A. What is HIPAA / HITECH?

The U.S. Congress passed the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to increase the privacy and security of medical information, to standardize certain common electronic business and financial transactions used in the health care industry, and to lower administrative costs associated with the business of health care. In 2009, the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which was enacted as a part of the economic stimulus legislation, modified certain provisions of HIPAA to strengthen its privacy and security protections.

Federal regulations implement both HIPAA and HITECH (the "HIPAA Regulations"). There are four main components to the HIPAA Regulations – the HIPAA Privacy Rule, the HIPAA Security Rule, the HIPAA Breach Notification Rule and the HIPAA Enforcement Rule.

A more detailed overview of HIPAA, HITECH and the HIPAA Regulations can be found at Appendix A.

B. Covered Entities and Business Associates

HIPAA and the HIPAA Regulations generally apply to health plans, health care clearinghouses, and any health care provider that transmits "Protected Health Information" (also referred to as "PHI," defined in Section II) in electronic form in connection with certain billing and financial transactions for which the U.S. Department of Health and Human Services ("HHS") has adopted standards under HIPAA. Such persons and entities are referred to as "Covered Entities" under HIPAA.

HIPAA and certain of the HIPAA Regulations also apply to persons or entities that perform or assist in the performance of certain services or activities for or on behalf of a Covered Entity, if the performance of the services or activities involves the creation, receipt, maintenance or transmission of PHI. Such persons and entities are referred to as "Business Associates" under HIPAA.

A Covered Entity is required to have a written contract in place with each of its Business Associates, often referred to as a "Business Associate Agreement" (or "BAA"). Prior to HITECH, a Business Associate was only contractually liable to a Covered Entity under the terms of its BAA. However, post-HITECH, Business Associates are now subject to, and directly liable under, HIPAA and certain of the HIPAA Regulations – in addition to their contractual obligations to the Covered Entity under the BAA. Even if a Covered Entity fails to enter into a BAA with a Business Associate, a person or organization that meets the definition of a Business Associate is still subject to, and directly liable under, HIPAA and certain of the HIPAA Regulations.

C. How Does HIPAA Affect Company?

Doctors Choice Home Care Inc (referred to as "Company") meets the definition of a HIPAA Covered Entity. As a provider of health care services, Company is required to maintain the privacy and security of PHI it creates, and the health care information it obtains from most other sources. Protecting the privacy and security of PHI is critical to maintaining the trust of the patients that Company directly serves.

D. Penalties for Noncompliance

HIPAA has penalties for noncompliance, which will take into consideration Company's good faith compliance efforts. The Secretary of HHS may impose fines up to $1.5 million per violation, and criminal penalties of up to 10 years imprisonment for knowing misuse of PHI for personal gain. If there is more than one violation, penalties can exceed $1.5 million. It is thus very important for all employees and other members of the Workforce to understand these HIPAA Privacy Policies and Procedures and to ask questions.

Complaints may be filed with HHS' Office for Civil Rights ("OCR") by any person who believes that a Covered Entity or Business Associate is not complying with the applicable requirements of the HIPAA

Regulations. Additionally, state Attorneys General can bring enforcement actions on behalf of Patients, and issue monetary penalties directly against Covered Entities and Business Associates.

E. HIPAA Policies and Procedures

These HIPAA Privacy Policies and Procedures apply to Company (as defined above). Company employees must treat all PHI as confidential and subject to these HIPAA Privacy Policies and Procedures. All members of Company's Workforce (defined in Section II), including employees and agents performing work on behalf of Company are expected to maintain the privacy and security of PHI in accordance with the HIPAA Privacy Policies and Procedures. *See also Company's HIPAA Security Policies and Procedures*.

The unauthorized Disclosure of PHI by any member of Company's Workforce could subject Company to civil fines and/or criminal penalties. As such, these HIPAA Privacy Policies and Procedures must be reviewed, understood and followed by all members of Company's Workforce that have access to PHI.

ANY MEMBER OF COMPANY'S WORKFORCE WHO KNOWS OF OR SUSPECTS A VIOLATION OF HIPAA OR THESE HIPAA PRIVACY POLICIES AND PROCEDURES IS REQUIRED TO REPORT THE INCIDENT TO COMPANY'S PRIVACY OFFICER OR HIS OR HER SUPERVISOR.

COMPANY STRICTLY FORBIDS RETALIATION OR THREATS OF ANY KIND AGAINST ANYONE WHO, IN GOOD FAITH, REPORTS OR EXPRESSES AN INTENTION TO REPORT A SUSPECTED VIOLATION OF HIPAA OR THESE HIPAA PRIVACY POLICIES AND PROCEDURES. SUCH RETALIATION OR THREATS WILL RESULT IN DISCIPLINARY ACTION, INCLUDING, AS APPROPRIATE, TERMINATION.

Key Definitions

This list paraphrases official definitions of some of the most common and important terms used in these HIPAA Privacy Policies and Procedures. Consult the HIPAA Regulations or the Privacy Officer for full and complete legal definitions.

- ***Authorization.*** A written document or form signed by a Patient or a Patient's Personal Representative that authorizes the Covered Entity or Business Associate to Use or Disclose PHI for a purpose not otherwise permitted under the HIPAA Regulations.

- ***Breach.*** An unauthorized acquisition, access, Use, or Disclosure of Unsecured PHI which compromises the security or privacy of such information. A Breach does not include the following:

  (a) the unauthorized acquisition, access, or Use of PHI by a Workforce member if such acquisition, access or Use was unintentional, made in good faith and within the course and scope of the employment or other professional relationship with the Covered Entity or Business Associate, and such information is not further acquired, accessed, Used or Disclosed without authorization;

  (b) an inadvertent Disclosure by an individual who is authorized to access PHI at an entity operated by a Covered Entity or Business Associate to another similarly situated individual at the same entity, as long as the PHI is not further acquired, accessed, Used, or Disclosed without authorization; or

  (c) a Disclosure of PHI where the Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

- ***Breach Notification Rule or the HIPAA Breach Notification Rule.*** The breach notification regulations promulgated pursuant to HITECH and codified at 45 C.F.R. Part 164, Subpart D, as may be amended from time to time.

- ***Business Associate.*** A person or entity who, on behalf of a Covered Entity, but not in the capacity of a member of the Covered Entity's Workforce, performs or assists in the performance of a function or activity involving the creation, receipt, maintenance or transmission of PHI, or provides legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services involving Disclosure of PHI.

- ***Covered Entity.*** A health plan, health care clearinghouse or health care provider who transmits any health information in electronic form in connection with a transaction covered by HIPAA.

- ***De-identified Health Information.*** Health information that does not identify an individual and with respect to which there is ***no*** reasonable basis to believe that the information can be used to identify an individual. De-Identified Health Information is not subject to the restrictions on Use and Disclosure which are applicable to PHI generally. In order for individual health information to be considered De-Identified Health Information, either (i) a person with appropriate knowledge and experience determines that the risk is very small that the information could be used to identify the Patient who is the subject of the information; or (ii) all of the following identifiers with respect to the Patient, or of relatives, employers, or household members of the Patient are removed:

  - Names

- Geographic subdivisions smaller than a state, including street address, city, county, zip code, precinct or other equivalent geocodes (except the initial three digits of a zip code may be used if the population in such three digit zip code is at least 20,000)
- All elements of dates (except year) for dates directly relating to a Patient, including birth date, admission date, discharge date, date of death, all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Fax numbers
- Email addresses
- Social Security Numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identification or license numbers
- Device identifiers and serial numbers
- URLs
- IP address numbers
- Biometric identifiers, including finger and voiceprints
- Full face photographic images
- Any other unique identifying number, characteristic or code

On November 26, 2012, OCR published formal guidance regarding methods for the de-identification of PHI in accordance with HIPAA. That guidance, and any further guidance issued by OCR on the meaning of De-Identified Health Information, is incorporated in these HIPAA Privacy Policies and Procedures as *Use and Disclosure of Protected Health Information for Research Purposes Policy (1.2.10)*.

- ***Designated Record Set.*** A group of records maintained by or for Company that includes medical, billing, enrollment, payment, claims adjudication, and other records used by Company, in whole or part, to make decisions about a Patient. *See also* Designated Record Set (Policy No. 1.1.6).

- ***Disclosure.*** The act of releasing, transferring, divulging, or providing access to PHI to an organization or individual that is not the Covered Entity maintaining that information.

- ***Discovered.*** The first day upon which a Breach is known, or by exercising reasonable diligence, should have been known.

- ***HHS.*** The U.S. Department of Health and Human Services.

- ***HHS Office for Civil Rights or "OCR".*** HHS' civil rights and health privacy rights law enforcement agency. OCR investigates complaints, enforces rights, promulgates regulations, develops policy, and provides technical assistance and public education to ensure understanding of and compliance with non-discrimination and health information privacy laws, including HIPAA.

- ***Electronic Health Record or "EHR".*** An electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care providers and staff.

- ***Electronic Protected Health*** Information ***or "E-PHI," "ePHI."*** PHI that is transmitted by electronic media or maintained in any electronic format or media.

- ***Health Care.*** Care, services, and supplies relating to the health of a Patient, including preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, etc.

- ***Health Care Operations.*** Activities normal to the business of providing health care; some examples include development of clinical guidelines, quality assessments, outcomes evaluations, clinical performance evaluations, business planning and development, providing customer/Patient services, etc.

- ***Health Care Provider.*** A provider of health care and any person or organization who furnishes, bills, or is paid for health care in the normal course of business.

- ***Health Information.*** Any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearing house; and relates to the past, present, or future physical or mental health or condition of a Patient; the provision of health care to a Patient; or the past, present, or future Payment for the provision of health care to a Patient.

- ***HITECH.*** The Health Information Technology for Economic and Clinical Health Act, Title XIII, Subtitle D, of the American Reinvestment and Recovery Act of 2009 (Pub. L. 111-5).

- ***Individually Identifiable Health Information.*** A subset of Health Information that incorporates the previous definition of Health Information and includes demographic information, and either identifies the Patient or provides a reasonable basis for believing it can be used to identify the Patient.

- ***Limited Data Set.*** Information that may be Individually Identifiable Health Information, and:

    (a) That summarizes the claims history, claims, or type of claims experienced by Patients; and

    (b) From which all of the identifiers listed in the definition of De-identified Health Information have been eliminated except that the information in a Limited Data Set may include: (i) the Patients' town, city, state and the last three (3) digits of a Patient's zip code; and (ii) elements of dates related to a Patient including birth date, admission date, discharge date, and date of death.

- ***Marketing*.** Communications about a product or service that encourages the recipient of the communication to purchase or use the product or service. Marketing communications do not include any of the following:

    (a) Communications to provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by the Covered Entity in exchange for making the communication is reasonably related to the Covered Entity's cost of making the communication.

    (b) Communication for the following Treatment and Health Care Operations purposes, except where the Covered Entity receives financial remuneration (direct or indirect payment from or on behalf of a third party whose product or service is being described) in exchange for making the communication:

        (i) For Treatment of a Patient by a health care provider, including for case management or care coordination for the Patient, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the Patient;

        (ii) To describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the Covered Entity making the communication, including communications about:

            - The entities participating in a health care provider network or health plan network;

            - Replacement of, or enhancements to, a health plan; and

            - Health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.

        (iii) Contacting of individuals with information about treatment alternatives, and related functions, to the extent these activities do not fall within the definition of Treatment.

- ***Notice of Privacy Practices or "NPP".*** A document that health care providers and Health Plans are required to provide to Patients describing the individual rights under HIPAA and the manner in which the Covered Entity may Use or Disclose PHI. A Covered Entity that is in a direct Treatment relationship with the Patient is required to provide Patients with a NPP no later than the first service delivery date (or, in an emergency, as soon as reasonably practicable) and, if the Covered Entity maintains a physical service delivery site, have the NPP available upon request and posted in a clear and prominent location. If a Covered Entity maintains a website, it must post the NPP to its website.

- ***Patient.*** The person who is the subject of PHI.

- ***Payment.*** Any activities such as billing, collection, and related actions taken by a Covered Entity and/or its Business Associates to obtain reimbursement for health care services rendered.

- ***Personal Representative.*** A Personal Representative is a person with authority under state law to act on the Patient's behalf on matters relating to health care. Generally, a parent of a patient if the patient is a minor; a person empowered under the Patient's Power of Attorney (general or for health care); a legal guardian; or an executor or administrator of a Patient's estate will be Personal Representatives. The

HIPAA Privacy Rule permits a Patient's Personal Representative to stand in the place of the Patient and exercise any rights the Patient may otherwise exercise pursuant to HIPAA.

- ***Privacy Rule or the HIPAA Privacy Rule.*** The regulations regarding the privacy of certain health care information promulgated pursuant to HIPAA and codified at 45 C.F.R. Parts 160 and 164, Subparts A and E, as may be amended from time to time.

- ***Protected Health Information or "PHI".*** Protected Health Information (or "PHI") is information about a Patient's health care, created, received or maintained by a Covered Entity, such as Company, that identifies a Patient or with respect to which there is a reasonable basis to believe the information can be used to identify the Patient. PHI includes information related to the past, present or future physical or mental health or condition of a Patient; information about the provision of health care to a Patient; and information related to the past, present or future Payment for the provision of health care to a Patient. The following are not considered PHI: (i) employment records, including results of pre-employment or annual physicals and doctors' notes for return to work following illness or injury; (ii) information relating to disability insurance or life insurance; (iii) workers' compensation records; and (iv) records regarding a person who has been deceased for more than 50 years.

- ***Secretary.*** The Secretary of HHS or his/her designee.

- ***Security Incident.*** The attempted or successful unauthorized access, Use, Disclosure, modification, or destruction of information or interference with system operations in an information system.

- ***Security Rule or the HIPAA Security Rule.*** The federal security standards under HIPAA as contained in 45 C.F.R. Parts 160 and 164, Subparts A and C, as may be amended from time to time.

- ***Subcontractor.*** A person or organization which a Business Associate has contracted to perform the services or activities on behalf of a Covered Entity, like Company.

- ***Treatment.*** The provision, coordination, or management of health care and related services that health care providers render to a Patient. Treatment includes management of health care with a third party, consultation between providers relating to a Patient, or the referral of a Patient for care or services to another provider. HIPAA permits Disclosure of PHI for purposes of providing Treatment without an Authorization or need for a Business Associate Agreement.

- ***Unsecured PHI.*** PHI that is not secured through the use of a technology or methodology specified in guidance issued by the Secretary of the HHS detailing those technologies and methodologies that render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

- ***Use.*** The sharing, employment, application, use, examination, or analysis of PHI within an entity that maintains such information.

- ***Workforce.*** Employees, volunteers, trainees, and other persons, including contractors and agents, whose conduct, in the performance of work for a Covered Entity or Business Associate, is under the direct control of such entity, whether or not they are paid by the Covered Entity or Business Associate.

Appendix A

DETAILED OVERVIEW OF HIPAA, HITECH AND THE HIPAA REGULATIONS

The U.S. Congress passed Health Insurance Portability and Accountability Act of 1996 ("HIPAA") to give people greater control over the privacy of their medical information, to standardize certain common electronic transactions used in the health care industry, and to lower administrative costs associated with the business of Health Care. In 2009, the Health Information Technology for Economic and Clinical Health Act ("HITECH"), which was enacted as a part of the economic stimulus legislation, modified certain provisions of HIPAA to strengthen its privacy and security protections.

Federal regulations implement both HIPAA and HITECH (the "HIPAA Regulations"). There are four main components to the HIPAA Regulations -- the HIPAA Privacy Rule, the HIPAA Security Rule, the HIPAA Breach Notification Rule and the HIPAA Enforcement Rule.

On January 25, 2013, the long-awaited HIPAA Final Omnibus Rule (the "Final Rule") was published. The Final Rule implemented changes to HIPAA, and the HIPAA Regulations – including the final modifications mandated by HITECH.

Discussed below are some of the key terms and concepts covered by HIPAA, HITECH and the HIPAA Regulations (including some of the more notable changes implemented by the Final Rule):

1. Covered Entities

HIPAA and the HIPAA Regulations generally apply to health plans, health care clearinghouses, and to any health care provider who transmits "Protected Health Information" (also referred to as "PHI," as described below) in electronic form in connection with certain covered transactions for which the Secretary of the U.S. Department of Health and Human Services ("HHS") has adopted standards under HIPAA. Such persons or entities are considered "Covered Entities" under HIPAA.

2. Business Associates

HIPAA and certain of the HIPAA Regulations also apply to persons or entities that perform or assist in the performance of certain services/activities for or on behalf of a Covered Entity, if the performance of the services involves the Use or Disclosure of PHI. Such persons and entities are considered "Business Associates" under HIPAA.

3. Business Associate Agreements

When a Covered Entity uses a contractor or other non-Workforce member to perform "Business Associate" activities and services, HIPAA requires that the Covered Entity and the Business Associate enter into a "Business Associate Agreement" ("BAA") In the BAA, a Covered Entity must, among other things, impose specified written safeguards on the PHI Used or Disclosed by its Business Associate and require the Business Associate to report any Use or Disclosure of such information not authorized by the agreement.

The Final Rule also requires additional elements be included in a BAA, such as (i) a statement that the Business Associate must comply with Subpart C of Part 164 of the HIPAA Security Rule; (ii) a statement that the Business Associate must report Breaches of Unsecured PHI to the Covered Entity; (iii) a statement that the Business Associate must obtain satisfactory assurances (in the form of a written BAA) from any Subcontractor that creates or receives PHI on behalf of the Covered Entity that the Subcontractor agrees to the same restrictions and conditions that apply to the Covered Entity with respect to such information; and (iv) to the

extent the Business Associate is delegated to carry out a Covered Entity's obligations under the HIPAA Privacy Rule (*e.g.*, responding to accounting of Disclosures or providing a Patient with a Notice of Privacy Practices or access to PHI), the Business Associate must comply with the requirements of the HIPAA Privacy Rule that apply to the Covered Entity in the performance of such delegated obligations.

4. Protected Health Information

HIPAA protects all "Individually Identifiable Health Information" held or transmitted by a Covered Entity or a Business Associate, in any form or media, whether electronic, paper, or oral. HIPAA calls this information "Protected Health Information" (or "PHI").[1]"Individually identifiable health information" is information, including demographic data, that relates to: (a) the Patient's past, present or future physical or mental health or condition; (b) the provision of health care to the Patient; or (c) the past, present, or future Payment for the provision of health care to the Patient, and that identifies the Patient or for which there is a reasonable basis to believe can be used to identify the Patient. Individually identifiable health information includes many common identifiers and demographics (*i.e.*, name, address, birth date, Social Security Number) and all kinds of medical data such as diagnoses, prescriptions, medication history, bills, and Patient education materials. Note: *Demographic information does not have to be linked to medical data in order to be considered PHI.* If Individually Identifiable Health Information is "de-identified"[2] and provides no reasonable basis to identify a Patient, then there are no restrictions on the Use or Disclosure of such De-identified Health Information.

5. The HIPAA Privacy Rule

The HIPAA Privacy Rule, as amended by HITECH, generally establishes requirements to protect PHI maintained and Used by a Covered Entity or a Business Associate. Among numerous other requirements, the HIPAA Privacy Rule: (i) limits certain uses and Disclosures of PHI; (ii) limits most Disclosures of PHI to the minimum necessary for the intended purpose; (iii) requires Patient Authorizations for certain uses and Disclosures of PHI; (iv) guarantees Patients the right to access their medical records and to know who else has accessed them; (v) establishes requirements for Breach notification; and (vi) imposes criminal and civil sanctions for improper uses or Disclosures of PHI. The HIPAA Privacy Rule requires a Covered Entity and, to a certain extent, a Business Associate to have policies in place addressing these requirements and to maintain those policies for 6 years from the date of creation.

Under the HIPAA Privacy Rule, the basic concept is that a Covered Entity may Use and Disclose a Patient's PHI only (i) as the Patient permits (*e.g.*, through an Authorization); or (ii) as permitted under the HIPAA Regulations.

A Covered Entity is permitted to Use and Disclose PHI for, among other things: (1) Treatment; (2) Payment; and (3) Health Care Operations. These core health care activities are defined in the HIPAA Privacy Rule:

A. Treatment is generally defined as the provision, coordination, or management of health care and related services for a Patient by one or more health care providers, and the referral of a Patient by one provider to another.

---

[1] Excluded from the definition of PHI are (i) employment records held by a Company in its role as an employer; and (ii) Individually Identifiable Health Information about a person who has been deceased for more than 50 years.

[2] There are two ways to de-identify information: (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the Individual and of the Individual's relatives, household employees, and employers is required (as indicated at 45 C.F.R. §164.502(d)), and is adequate only if Company has no actual knowledge that the remaining information could be used to identify the Individual. On November 26, 2012, HHS' Office for Civil Rights published formal guidance regarding methods for de-identification of PHI in accordance with HIPAA.

B. **Payment** encompasses activities of a health care provider to obtain Payment or be reimbursed for the provision of health care to a Patient (*i.e.*, determinations of coverage eligibility, billing, collection activities, and utilization review).

C. **Health Care Operations** include the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) the sale or purchase of a practice (and the due diligence process relating thereto); and (e) business management and general administrative activities of the entity.

There are a number of other uses and Disclosures permitted under the HIPAA Privacy Rule, such as a Use or Disclosure required by law, for public health activities, to the Food and Drug Administration (in certain circumstances), to law enforcement or for law enforcement purposes, to a health oversight agency, in judicial and administrative proceedings, to avert a serious threat or health or safety, for research, to the military and correctional institutions and to the extent necessary to comply with worker's compensation laws.

Moreover, a Covered Entity and Business Associate must make reasonable efforts to Use, Disclose, and request only the minimum amount of PHI needed to accomplish the intended purpose of the Use, Disclosure, or request (known as the "Minimum Necessary Rule"). When the Minimum Necessary Rule applies to a Use or Disclosure, a Covered Entity and Business Associate may not Use, Disclose, or request the entire medical record for a particular purpose, unless it can specifically justify the whole record as the amount reasonably needed for the purpose. The Minimum Necessary Rule is not imposed in all circumstances; for example, it is not imposed on a Disclosure to or a request by a health care provider for Treatment or a Use or a Disclosure that is required by law.[3]

If a Use or Disclosure is not permitted under the HIPAA Regulations, a written Authorization must be obtained from the Patient. For example, a written Authorization must be obtained to Use or Disclose PHI for Marketing purposes (regardless of whether remuneration is received). Marketing does not include face-to-face communications to the Patient as to Treatment options, providing gifts of nominal value, or communications to describe health-related products or services that are provided by a Covered Entity.

A Covered Entity generally may *not* condition Treatment on the Patient signing an Authorization (unless, for example, the Patient's PHI will be used for research). The Patient may revoke the Authorization at any time in writing, except to the extent that it has been relied on by the Covered Entity. The Authorization form must be obtained prior to the Disclosure of any PHI for which an Authorization is required. The HIPAA Privacy Rule contains certain requirements for Authorizations, including: (i) a description of the PHI to be Used or Disclosed; (ii) identification of who is authorized to make the requested Use or Disclosure; (iii) identification of to whom the authorized Use or Disclosure will be made; (iv) a statement of the purpose of the Use or Disclosure; (v) the date or event upon which the Authorization will expire; (vi) an indication that the Patient has the right to revoke the Authorization in writing, unless it has been relied upon prior to the time of revocation; (vii) statement that information Used or Disclosed pursuant to the Authorization may be subject to re-Disclosure by the recipient(s) and no longer protected by the HIPAA Privacy Rule; and (viii) a statement that Treatment will not be conditioned on signing the Authorization, except where allowed by law (e.g., for

[3] The HIPAA Privacy Rule does not require that every risk of an incidental Use or Disclosure of PHI be eliminated. A Use or Disclosure of this information that occurs as a result of, or as "incident to," an otherwise permitted Use or Disclosure is permitted as long as Covered Entity has adopted reasonable safeguards as required by the HIPAA Privacy Rule, and the information being shared was limited to the minimum necessary.

research). The Authorization must be dated and signed by the Patient. It should be retained for at least six (6) years after signature by the Patient.

Under the HIPAA Privacy Rule, Covered Entities are also required to (i) appoint a "privacy officer" to be responsible for the development and implementation of the privacy policies and procedures; (ii) designate a contact person to be responsible for receiving complaints and responding to inquiries about privacy matters (often times this is the privacy officer); and (iii) provide privacy training to all Workforce Members who have access to PHI (this training should be documented).[4] While Business Associates are not required to implement these requirements, it is considered best practice for Business Associates to implement at least some of these requirements.

6. The HIPAA Security Rule

The HIPAA Security Rule, as amended by HITECH, generally requires a Covered Entity and a Business Associate to implement administrative, physical, and technical safeguards to ensure the privacy and confidentiality of PHI when it is electronically stored, maintained, or transmitted. If a Covered Entity or Business Associates does not store, maintain or transmit E-PHI, then the HIPAA Security Rule does not apply. If a Covered Entity or Business Associates does store, maintain or transmit E-PHI, the HIPAA Security Rule only applies to that E-PHI.

Under the HIPAA Security Rule, certain specifications of safeguards are required and other specifications of safeguards are suggested or "addressable." In determining whether to implement an "addressable" specification, a Covered Entity or Business Associate must assess whether the specification is a reasonable and appropriate safeguard in its environment, taking into consideration the specification's contribution to protecting the entity's E-PHI, the size, complexity, and capabilities of the entity, the entity's technical infrastructure, hardware, and software security capabilities, the cost of the security measure, and the probability and criticality of potential risks to the E-PHI. Following such an assessment, the Covered Entity or Business Associate must implement the specification if it is reasonable and appropriate; or, if not, document why it would not be reasonable and appropriate, and implement an alternative measure.

The HIPAA Security Rule also requires a Covered Entity and a Business Associate: (i) to appoint a "security officer" who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Rule; (ii) to have policies and procedures in place addressing the safeguards; (iii) to maintain those policies for six (6) years from the date of creation.

7. Patient Rights

The HIPAA Regulations provide Patients with a number of rights with respect to their PHI. Those rights include:

A. A right to receive a written notice as to how their PHI will be Used and Disclosed and how they can gain access to the information.

This notice is often referred to as a Notice of Privacy Practices ("NPP"). It must be provided by a Covered Entity to the Patient at the first office visit, unless the Patient presents an emergency situation, in which case it should be obtained as soon as practicable. Business Associates are not required to provide a NPP.

The HIPAA Privacy Rule requires the NPP to include, among other things : (i) a description of the uses and Disclosures of PHI that may be made for Treatment, Payment and Health Care Operations; (ii) a description of

[4] Each new employee should be trained within a reasonable time after commencement of employment.

each of the purposes for which the law allows a Covered Entity to Use or Disclose the Patient's PHI without obtaining the Patient's Authorization; (iii) a statement that other uses will be made only with the Patient's Authorization, and that such Authorization may be revoked; (iv) a description of the Patient's rights with respect to their PHI (e.g., that a Patient has a right to receive notice if there is a Breach of his/her Unsecured PHI and the Patient has the right to request a restriction on the Disclosure of information to a health plan if the information relates solely to an item or service for which the Patient has paid out of pocket in full (discussed below); (v) if the health care provider intends to contact the Patient to raise funds, the Patient will have the opportunity to opt-out of receiving such communications[5]; (vi) the name, title and telephone number of the Covered Entity's contact person where the Patient may obtain further information about the Covered Entity's privacy practices or submit a complaint).

The NPP should be signed by the Patients to indicate that they have received a copy of it. If the Patient refuses to sign the notice, the refusal must be documented. The signed notice should be retained for six (6) years. If there is a material change to the notice, the revised notice must be made available to a Patient upon the Patient's request. A Covered Entity health care provider is also required to have the revised NPP available and posted in a clear and prominent location at the care delivery site.

B. A right to inspect and obtain copies of their PHI.

A Covered Entity has 30 days after receiving a request for access or copies from a Patient in which to provide the access or information. 60 days is allowed for a response if the records are maintained off-site. A 30-day extension may be obtained if, within the initial 30-day period, the Covered Entity provides written notice to the Patient of the reasons for the delay and gives a date on which a response will be given. Requests for access or copies from a Patient should be in writing.

Under the Final Rule, a Covered Entity health care provider is required to give a Patient, upon the Patient's request, an electronic copy of PHI that is maintained electronically in a Designated Record Set. This means that if a provider maintains its medical records electronically, the provider must be able to provide a Patient with his/her records on a disc or via secure email formatted as a PDF or Word file, or through a secure web-based portal within 30 days of the Patient's request (or within 60 days if the provider gives the Patient proper notice of its need for an extension). A provider can charge the Patient a "reasonable, cost-based fee" to provide the electronic copy of the PHI. This fee may include (i) technical Workforce members time spent creating and copying the electronic file, such as compiling, extracting, scanning and burning PHI to media; (ii) the cost of supplies for creating electronic media (e.g., discs, flash drives, etc.); and (iii) the cost of postage if the Patient requests that the portable media be sent by mail or courier.

C. A right to amend or modify their PHI.

Although there are exceptions set out in the rule, Patients generally have the right to ask the Covered Entity to amend their PHI. Such a request should be made in writing. If the Covered Entity amends the information, a list of persons or entities that the Patient wants the Covered Entity to inform of the amendment must be obtained from the Patient, along with an authorization to inform them. The Covered Entity must then undertake reasonable efforts to notify those persons and entities of the amendment. However, the Covered Entity is allowed to deny the Patient's request if, among other reasons, the information is accurate and complete, or the Covered Entity did not create the information. If the Covered Entity denies the request, it must be denied in

[5] Under the Final Rule, a Healthcare Provider can Use an Individual's PHI for purposes of making a communication about raising funds for the provider; however, the Individual receiving the fund-raising communication (in writing or over the phone) must be provided with a clear and conspicuous opportunity to opt-out of receiving any further fundraising communications. If the Individual opts-out of receiving future fundraising communications, the provider must treat the Individual's choice to opt-out as a revocation of the Individual's Authorization to Use his or her PHI for fundraising communications.

writing. Any written denial must also advise the Patient of the reasons for the denial, allow the Patient to submit a "written disagreement," state that the Patient may ask that the request to amend and the denial be included with any future Disclosure of the subject information (if no "written disagreement" is submitted), and mention the Patient's right to file a complaint with the Secretary.

D. A right to request restrictions on the Use and Disclosure of their PHI.

Although Patients are allowed to request restrictions on the Use and Disclosure of their PHI, the Covered Entity is not obligated to honor the request – except as provided below. If the Covered Entity agrees to the request, he/she must adhere to it unless the Patient presents an emergency situation.

Under the Final Rule, if a Patient asks a Covered Entity health care provider to restrict the Disclosures of his/her PHI to a health plan made for Payment and Health Care Operations purposes and the PHI pertains solely to a health care item or service for which the Patient (or someone acting on the Patient's behalf) has paid the provider in full, the health care provider must agree to the restriction. While a provider is not required to create a separate medical record or otherwise segregate PHI subject to such a restriction, a provider will need to flag or use some other method to identify portions of the record that contain PHI subject to the restriction in order to ensure it is not inadvertently sent or made accessible to the health plan for Payment or Health Care Operations purposes (*e.g.*, during audits by the health plan).

E. A right to request confidential communication of their PHI.

A Patient may, for example, request that the communication of his or her PHI be made by alternative means (*i.e.*, sending correspondence to the Patient's office rather than to his or her home). If such a request is made, the Covered Entity must comply with it if the request is reasonable. The Covered Entity may not inquire as to the reasons for the request. However, the Patient can be asked to provide this request in writing, which is generally advisable.

F. A right to receive an accounting of certain Disclosures made by Covered Entity of their PHI.

Patients have the right to receive an accounting of certain Disclosures of their PHI made by the Covered Entity within 6 years from the date of the request. The accounting must include: the date of Disclosure; the name and address of the person or entity who received the PHI; a brief description of the information Disclosed; and, a brief description of the purpose for the Disclosure. There are several exceptions to this requirement, e.g., Disclosures relating to Treatment, Payment, or Health Care Operations, Disclosures made pursuant to an Authorization that has been signed by the Patient; and incidental Disclosures. Any request for an accounting must be responded to within 60 days of the request. An additional 30 days can be obtained if, within the initial 60-day period, the Covered Entity notifies the Patient in writing of the reasons for the delay and provides a date on which a response will be given. A Patient is entitled to one free accounting within a 12-month period. The Covered Entity is permitted to charge a reasonable fee for each additional accounting if the Covered Entity gives the Patient notice of the fee at the time of the request.

G. A right to be notified if there is a Breach of their Unsecured PHI.

As described in more detail below, a Patient has the right to be notified within 60 days following the Discovery of a Breach of his/her Unsecured PHI.

8. The HIPAA Breach Notification Rule

Under the HIPAA Breach Notification Rule, Covered Entities and their Business Associates are required to provide notification following a Breach of Unsecured[6] PHI. A Breach is defined as the acquisition, access, Use or Disclosure of PHI in a manner not permitted by the Privacy Rule which compromises the security or privacy of such information. There are 3 exceptions to this definition:

1. Any unintentional acquisition, access or Use of PHI by a Workforce member or Patient acting under the authority of a Covered Entity or a Business Associate if such access or Use was made in good faith and within the scope of authority and does not result in a further unauthorized Use or Disclosure;

2. Any inadvertent Disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, and the information is not further Used or Disclosed in an impermissible manner; and

3. A Disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

Under the Final Rule, any unauthorized Use or Disclosure of PHI that does not meet one of the Breach exceptions is presumed to be a Breach unless the provider can demonstrate (through a written risk assessment) that there is a "low probability that the PHI has been compromised."

The 4 factors that must be considered in the risk assessment include:

1. the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

2. the unauthorized person who Used the PHI or to whom the Disclosure was made;

3. whether the PHI was actually acquired or viewed; and

4. the extent to which the risk to the PHI has been mitigated.

A Covered Entity may consider other factors (as appropriate), but the risk assessment must be documented, thorough, completed in good faith and the conclusions reached must be reasonable. However, a Covered Entity has the discretion to provide the required notifications following an impermissible Use or Disclosure of PHI without performing a risk assessment. Because the Final Rule creates the presumption that a Breach has occurred following every impermissible Use or Disclosure of PHI, a Covered Entity may decide to make required Breach notifications without evaluating the probability that the PHI has been compromised. Ultimately, a Covered Entity has the burden to prove that all notifications were provided or that an impermissible Use or Disclosure did not constitute a Breach (by demonstrating through a risk assessment that there was a "low probability that the PHI had been compromised"). Covered Entities and Business Associates must maintain documentation sufficient to meet that burden of proof.

Following a Breach of Unsecured PHI, a Covered Entity must provide notification of the Breach to affected Patients, the Secretary, and, in certain circumstances, to the media. In addition, Business Associates must notify Covered Entities that a Breach has occurred.

[6] Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized Individuals through the use of a technology or methodology specified by the Secretary in guidance.

Notice to the Patient(s):

Covered Entities must notify affected Patients following the Discovery of a Breach of Unsecured PHI. Covered Entities must provide this Patient notice in written form by first-class mail, or alternatively, by e-mail if the affected Patient has agreed to receive such notices electronically. If the Covered Entity has insufficient or out-of-date contact information for 10 or more Patients, the Covered Entity must provide substitute Patient notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected Patients likely reside. If the Covered Entity has insufficient or out-of-date contact information for fewer than 10 Patients, the Covered Entity may provide substitute notice by an alternative form of written, telephone, or other means.

These Patient notifications must be provided without unreasonable delay and in no case later than 60 days following the Discovery of a Breach and must include, to the extent possible, a description of the Breach, a description of the types of information that were involved in the Breach, the steps affected Patients should take to protect themselves from potential harm, a brief description of what the Covered Entity is doing to investigate the Breach, mitigate the harm, and prevent further Breaches, as well as contact information for the Covered Entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for Patients to contact the Covered Entity to determine if their PHI was involved in the Breach.

Notice to the Media:

Covered Entities that experience a Breach affecting more than 500 Patients of a State or jurisdiction are, in addition to notifying the affected Patients, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered Entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like Patient notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the Discovery of a Breach and must include the same information required for the Patient notice.

Notice to the Secretary:

In addition to notifying affected Patients and the media (where appropriate), a Covered Entity must notify the Secretary of Breaches of Unsecured PHI. Covered Entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a Breach report form. If a Breach affects 500 or more Patients, Covered Entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a Breach. If, however, a Breach affects fewer than 500 Patients, the Covered Entity may notify the Secretary of such Breaches on an annual basis. Reports of Breaches affecting fewer than 500 Patients are due to the Secretary no later than 60 days after the end of the calendar year in which the Breaches occurred.

Notification by a Business Associate:

If a Breach of Unsecured PHI occurs at or by a Business Associate, the Business Associate must notify the Covered Entity following the Discovery of the Breach. A Business Associate must provide notice to the Covered Entity without unreasonable delay and no later than 60 days from the Discovery of the Breach. To the extent possible, the Business Associate should provide the Covered Entity with the identification of each Patient affected by the Breach as well as any information required to be provided by the Covered Entity in its notification to affected Patients.

9. Enforcement

OCR and States Attorneys General may impose sanctions on Covered Entities and Business Associates for the failure to comply with requirements of the HIPAA, including civil monetary penalties ("CMPs") ranging from

$100 to $50,000 per HIPAA violation. Under HITECH, the maximum CMPs that can be applied for additional violations in any one year are within a range of $25,000 to $1,500,000. HHS is required to impose a CMP if a violation is found to constitute willful neglect of the law. The Final Rule implemented the following tiered penalties to reflect the level of the entity's culpability:

Violation Category	Each Violation	All Such Violations of an Identical provision in Calendar Year
Did Not Know	$100-$50,000	$1.5 million
Reasonable Cause	$1,000-$50,000	$1.5 million
Willful Neglect, Corrected within 30 Days	$10,000-$50,000	$1.5 million
Willful Neglect, Not Corrected within 30 Days	$50,000	$1.5 million

The Final Rule also clarified that HHS will not impose the maximum penalty amount in all cases but will instead determine the penalty based on (i) the nature and extent of the violation; (ii) the resulting harm (e.g., the number of Patients affected, reputational harm, etc.); (iii) the entity's history of prior offenses or compliance; (iv) the financial condition of the entity; and (v) any other factor that justice may require be considered. HHS also retains the ability to waive a CMP, in whole or in part, and to settle any issue or case or to compromise the amount of a CMP.

Finally, the Final Rule also clarified how HHS will count the number of violations and apply the tiered penalties (and the tiered penalty caps):

- Where multiple Patients are affected by an impermissible Use or Disclosure (such as in the case of a Breach of Unsecured PHI) for purposes of levying penalties, the number of violations of the HIPAA Regulations will be based on the number of Patients affected. For example, if a Breach involves the PHI of 1,000 Patients, the Breach will be viewed as 1,000 violations of the same provision.

- When a violation is continuous over a period of time (for instance, if a Covered Entity or Business Associate has inadequate technical safeguards in place over a period of time) for purposes of levying penalties, the number of identical violations will be based on the number of days in which the entity did not have adequate safeguards in place. For example, if an entity's technical safeguards are inadequate for 60 days, there will be 60 violations of the same provision.

- If an event involves violations of two provisions of the HIPAA Regulations (*e.g.,* there is an impermissible Use or Disclosure of PHI and there are inadequate safeguards in place), HHS may calculate a separate CMP for each provision. This means that the annual penalty cap for such an event would be $3 million -- $1.5 million cap for the impermissible Use or Disclosure of PHI plus the $1.5 million cap for inadequate safeguards.

HHS may also impose criminal penalties for certain wrongful Disclosures. These criminal penalties can be enforced against Covered Entities, Business Associates, and Patients, including, but not limited to, employees of a Covered Entity or Business Associate. The criminal penalties vary depending on whether the offense is

committed under false pretenses or with the intent to sell the information or use it for personal gain. Under HITECH, the maximum criminal penalties include fines up to $250,000 and up to 10 years imprisonment.

10. No Private Right of Action

Patients do not have a private right of action under the HIPAA Regulations; that is, a Patient may not sue under HIPAA for a violation of HIPAA. However, the HIPAA Regulations create a system which allows Patients to make complaints to OCR about potential violations, and the HIPAA Regulations require covered entities and Business Associates to develop a process to review complaints about such violations.[7]

11. State Laws

Separate from HIPAA and HITECH, there a number of state privacy and security laws that protect identifiable individual information, including information which is not health-related. These laws are generally related to special protections placed on specific types of health information (*e.g.*, mental health records or information related to a Patient's HIV/AIDS status).

In general, state laws that are contrary to the HIPAA Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply, unless the contrary state law provides more stringent protections to the privacy or security of the PHI than the HIPAA Regulations or the state law gives a Patient greater rights with respect to the Patient's PHI (e.g., a greater right to access PHI). In other words, the federal standards will not preempt a state law that is more stringent than the related federal requirements. In some instances, if federal and state requirements are not the same, but are not contrary to each other (i.e., compliance with one would result in the violation of the other), and then both the state law and the federal law must be followed. Please contact the Privacy Officer prior to making a Disclosure of sensitive information, including but not limited to, mental health/developmental disability records, HIV status, alcohol/drug abuse treatment records or genetic information.

[7] While HITECH did not create a private right of action for violations of the HIPAA Regulations, it did include a section which would allow harmed Individuals to benefit from and receive a portion of all CMPs and monetary settlements collected by OCR. As of the date this Guide was approved, Individuals do not have access to any percentage of such monies, as the implementing regulations for this requirement have not yet been finalized.