuals in a given state or jurisdiction, notification must be made to local media outlets.

A Covered Entity must also notify the Secretary of HHS of all breaches of unsecured PHI. If a Breach involves 500 or more individuals, a Covered Entity must notify the Secretary within sixty days of discovery. If a Breach involves less than 500 individuals, a Covered Entity may notify the Secretary on an annual basis no later than sixty days after the end of the calendar year in which the Breaches occurred.

VI. THE ENFORCEMENT RULE

HHS OCR is authorized to enforce the HIPAA Privacy, Security, and Breach Notification Rules. OCR investigates privacy complaints filed by individuals, evaluates breach reports received from Covered Entities, and engages in HIPAA Audits of Covered Entities.

If OCR determines that a Covered Entity has violated HIPAA, it may assess the following civil monetary penalties based on the Covered Entity's culpability as follows:

Violation Category	Each Violation	All Violations in a Calendar Year
Did Not Know	$100-$50,000	$1,500,000
Reasonable Cause to Know	$1,000-50,000	$1,500,000

Willful Neglect – Corrected	$10,000-50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

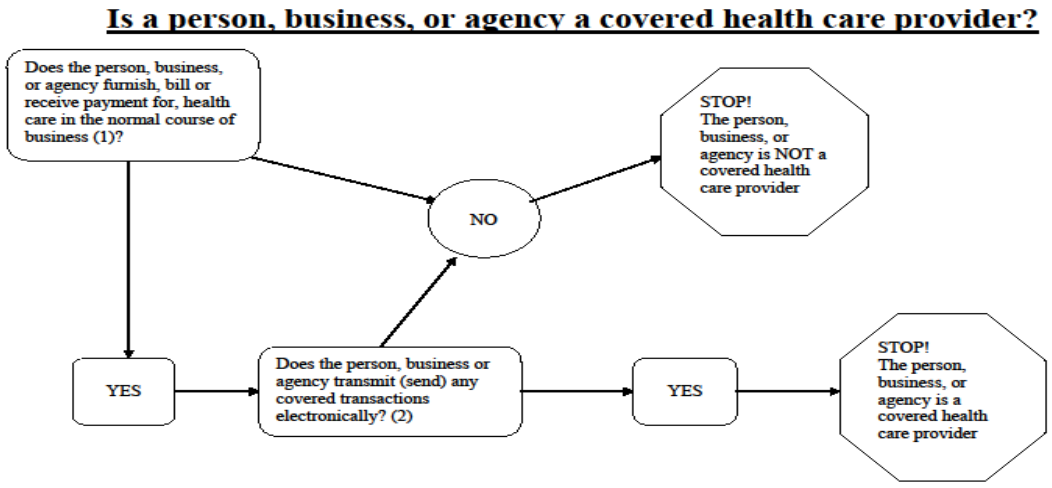
The "Did Not Know" tier applies to violations in which the Covered Entity establishes that it did not know and would not have known that the Covered Entity violated HIPAA. The "Reasonable Cause" tier applies to violations due to circumstances that would have made it unreasonable for the Covered Entity, despite the exercise of ordinary business care, to comply with HIPAA. The "Willful Neglect" tiers apply to conscious, intentional failure or reckless indifference on the part of the Covered Entity of its obligation to comply with HIPAA. The maximum penalty, for violations that are not corrected within thirty days of the Covered Entity's first becoming aware of the violation.

OCR will determine the extent of the penalty within each of the first three tiers based on the nature and extent of the violation, the nature and extent of the harm, as well as discretionary factors including the Covered Entity's history of compliance, financial condition, and such other matters as justice may require.

OCR also has the option to refer serious violations of HIPAA by Covered Entities, their agents, and their employees, to the Department of Justice for criminal investigation and enforcement. Criminal penalties for HIPAA violations range from $50,000 and up to one year of imprisonment to $250,000 and up to ten years imprisonment depending on whether the perpetrator intended to obtain a commercial advantage, personal gain, or to cause malicious harm.

* * *

Exhibit A



(1) Healthcare means: care, services, or supplies related to the health of an individual. It includes, but is not limited to, the following:
(1) Preventive, diagnostic, 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. See 45 C.F.R. 160.103.

(2) Covered transactions are transactions for which the Secretary has adopted standards; the standards are at 45 C.F.R. Part 162. If a healthcare provider uses another entity (such as a clearinghouse) to conduct covered transactions in electronic form on its behalf, the healthcare provider is considered to be conducting the transaction in electronic form.
A transaction is a covered transaction if it meets the regulatory definition for the type of transaction. These definitions for each type of covered transaction are provided below:

45 C.F.R. 162.1101: Healthcare claims or equivalent encounter information transaction is either of the following:

(a) A request to obtain payment, and necessary accompanying information, from a healthcare provider to a health plan, for healthcare.

(b) If there is no direct claim, because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting healthcare.

45 C.F.R. 162.1201: The eligibility for a health plan transaction is the transmission of either of the following:

(a) An inquiry from a healthcare provider to a health plan or from one health plan to another health plan, to obtain any of the following information about a benefit plan for an enrollee:

(1) Eligibility to receive healthcare under the health plan.
(2) Coverage of healthcare under the health plan.
(3) Benefits associated with the benefit plan.

(b) A response from a health plan to a health care provider's (or another health plan's) inquiry described in paragraph (a) of this section.

45 C.F.R. 162.1301: The referral certification and authorization transaction is any of the following transmissions:

(a) A request for the review of healthcare to obtain an authorization for the healthcare.

(b) A request to obtain authorization for referring an individual to another healthcare provider.

(c) A response to a request described in paragraph (a) or paragraph (b) of this section.

45 C.F.R. 162.1401: A healthcare claim status transaction is the transmission of either of the following:

(a) An inquiry to determine the status of a healthcare claim.

(b) A response about the status of a healthcare claim.

45 C.F.R. 162.1501: The enrollment and disenrollment in a health plan transaction is the transmission of subscriber enrollment information to a health plan to establish or terminate insurance coverage.

45 C.F.R. 162.1601: The healthcare payment and remittance advice transaction is the transmission of either of the following for healthcare:

(a) The transmission of any of the following from a health plan to a healthcare provider's financial institution:

(1) Payment.
(2) Information about the transfer of funds.
(3) Payment processing information.

(b) The transmission of either of the following from a health plan to a healthcare provider:

(1) Explanation of benefits.

(2) Remittance advice.

45 C.F.R. 162.1701: The health plan premium payment transaction is the transmission of any of the following from the entity that is arranging for the provision of healthcare or is providing healthcare coverage payments for an individual to a health plan:

(a) Payment.

(b) Information about the transfer of funds.

(c) Detailed remittance information about individuals for whom premiums are being paid.

(d) Payment processing information to transmit healthcare premium payments including any of the following:

(1) Payroll deductions.
(2) Other group premium payments.
(3) Associated group premium payment information.

45 C.F.R. 162.1801: The coordination of benefits transaction is the transmission from any entity to a health plan for the purpose of determining the relative payment responsibilities of the health plan, of either of the following for healthcare:

(a) Claims.

(b) Payment information.