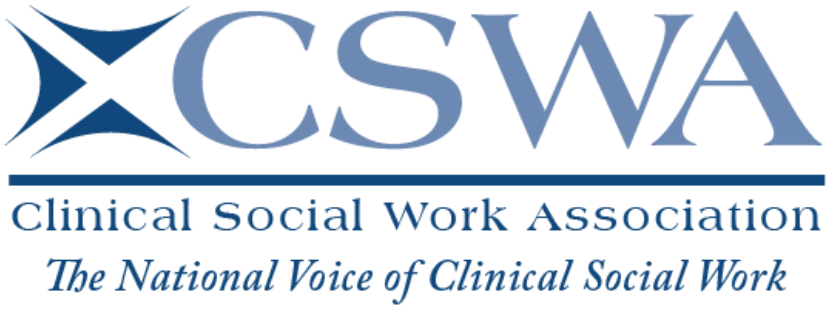


Clinical Social Work Association

HIPAA - Eleven Years Later

Compliance with HIPAA Privacy and Security Rules: The Impact on LCSW Practice

Prepared by:
Laura W. Groshong, LICSW
R. Keith Myers, LICSW
David G. Schoolcraft, JD

{CFM1070926.DOC;5/99910.002222/}

[This page intentionally left blank.]

Contents

[This page intentionally left blank.]

Foreword

In 1996, Congress passed the Health Information Portability and Accountability Act. Part of this bill included a requirement for the development of privacy regulations to protect health care information. The purposes of the Privacy Rule were to protect misuse of individual health information; to limit the sharing of healthcare information to specific groups for specific purposes; to give new rights to the patient as to how and when his/her health care information is disclosed; and to give new rights to the patient to review and correct what is written in their health care records. The initial set of Rules were completed in 2000 under the auspices of the Office of Civil Rights (OCR) within the Department of Health and Human Services (HHS) led by Sec. Donna Shalala, and were entered into the Federal Register as law (RIN 0991-AB14).

Privacy of communication between patient and therapist is a primary concern of clinical social workers, in fact, of all clinicians. All major disciplines have sections in their codes of ethics that spell out the responsibilities of the clinician to maintain the privacy of the treatment relationship, with some differences in emphasis. Most states have regulations about the privacy of medical/mental health records, which vary considerably. The Federal regulations that were phased in on April 14, 2003, were the first attempt at the Federal level to construct protection of medical/mental health records. This Manual will compare the existing privacy standards as presented in the Clinical Social Work Association (formerly the Clinical Social Work Federation) Code of Ethics, the new standards of the Health Insurance Portability and Accountability Act ("HIPAA"), and the changes in current standard practices that are needed to comply with HIPAA requirements.

This Manual will detail existing privacy standards according to HIPAA as of September 23, 2013 and the changes in current standard practices that may be needed to comply with HIPAA requirements.

[This page intentionally left blank.]

The Clinical Social Work Association

The Clinical Social Work Association (CSWA), the Voice of Clinical Social Work, is made up of individual members from every state/jurisdiction and internationally and 15 affiliated state societies. The Association works for improvement in the standards of the profession, the protection of clients, and the professional development of its members. The Federation provides both clients and members with advocacy on mental health issues before the Congress and regulatory bodies and assists the state societies with advocacy at the state level. Association members, all of whom hold advanced degrees and have undergone thousands of hours of supervised clinical internships before being licensed or certified, provide more than half of all the mental health services delivered in the country. Its Board of Directors is made up of licensed clinical social workers from around the country.

The Clinical Social Work Federation, now the Clinical Social Work Association (CSWA), strongly supported the original Rule and objected to the revisions made in 2002. CSWA is a membership organization, affiliated with 15 state societies, that works toward the provision of ethical mental health treatment by clinical social workers through education, legislation, and advocacy. There are currently approximately 170,000-200,000 licensed clinical social workers in the United States who provide 50–60% of all mental health treatment in the country (SAMHSA, 1999, CSWF, 2005). CSWA is working toward reinstatement of the original provisions of the Rule providing stronger protections for the individual. CSWA also views the current Rule as a floor for privacy standards, not a ceiling. Many states exceed HIPAA requirements in some or all areas, as does the privacy Rule in the CSWA Code of Ethics (see Appendix 2).

This Manual represents the Association's view of how HIPAA standards fit into ethical clinical social work practice and, thus, goes beyond the requirements of the HIPAA Rule. The Manual indicates where recommended practices herein exceed HIPAA standards. Though the ethical standards used in this manual meet most state laws whose privacy standards exceed those of HIPAA, we recommend everyone educate themselves about their state privacy standards and how they compare to the standards used in this manual and the HIPAA Rule.

[This page intentionally left blank.]

Acknowledgements

Upon its original completion in 2003, the compilation of this Manual spanned more than a year. The four revisions that have occurred since 2003 have incorporated changes to the HIPAA Rule as they occurred. The research, development of materials, and training presentations could not have come about without the dedication and tireless efforts of many individuals. The authors wish to thank the many individuals who helped us undertake the arduous task of researching and writing the material for CSWF, now CSWA.

First, the Association wishes to thank David Schoolcraft, JD, Dana Kenny, JD, and Casey Moriarty, JD, of Ogden Murphy Wallace law firm for their assistance with the current 2014 version of this Manual, and Mr. Schoolcraft for his invaluable assistance as a co-author.

Much appreciation goes to Jan Sklennik, our Graphics Editor and Production Manager, without whom this work could not have been developed.

The update of the Manual for 2014 was completed by Laura Groshong, LICSW, R. Keith Myers, LICSW, and David Schoolcraft, JD,(see bios below) during the CSWA Presidency of Stephanie Hadley, LCSW. The leadership of CSWA has been instrumental in creating and updating this Manual.

Laura W. Groshong, LICSW, has been a clinical social worker in private practice for 37 years in Seattle, Washington. She graduated from the University of Chicago School of Social Service Administration in 1974 and received Certification in Adult Psychotherapy from the Seattle Psychoanalytic Institute in 1979. Ms. Groshong is also a Registered Lobbyist in Washington state and has lobbied on behalf of 8 mental health groups for better access to mental health treatment for 20 years. She has also been the Government Relations Director for Clinical Social Work Association since 2006 and in that capacity has worked with LCSWs in over 30 states to create or improve their social work licensure laws and on other legislative/regulatory issues throughout the country and at state and national levels. She is the author of Clinical Social Work Practice and Regulation: An Overview (Rowman and Littlefield, 2009).

R. Keith Myers, LICSW, is the Past-President of the Clinical Social Work Federation. He is a nationally known presenter on clinical and regulatory topics pertaining to clinical social work. He is an Auxiliary Faculty Member of the University of Washington School of Social Work. He has served on the boards of several psychoanalytic organizations. He is also Vice President of Clinical and Training Services for Wellspring Family Services in Seattle, Washington, where he oversees the activities of over 60 mental health therapists who work for the agency. He serves as the HIPAA Privacy Official for that agency.

David Schoolcraft, JD, is a member of Ogden Murphy Wallace law firm in Seattle, Washington, with a practice focusing on health care, corporate representation, technology, and data privacy. His health care transaction practice includes acquisitions, joint ventures, MSOs, IPAs, and general business and operation transactions. His regulatory and compliance practice includes fraud and abuse, Stark, EMTALA, HCQUIA, medical reimbursement, antitrust, licensing, and implementation of compliance programs. Mr. Schoolcraft also advises on e-health issues, data protection and privacy including HIPAA, and other federal and state privacy laws.

[This page intentionally left blank.]

Goals of This Manual

The HIPAA Privacy and Security Standards are the main focus of this manual (for the history of the HIPAA regulations and a brief summary of the regulations, see below) In general, privacy is about who has the right to access and use personally identifiable health information. The Privacy and Security Standards cover all individually identifiable health information in the hands of what HIPAA calls "Covered Entities," those individuals and organizations that are covered by HIPAA regulations, regardless of whether or not the information is or has been in electronic form.

The Privacy and Security Standards:

- Impose limitations on the use and disclosure of private health information;
- Give new patient rights provisions including the right to access medical records and to know who else has accessed them;
- Restrict disclosures of health information to the minimum necessary for the intended purpose, except for treatment purposes;
- Provide recommendations for the management of PHI and ePHI;
- Provide requirements for the tangible security of computers on which ePHI is stored;
- Impose new criminal and civil sanctions for improper use or disclosure; and
- Impose new requirements for access to records by researchers and others.

Effective compliance requires certain implementation steps. They include:

- Building initial awareness of HIPAA;
- Comprehensive assessment of the individual's or organization's information security systems, policies and procedures;
- Developing and implementing an action plan with deadlines and timetables;
- Developing a GAP Analysis, Risk Management Assessment and Risk Management Policies for PHI and ePHI;
- Developing new policies, processes, and procedures;
- Breach notification;
- Developing new internal communications; and
- Training and enforcement where applicable.

This Manual follows these implementation steps and provides what we believe to be a practical approach to compliance with the Privacy Standards. The recommendations made take into consideration both the HIPAA Privacy Standards and clinical social work ethical standards for privacy, making them more rigorous in some areas than HIPAA regulations alone.

[This page intentionally left blank.]

Introduction

Privacy of communication between patient and therapist is a primary concern of clinical social workers, in fact, of all mental health clinicians. All major disciplines have sections in their codes of ethics that spell out the responsibilities of the clinician to maintain the privacy of the treatment relationship, with some differences in emphasis. Most states have regulations about the privacy of medical/mental health records, which vary considerably (see summary below). The Federal regulations that were phased in starting April 14, 2003, were the first attempt at the Federal level to construct protection of medical/mental health records. This Manual will compare the existing privacy standards of the CSWA Codes of Ethics, the new Standards of the Health Insurance Portability and Accountability Act ("HIPAA"), and the changes in current standard practices that will be needed to comply with HIPAA requirements.

The CSWA Code of Ethics (see Appendix 2) clearly states the importance or patient information as follows:

> *"Clinical social workers have a primary obligation to maintain the privacy of both current and former clients, whether living or deceased, and to maintain the confidentiality of material that has been transmitted to them in any of their professional roles. Exceptions to this responsibility will occur only when there are overriding legal or professional reasons and, whenever possible, with the informed consent of the client."* (CSWA Code of Ethics, 1997)

Additionally, the CSWA Code of Ethics showed some anticipation of the need to protect electronic information as follows:

> *"The development of new technologies for the storage and transmission of data poses a greater danger to the privacy of individuals. Clinical social workers take special precautions to protect the confidentiality of material stored or transmitted through computers, electronic mail, facsimile machines, telephones, telephone answering machines, and all other electronic or computer technology. When using these technologies, disclosure of identifying information regarding the client(s) should be avoided whenever possible."* (Ibid, p.9)

In the past 5–10 years, information about patients, primarily for billing purposes, has increasingly been sent to insurers through the Internet. In addition, there has been an increase in the communication between patient and therapist through email, sometimes as the primary method of therapeutic communication. Most people who use the Internet to communicate believe their communications are protected, except from "hackers" whose intrusions are rare.

This is not the case. Sending information through unprotected channels (including standard servers such as aol.com, msn.com, etc.) on the Internet without using encryption is like sending a postcard through the mail. While there is no guarantee someone will read a post card, there is a much greater possibility of it being read than a letter sent in a sealed envelope. The protection of electronically transmitted data is something every responsible clinician should be concerned about. To this degree, there is no conflict between the HIPAA regulations and standard confidentiality practices. HIPAA regulations force us to face the reality of electronic transmission and the ways that this information is vulnerable.

All medical and mental health providers who are Covered Entities because they have engaged in covered transactions had to comply with the HIPAA Privacy and Security Standards as of 2003 or 2005. Although fines of up to $25,000 are possible, the government appears more concerned that providers understand the requirements of the regulations and come into compliance with them.

Secretary Tommy Thompson, who became HHS Secretary in 2001, significantly altered the Rules to weaken their impact in two key areas, the requirement of informed consent for the release of an individual's information and the use of that information for marketing purposes. The original Rule required that information be disclosed only with the informed consent of the individual. The revised rule substitutes "regulatory permission" for that of the consent of the individual, a significantly lower level of protection. Under the original Rule, individuals had been given the option to "opt-in" regarding the sale of their health care information, that is, that their information could not be used for marketing purposes without their specific consent. The revised Rule now allows for an "opt-out" option, that is, the individual must specifically request their health care information not be used for these purposes. This is at odds with the CSWA Code of Ethics and is a problem CSWA is working to correct.

Since the passage of the HITECH Act of 2009 as part of the American Recovery and Reinvestment Act (ARRA), with the accompanying new Rules that went into effect on September 23, 2013, HIPAA has become much stronger. Sections that were sketched out in the original Rule have been spelled out and further developed including encryption, enforcement, audit trails, health information technology certification and use, and much more. We will likely continue to see changes in HIPAA rules over the next four years as health care reforms affect the use of HIPAA. Medical homes will likely have HIPAA considerations, as will mental health parity. The changes to health care delivery and how health care records are shared are exciting and potentially will improve communication between patients and providers, as well as between providers. CSWA is tracking all changes to health care and HIPAA to maintain the highest level of privacy for mental health records.

Basic HIPAA Knowledge and Language

History and Summary of HIPAA Privacy and Security Regulations

HIPAA is the acronym for the Health Insurance Portability and Accountability Act of 1996. In addition to provisions related to the continuation and portability of health insurance coverage, the so-called "Administrative Simplification" provisions of HIPAA mandate a federal regulatory structure governing the privacy, security, and electronic transfer of health care information.

On December 28, 2000, the Department of Health and Human Services (HHS) issued the Privacy Standards establishing federally mandated policies regarding how health information can be used and disclosed, new individual rights, and new administrative requirements. The Privacy Standards were revised and amended by HHS on May 31 and August 14, 2002. The Security Standards went into effect on May 23, 2005. A complete copy of the final regulation text is available at www.hhs.gov/ocr/index.html. New parts of the Rule were implemented in 2009, 2010, and 2013.

It is important for all mental health clinicians, including LSCWs to have a basic understanding of the major components of HIPAA's Administrative Simplification provisions, i.e., the HIPAA Privacy and Security Rules.

Transaction and Code Set Standards

The HIPAA Transaction and Code Set Standards are rules that standardize the electronic exchange of health care information. They are based on electronic data interchange (EDI) standards, which allow electronic exchange of information from computer to computer without human involvement. What is important for mental health practitioners to know is that HIPAA set the Current Procedural Terminology (CPT) as the standard for procedure codes and International Classification of Diseases, Ninth Revision, Clinical Modification (ICD- 9-CM) as the standard for diagnoses. CPT codes are the ones most practitioners are currently using. They are a five digit code that tells insurance companies whether you are providing individual, group, family etc. counseling. The most common codes for LCSWs are 90801 and 90806, which are the diagnostic interview and for a 45–50 minute individual psychotherapy interview, respectively. The ICD was chosen over the Diagnostic and Statistical Manual, Fourth Edition (DSM-IV-TR). The implementation of Tenth Revision of the ICD Codes (ICD-10) is scheduled to take place in October of 2012. Insurance companies and government- run health programs, e.g., Medicare and Medicaid, already comply electronically with the transaction standards set forth in this part of HIPAA.

Protected Health Information (PHI and ePHI)

In order to fully understand the HIPAA Privacy and Security Standards, LCSWs need to start with an understanding of protected health information, or PHI, and electronic protected health information, or ePHI, as they are defined in the regulations. Generally stated, PHI is health information that is identifiable to a specific individual and that is maintained or transmitted by a Covered Entity in any form, whether in oral, paper, or electronic form. EPHI is any identifiable health care information sent electronically by a Covered Entity.

A chart, bill for services, or even a hallway conversation between two clinicians about an individual's care is a conversation involving PHI. Information is considered to be individually identifiable if it identifies the individual or if there is a reasonable basis to believe that the information can be used to identify the individual. Thus, PHI can include demographic information such as name, address, and age.

The Difference Between Privacy and Security Standards

There has been confusion about the difference between privacy standards and security standards as described by HIPAA. Privacy standards are about who has the right to disclose and use protected health information, and when they can do so. This standard applies to all PHI communicated by a Covered Entity whether expressed orally, in writing on paper, or electronically transmitted. Security standards apply to the security of paper records as well as electronically stored or transmitted information. In addition, electronic records must be protected from corruption by viruses, theft by 'hackers', and/or putting information at risk by sending ePHI on unsecured channels.

Compliance Deadlines for Clinicians as Covered Entities

The deadline for compliance with the Privacy Standards was April 14, 2003. The deadline for compliance with the Security Standards was May 23, 2005.

The Transaction and Code Set Standards compliance deadline was October 16, 2003.

The new HITECH Act rules for Business Associate Agreements, Breach Notifications, Notice of Privacy Practices, Fundraising, and Marketing became effective on September 23, 2013.

Covered Entities under HIPAA

The HIPAA regulations directly regulate only those who meet the definition of a Covered Entity. In general, clinicians who engage in electronic billing become Covered Entities and fall within scope of the HIPAA standards. If you do not bill electronically or otherwise transmit health information in connection with one of the defined "covered transactions" (see below) under HIPAA, you are not covered by the regulations. The HIPAA rules are moving payers towards adopting EDI as the standard for billing and related transactions. For example, as of October, 2003, Medicare will refuse to pay any claims that are not filed electronically from all healthcare providers, except those with less than 20 employees. As of 2008, many clinicians who continue to file paper claims have found them rejected by Medicare if they are not completely 'clean', i.e., with no lines outside the boxes.

Even if the HIPAA regulations do not directly apply, and you choose to maintain a "paper only" practice, it is important to consider the risks and drawbacks that could arise in a legal world based on HIPAA standards. Probably the greatest risk is the indirect impact the Privacy and Security Standards could have on health care providers. Even if you are not technically a Covered Entity, you will still be practicing in a privacy environment with new legal parameters after April 23, 2003. The risk is that these Privacy Standards will be applied by courts (rightly or wrongly) as the standard of care for handling client information. In other words, even if HIPAA does not technically apply, it may be difficult to justify actions that are not consistent with the new federal standards is a confidentiality complaint is filed against you as a clinician.

Covered Transactions

A covered transaction is any computer-to-computer transmission of healthcare claims, payment and remittance, benefit information, or health plan eligibility information. As a health care provider, if you submit any bills (even for a single client) electronically to insurers, MCOs or any other party directly or through a billing service, you are a Covered Entity. Other covered transactions include:

1. **Health Care Claims** – request for reimbursement by a provider to a health plan for health care services.
2. **Eligibility for Treatment** – request for information by a provider to a health plan about eligibility, coverage limits, and/or benefits in a health plan for a client or potential client.
3. **Authorization for Treatment** – request made to a health plan for authorization of mental health treatment by a mental health provider.
4. **Health Care Claims Status** – request by a mental health provider to a health care plan for the status of a health care claim previously made.

Note that simply receiving funds transferred electronically through a bank account is not a covered transaction. Also note that voice communications via telephone or transfers of information by fax do not constitute electronic transactions, but HHS has indicated that it considers PC based fax transmissions to be electronic transactions under the rule. In addition, recent interpretations by HHS officials indicate that they consider some automated key pad phone information systems to be covered transactions. The basic guide to this rule seems to be that if there is an electronic record of the information retained somewhere after it is sent, it is a covered transaction. Since verbal interactions disappear after they are spoken, no record exists. Likewise, since no record exists after a paper fax is transmitted, it is not considered a covered transaction.

Treatment, Payment and Health Care Operations (TPO)

The Privacy Standards generally prohibit the use and disclosure of PHI without an individual's prior written authorization. The most significant exception to this general rule is that a Covered Entity may use and disclose PHI, without prior authorization, for purposes of treatment, payment, and health care operations. The practical implication of this exception is that for most purposes, a clinician will not need to obtain a client's written approval in order to deliver treatment, facilitate payment, and otherwise operate a practice.

It is important to note that each of these terms (treatment, payment, and health care operations) has detailed definitions under the Privacy Standards which are also included in the Frequently Asked Questions at the end of this manual. Any other reason for disclosure of information (excluding certain disclosures permitted or required by law such as disclosures to child protection agencies) requires a separate authorization signed by the patient. It is also important to note that each state has its own Privacy and Security Laws which should be reviewed in addition to HIPAA Privacy and Security Rules.

Uses and Disclosures of Protected Health Information (PHI and ePHI)

According to HIPAA standards, once a patient has acknowledged receipt of the Notice of Privacy Practices form (see below), there is no need to have the patient sign a separate form for the disclosure of information for TPO purposes. HIPAA standards require an Authorization to be signed for the disclosure of psychotherapy notes. However, we recommend best practices for clinicians include having a patient sign an Authorization for the release of any PHI or ePHI, electronically or on paper, including TPO information, consultation for medical review, and any other purpose.

We also recommend any information that is sent out about the patient be discussed directly with the patient prior to sending such information. State laws should also be considered as some states do require an Authorization be signed before TPO information can be sent. As a Covered Entity under HIPAA, you must allow clients to request that you restrict the use and disclosure of PHI and ePHI. However, HIPAA regulations say you are not necessarily required to agree with the restriction. Under HIPAA, clients cannot restrict disclosure for treatment, payment and health care operations (TPO). Furthermore, disclosures are permitted for involvement in the individual's care and notification purposes. This is one of the requirements in HIPAA that generally goes against good psychotherapy practice. The ability to release information without client consent goes against most codes of ethics in virtually all mental health fields.

However, since HIPAA standards define the floor, you can set your own policies so that they are more "stringent" than the HIPAA standards. The sample policies we have developed (see below) are more stringent and are consistent with most mental health codes of ethics. Another area where the HIPAA "floor" for privacy standards differs significantly from best psychotherapy practices is that PHI or ePHI may be disclosed to family members or for public health activities. The only time PHI or ePHI should ever be disclosed by a clinician without a written Authorization is if the patient represents a danger to himself or herself or others and is unable to recognize this. A patient should be notified verbally that the clinician intends to contact CPS or Involuntary Treatment Assessment experts before doing so.

In order to be compliant with HIPAA standards for disclosure of PHI and ePHI, an Authorization Form must contain the following elements:

- A description of the information to be disclosed;
- Who (individual or organization) is making the request;
- Expiration date of the request;
- A statement that the individual has the right to revoke the request;
- A statement that information may be subject to re-disclosure by the receiving party;
- Signature and date; and
- If signed by a representative, a description of their authority to make the disclosure.

Summary of ARRA/HITECH Law

The President signed the American Recovery and Reinvestment Act (H.R. 1) on February 17, 2009, which includes the HITECH (Health Information Technology for Economic and Clinical Health Act) on privacy rules for the use of electronic health information. There are some important elements that affect clinical social workers.

There was a last minute consideration of the removal of the patient-psychotherapist privilege, granted by the Supreme Court (1996) in Jaffee v. Redmond. This would have been a terrible blow to the cornerstone of our clinical work. Due to much work by mental health associations, the bill instead has a protection of privilege, stating that nothing in the Subtitle on privacy will constitute a waiver of "any privilege otherwise applicable to an individual with respect to the protected health information of such individual." Section 13421(c).

Additionally the bill includes the following protections of health care information:

- Patient notification of all disclosures without consent, or "breaches", of protected health information;
- Creation of an Health Information Technology Policy Commission charged, among other things, with creating electronic records which will "segment" or separate mental health information (and other sensitive information) from the general record with greater privacy protection;
- Encryption of patient information when sent outside a health care network;
- Audit trails to determine who has accessed health care information and for what purpose;
- The right of the provider to determine what "minimum necessary" information is for disclosures (the Secretary may issue guidelines later); and
- Opt-in requirements for sale of patient information, i.e., patients must consent in writing to the sale of their health care information.

Finally, there will be grant money available for providers who need financial assistance for building an electronic health care record, though currently this funding is not available for LCSWs.

Security Standards

The final piece of the 1996 HIPAA Act was the Security Standards. The Security Standards were published on April 21, 2003. All Covered Entities were required to have Security Standards in place by April 21, 2005, except for small businesses (under 50 employees) which had until April 21, 2006. All agencies are responsible for educating employees on the HIPAA Security Standards and making sure they implement HIPAA Security Standards.

The HIPAA Security Standards mandate safeguards for physical storage and maintenance, protection, and access to individual health information in electronic form. The term ePHI is used when referring to protected health information covered by the Security Standards, as these standards apply only to information in electronic form.

The Privacy and Security Standards together require the clinician to take reasonable precautions to safeguard Protected Health Information (PHI) and electronic Protected Health Information in electronic or paper form.

HIPAA Security Standards address the tangible security of health care information, whether stored on computer or on disc, and how it is protected, as opposed to how the information is transmitted to others, which was addressed in the Privacy Standards. These standards are less complex than the Privacy Standards, but vary from the Privacy Standards in ways it is important for all those who have protected health information (PHI) to understand. The HIPAA Security Standards apply to all mental health clinicians who are Covered Entities.

The implementation of the Security Standards has some of the same procedural requirements as the implementation of the Privacy Standards. All clinicians who are Covered Entities must become aware of what the Security Standards are and how they affect the way they manage the security of their records; complete a comprehensive assessment of their current practices to protect the security of their records (GAP Risk Analysis); develop policies which will incorporate the Security Standards into their security practices; and develop a Risk Management Action Plan for implementing the Security Standards.

There is one key difference between HIPAA Security Standards and Privacy Standards. While Privacy Standards were expanded to apply to oral and written communication of PHI as well as electronic communication, Security Standards are specific to electronic communication. As with the Privacy Standards, however, the Security Standards apply to Covered Entities, or anyone with PHI who has sent PHI at least once electronically in a Covered Transaction. This is why when PHI is referenced in Security Standards, it is called “ePHI”, to indicate that the standards only apply to electronic records.

De-identification of PHI and ePHI

PHI and ePHI may be released when the information contained is “de-identified.” This process of de-identification involves the removal of 19 “identifiers” which make health information identifiable as belonging to a specific person.
Here are the 19 items that must be de-identified to release PHI and ePHI:

A. Names;

B. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

- The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

- The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

C. All elements of dates (except year) for dates directly related to an 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 age, except that such ages and elements may be aggregated into a single category of age 90 or older;

D. Telephone numbers;

E. Fax numbers;

F. Electronic mail 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 as permitted by paragraph (c) of this section; and

S. The Covered Entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Email Systems

While there is no prohibition to the use of email systems in the Security Standards, there IS a requirement that all ePHI sent electronically must be kept secure and protected from unapproved access by others. Since sending an email over open networks (gmail.com, comcast.net, etc.) is like sending a postcard through the mail, use of major email servers without some form of data encryption is unlikely to meet Security Standards.

Encryption

Encryption is a computer program that puts the original document in code that hides the wording and meaning of the document. It is likely that encryption will become an electronic health record requirement, though it is not at this time. Some insurers provide these programs to their providers. The burden of protecting ePHI, however, rests with the provider. When storing Electronic Medical Records (EMRs) and Electronic Health Records (EHRs) in the virtual 'cloud', best practice should be encryption for the protection of these records. Most cloud-based records are encrypted because of the privacy dangers of interoperable systems.

Safeguards for ePHI

Passwords and automatic logoffs are required to protect access to stored information. Encryption of ePHI is not required by the HIPAA Security Rule, though it is a best practice for protecting electronic communication of ePHI. Firewall and virus scans are required to protect the internal integrity of the ePHI so that it cannot be stolen or changed. Backing up all ePHI is necessary because if computer-stored ePHI should be corrupted, deleted, or otherwise lost, the responsibility for maintaining access to the ePHI rests with the provider. The only way to guarantee access is to have a backed up copy of the ePHI on a thumb drive or in a cloud-based backup system, e.g., Carbonite.com.

Review of Security Procedures

All Covered Entities must review their security procedures. The process of assessing your security procedures is called a Risk Assessment. The process of documenting what you are doing to protect ePHI is a called Risk Management Plan. In the Risk Analysis, any potential risk to maintaining the privacy and integrity of ePHI is identified (see Security GAP Analysis form). In the documentation of Risk Management, all steps taken to protect against risks to the privacy and integrity of ePHI are identified (see Security GAP Analysis).

1. **Are backup discs containing ePHI and printed copies of ePHI covered by the Security Standards?**

   Yes. Any form of electronically generated, stored, or transmitted ePHI must have risks to the privacy and integrity of the information assessed.

2. **How many times does a provider need to send ePHI electronically as part of a covered transaction to be considered a Covered Entity? What forms of transmission are considered covered transactions?**

   If a provider sends ePHI electronically once as part of a covered transaction, the provider is a Covered Entity. Covered transactions include computer to computer transmissions; computer fax to computer or paper fax transmissions, and key pad telephone transmissions. Covered transactions do not include paper to paper faxes or voice mail transmissions.

3. **What happens if a Covered Entity loses ePHI through computer error or inadequate security procedures?**

   The Covered Entity is responsible for the security of all ePHI and will be found in violation of HIPAA Security Standards, if there is no documentation of Security Policies and Procedures, a Risk Analysis, and Risk Management Plan.

4. **Does a provider need to guarantee the confidentiality of a paper to paper fax?**

   While the Security Standards do not specifically address this issue, the Privacy Standards do require that all PHI be kept confidential. Therefore, a Covered Entity should ensure the privacy of PHI sent on paper to paper faxes.

5. **What are the security risks a Covered Entity should consider in doing a Risk Analysis?**

   A Risk Analysis should include risks to the computer systems containing ePHI, and all PHI generated in paper or electronic form from computer systems, which may be unintentional or intentional. The risks considered include administrative, technical and physical risks to the confidentiality and integrity of ePHI.

6. **What are the security risks that are administrative risks?**

   These risks include violation of BAA agreements with non-Covered Entities, violation of agreements by staff or partners to follow Risk Management practices, lack of training for staff, and lack of documented Risk Management Practices.

7. **What are required security procedures to guard against administrative security risks?**

   Required security procedures include chain of trust partner agreements; procedures to be followed for data backup; data storage; testing of security system; shared access authorization and modification; supervision of non-authorized personnel who have access to ePHI; BAA with all Covered Entities who have access to ePHI; installation of security hardware and software and testing of same; Risk Analysis and Risk Management documentation; internal sanction procedures for anyone who violates Risk Management practices; documentation of all violations of Risk Management practices and consequences; training of all staff in use of computer passwords, virus scan programs, and automatic logoffs; and termination procedures for personnel who no longer have access to ePHI to prevent any further access to ePHI or changes to the integrity of ePHI (see GAP Analysis).

8. **What are the security risks that are technical risks?**

   These risks include unauthorized access to computer generated ePHI (confidentiality), unauthorized changes to ePHI (integrity), and ways to document unauthorized access to and changes to ePHI (availability).

9. What are possible security procedures to guard against technical security risks?

Possible security procedures against technical security risks include audit controls (audit trails); user and/or role identification (passwords - REQUIRED); automatic logoffs (REQUIRED); encryption, alarms, documentation of all violations of Risk Management Practices, emergency access procedures to PHI, and context-based access to PHI.

10. What are security requirements for the physical safety of PHI?

Requirements include an assigned security 'officer'; auditing controls; data backup; secure data storage; PHI secure disposal procedures; disaster recovery program; emergency mode operations; procedures authorizing physical access to work station or data storage areas; building security plan; "need-to-know" levels of PHI access; and system testing.

11. Are there absolute requirements for how any Risk Management is implemented?

No, there are no absolute requirements, just areas of administrative, technical, and physical risk to ePHI which must be addressed in some way and documented by the Covered Entity.

12. Is it possible to be "certified" as compliant with HIPAA Security Standards?

No. There are no certifications available to certify compliance. Periodic internal evaluations and/or evaluations by independent agencies expert in assessing security systems may be used to assess compliance. However, no evaluation will prohibit HHS from finding violation(s) of compliance with HIPAA Security Standards.

13. How will a Covered Entity know if compliance with HIPAA Security Standards has been achieved?

There is no definite way to know at this time beyond making every effort to document that a Risk Analysis has been completed, and Risk Management Plan has been put in place including all required elements in the Security Standards.

14. Do the Security Standards apply to voice mail or video teleconferencing?

Yes, because they are an electronic form of the health care record.

Notice of Privacy Practices (NPP)

The privacy regulations of HIPAA allow you to disclose PHI for TPO without authorization, but require written authorization for almost all other types of releases. However, best practices for clinical social workers would be to have patients sign an Authorization form for any release of information, including TPO. What follows is a summary of what HIPAA standards require, not what best practices for CSWs would be.

To insure that clients know their privacy rights, HIPAA requires that you provide clients a Notice of Privacy Practices (NPP) at the time of the first session. You must maintain documentation that the client received the NPP. We suggest that you have clients sign two copies of the NPP and retain one in the client file and give the other to the client.

Alternatively, you may choose to have clients sign a form stating that they received the NPP (see below). If for some reason, you are unable to obtain a client's signature, you should document your attempts to do so and the reasons why you were unable to obtain the signature. The only time you are not required to make a good faith effort to obtain receipt of the NPP is in emergency treatment situations.

It is important that you reserve the right to change a privacy practice in your NPP. If you do not do this, you are required to follow the practices stated in the NPP as long as it is in effect. By including this language in the NPP, you allow the flexibility to change your practices when applicable.

CHANGES TO NPP:

On September 23, 2013, the following changes to the NPP went into effect:

- Every NPP must contain a description of the LCSW's policies on disclosures that require authorization, including disclosures for psychotherapy notes, marketing, and sale of protected health information.
- Every NPP must contain a statement that patients will be notified of a breach of unsecured protected health information.
- If the LCSW may contact patients for fundraising purposes, every NPP must contain a statement that the LCSW may contact the patient to raise funds, and that patients have a right to opt out of receiving such communications.
- Every NPP must contain a statement that the LCSW is not required to agree to a patient's request to restrict disclosures of PHI, unless the patient requests a restriction on the use and disclosure of PHI to the patient's health plan, and the patient has paid the LCSW out of pocket in full for such services.
- All NPPs must be updated by September 23, 2013 or as soon as possible after this date. The new effective date for the NPP must be included.
- LCSWs must provide the revised NPP to new patients. LCSWs should have the revised NPP available for existing patients in the LCSW's office and on his or her web site.

"Minimum Necessary" Information

The concept of "minimum necessary" is an important one in HIPAA standards. From 2003 to the present, minimum necessary has meant that when you disclose information without an authorization to do so, you must disclose only the "minimum necessary" information to fulfill the intent of the disclosure. This means you must be careful to limit the information you disclose and not provide more information than is being asked for. As we move toward "meaningful use," the adoption of electronic health records and personal health records, "certified" health care records, etc., the definition of "minimum necessary" may become more restricted (see below).

The minimum necessary standard does not apply to disclosures of PHI to health care providers for treatment purposes or to requests by a provider for information related to treatment. For example, the disclosure of PHI from one clinician to another is not subject to the minimum necessary requirement. However, the minimum necessary standard does apply to disclosures related to billing and collection of payment for services provided. Finally, "minimum necessary" does not apply to disclosures where there is a valid authorization to release information in addition to the TPO exception.

Business Associates

As of September 23, 2009, Business Associates are directly regulated by HIPAA. As of February 10, 2010, Business Associates are liable for breaches of PHI and ePHI directly. Prior to this date, Business Associates were only regulated indirectly through the Covered Entity. This change means that Business Associates are equally responsible for HIPAA violations with Covered Entities. Nonetheless, Covered Entities should still ensure that they enter into a Business Associate Agreement with each of their Business Associates.

The HITECH Act Rules require that such Business Associate Agreements contain new language, including requirements for the Business Associates to comply with the HIPAA Security Rule, breach notification requirements, assurance that subcontractors of the Business Associate comply with HIPAA, and requirement for the Business Associate to comply with the HIPAA requirements on the LCSW to the extent that the Business Associate carries out an obligation of the LCSW under HIPAA.

Although not required by HIPAA, it is advisable for LCSWs to also require each Business Associate to indemnify LCSWS from damages resulting from the Business Associate's failure to comply with HIPAA, ensure that the Business Associate has the responsibility to bear the costs of breach notice and mitigation, and finally provide the LCSW with the ability to recover any costs incurred by the LCSW arising out of the Business Associate's failure to comply with HIPAA.

The HIPAA Privacy Rules contains a two part definition of Business Associate. First, a Business Associate is a person who performs a function or activity on behalf of a Covered Entity involving the use or disclosure of PHI including: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; re-pricing; or any other function or activity regulated by the Privacy Rule.

Second, the definition of Business Associate includes persons who provide legal, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to the Covered Entity where the provision of such services involves the disclosure of PHI.

The definition of Business Associate excludes employees, volunteers and other members of the Covered Entity's workforce. The Privacy Standards also specifically exclude from the definition of "Business Associate" disclosures of PHI or ePHI from a Covered Entity to a health care provider when the purpose of the disclosure is for treatment of an individual. Further, a Covered Entity will not be considered a Business Associate of another Covered Entity to the extent that both entities are engaged in an organized health care arrangement.

In commentary published with the Privacy Standards, the Department of Health and Human Services (HHS) clarified that it will not require a Covered Entity to enter into a Business Associate Agreement with a person or organization that acts merely as a conduit for PHI or ePHI, such as the US Postal Service; a financial institution that engages in consumer- conducted financial transactions by debit, credit or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or effects the transfer of funds for compensation for health care; or private couriers and their electronic equivalents. The determination of whether a particular person or entity is a Business Associate is more about the function or service provided than the title or profession of the person or entity.

If the service or function does not involve the use or disclosure of PHI or ePHI, the person or entity is not a Business Associate. Disclosures of PHI or ePHI may be made to Business Associates only when a Business Associate Agreement is in place. HIPAA regulations also require that you take remedial action against any Business Associate who does not live up to the agreement. HIPAA allows disclosure of PHI or ePHI without such an agreement between Covered Entities for the specific purposes of treatment, payment, or healthcare operations. This means you can generally disclose PHI to a mental health consultant or supervisor, health plan, insurance company or clearinghouse without needing a Business Associate Agreement (BAA).

Be sure to have those who you identify as Business Associates sign the Business Associate Agreement as soon as you become a Covered Entity.

Administrative Requirements—Privacy Official, Complaints and Grievances

All Covered Entities must designate a **Privacy Official** who is responsible for the development and implementation of HIPAA policies and procedures as well as a contact person or to receive complaints and provide further information about the Covered Entity's privacy practices.

For individual practitioners the choice of who to appoint is an easy one. In most cases, you must be the privacy officer and contact person for your practice. In situations where you may be in a small group practice the choice becomes a little more difficult. Who you chose will depend on several things.

First, if you are in a small group practice that has no affiliation other than sharing office space, it is best if each individual serve as his or her own privacy officer and contact person. This is especially true if each person in the practice reports income under his or her own Social Security number or tax ID number.

Second, if you are a small group that has incorporated under one tax ID number then you may choose to appoint one person to be the privacy officer and contact person. That person will need to be responsible for understanding HIPAA and making sure the group is in compliance. The designated employee must have a working knowledge of and familiarity with the regulations in order to properly analyze the HIPAA compliance issues that your practice may face. Each person in the group may also act as their own privacy officer. It is important to have appropriate safeguards to protect PHI and ePHI and reasonably safeguard it from any intentional or unintentional disclosure or other use. Such practices as placing PHI in locking file cabinets, limiting conversations to private locations, establishing security policies for ePHI, being aware of how you answer the telephone, handle and transport files, fax and talk on cell phones are all things you can do to limit the unintentional disclosure of PHI.

Furthermore, you should assure that if your computer contains ePHI that you use logins and passwords to gain access to it. Your computer should be in a secure location, as should your written records. Any person who believes that you are not complying with HIPAA requirements may file a complaint with the Secretary of HHS (see Appendix 7). If you have employees, you must have policies in place that detail sanctions for those who do not comply with your privacy policies and procedures. Finally, you must establish a process for both clients and employees to make complaints regarding policies and procedures. You may not intimidate, threaten, coerce, discriminate or retaliate against any client or employee making a complaint.

You must develop and implement policies and procedures that are designed to comply with the requirements of HIPAA. Furthermore, you must revise your policies and procedures when there are changes in the law or when there are changes in your NPP. You are required to keep copies of all your policies, even if they change, for at least six years from the date they are written or the date they were in effect, whichever is later. This way, you can refer back to what your policies were at any given time should there be a complaint filed against you. One of your policies must be that you cannot require a client to waive his or her right to file a complaint as a condition of treatment.

The compliance date for all the above was April 14, 2003, if you were a Covered Entity or have become one since this date. If you are not a Covered Entity, the minute before you become one, i.e., send any information electronically that is a covered transaction, you must be fully HIPAA compliant.

What is a Breach?

A “breach” is defined to mean, generally, the unauthorized acquisition, access, use, or disclosure of unsecured protected health information in a manner not permitted under HIPAA unless the CE or BA, as applicable, demonstrates that there is a low probability that the PHI has been compromised. A breach is a legal violation of HIPAA Rules, whether intentional or unintentional, though there is a range of probable harm. Breaches are one of the most serious violations that HIPAA enforces.

Breach Notification for Unsecured Protected Health Information

The rules for notifying patients of breaches of unsecured protected health information apply to HIPAA Covered Entities and their Business Associates and require these Covered Entities and Business Associates to provide notification to affected individuals and to the Secretary of HHS. In addition, the rules requires Covered Entities to provide immediate notification to the media and to the Secretary of HHS of breaches of more than 500 individuals.

The general rule is that a Covered Entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the Covered Entity to have been, accessed, acquired, used, or disclosed as a result of such a breach.

Some Examples of Breaches (see Appendix 3, p. 73)

- Inappropriately accessing a health care record of a client (electronically or paper record)
- Sending unencrypted email with PHI to the wrong recipient
- Losing a CD or flash drive with client information that is not encrypted
- Faxing or mailing health care records to the wrong place or recipient
- Sending mobile data that is not encrypted to the wrong recipient, e.g., using smart phones
- Sending one client's information to another client (e.g., including a copy of a record co-mingled with another record).

Breach Exceptions

- Any unintentional acquisition, access, or use by PHI by a workforce member of a Covered Entity or Business Associate if the release was made in good faith and does not result in further use or disclosure, e.g., employee without authorization accidentally viewed PHI without authorization.

- 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 PHI is not further used or disclosed in a manner prohibited by HIPAA.

- A disclosure of protected health information 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.

HHS/OCR has had over has had over 90,000 complaints of PHI or ePHI violation since 2003 with a steady rise in the number of complaints over the years and the number of investigations by Office of Civil Rights. There have been over 22,000 investigations where PHI or ePHI information was "breached" and disclosed without patient authorization when not released for TPO purposes, resulting in enforcement through financial penalties. This fact illustrates that PHI/ePHI breaches are becoming more common and/or being reported more fully. The largest group of Covered Entities found to be in violation of protecting PHI or ePHI are private practitioners, a cautionary figure for LCSWs (see Appendix 9). Physical security of records continues to be a major problem, as does the loss of PHI and ePHI.

What is Unsecured PHI?

"Unsecured PHI" is defined as "PHI that is not secured through the use of a technology or methodology specified by the Secretary in guidance." This "guidance" specifies the types of "technologies and methodologies" that render PHI unusable, unreadable, or indecipherable to unauthorized individuals. Covered Entities and Business Associates that implement these technologies and methodologies are not required to provide notifications in the event of a breach of such information—that is, the information is not considered "unsecured" in such cases.

Encryption (the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key) and destruction (shredding in the case of paper, film or other hard copy media, and in the case of electronic media, cleared, purged or destroyed consistent with National Institute of Standards and Technology (NIST) Publication 800-88, such that the PHI cannot be retrieved) are the two technologies and methodologies for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals.

Covered Entities can be in compliance with the Security Rules and not encrypt their electronic PHI. However, if firewalls are breached and the information is not encrypted, the breach notification requirement must be met. If firewalls are breached and the information is encrypted, there may be no need to follow the breach notification procedures if the information is properly rendered unusable. Encryption keys are to be kept on separate devices from the data they encrypt. Redaction of paper records is not an accepted alternative to secure paper-based PHI, only destruction. However, redacted information may meet the definition of de-identification and therefore a release of redacted information may not require notification because it is no longer PHI.

What are the Penalties for PHI and ePHI Breach?

DHHS and OCR in 2014 established four new tiers of penalties for PHI and ePHI as follows:

Category	Each Violation
Unknowing Violation of HIPAA	$100 – $50,000
Reasonable Cause to Know Violation	$1,000 – $50,000
Violation Result of Willful Neglect and was Later Corrected	$10,000 – $50,000
Violation Result of Willful Neglect and was not Corrected	At least $50,000

Maximum penalties for violations of the same HIPAA provision is $1.5 million per year

How is a Breach Determined and is Notification Necessary?

To determine if an impermissible use or disclosure of PHI constitutes a breach, Covered Entities and Business Associates must analyze the following four factors (as explained in the HITECH final rule) to determine whether there is a low probability that the PHI has been compromised.

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

To assess this factor, entities should consider the type of PHI involved in the impermissible use or disclosure, such as whether the disclosure involved information that is of a more sensitive nature. For example, with respect to clinical information, this may involve considering not only the nature of the services or other information but also the amount of detailed clinical information involved (e.g., treatment plan, diagnosis, medication, medical history information, test results).

(2) The unauthorized person who used the PHI or to whom the disclosure was made.

Entities should consider whether the unauthorized person who received the information has obligations to protect the privacy and security of the information. For example, if PHI is impermissibly disclosed to another entity obligated to comply with HIPAA, there may be a lower probability that the PHI has been compromised since the recipient of the information is obligated to protect the privacy and security of the information in a similar manner as the disclosing entity

(3) Whether the PHI was actually acquired or viewed.

For example, if a laptop computer was stolen and later recovered and a forensic analysis shows that the PHI on the computer was never accessed, viewed, acquired, transferred, or otherwise compromised, the entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed. In contrast, however, if a covered entity mailed information to the wrong individual who opened the envelope and called the entity to say that she received the information in error, then, the unauthorized recipient viewed and acquired the information.

(4) The extent to which the risk to the PHI has been mitigated.

Covered entities and business associates should attempt to mitigate the risks to the PHI following any impermissible use or disclosure, including obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed, and should consider the extent and efficacy of the mitigation when determining the probability that the PHI has been compromised.

A Covered Entity must retain extensive documentation of the breach assessment and response to the breach because, if it decides not to notify the patient, it bears the burden of demonstrating that there was a low probability that the PHI was compromised.

Notification to Individuals

Covered Entities are required to notify each individual whose unsecured protected health information has been, or believed to have been, accessed, acquired, used, or disclosed as a result of a breach.

Timeline

Once a breach has been discovered, or reasonably should have been discovered, a Covered Entity must inform affected individuals without unreasonable delay and no later than 60 days from the date of the discovery of the breach.

Content of Notification

The following information should be included in the notification to individuals whose unsecured PHI has been released, and must be written in plain language:

- A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

- A description of the types of unsecured protected health information that were involved in the breach (such as name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information);

- Any steps individuals should take to protect themselves from potential harm resulting from the breach;

- A brief description of what the Covered Entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

- Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

How to Notify Individuals

Notification to affected individuals must be in the following form:

- Written notification by first-class mail to the individual (or in the case of minors, their parent or guardian) at the last known address of the individual or, if the individual agrees, by electronic mail.

    - The notification may be provided in one or more mailings as information is available.

        - If you have out-of-date information for less than 10 individuals, you must still contact them by an alternative method such as phone, or email and make every effort to find current contact information.
        - If you have out-of-date information for 10 or more individuals, you must develop substitute methods of notice (such as postings on your website for at least 90 days, or conspicuous notice in major print or broadcast media, and a toll free number for further information for at least 90 days) as soon as possible.
        - Care should be taken to limit the information left on such things as answering machines when using alternative forms of communication (minimum necessary).

- If the Covered Entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual, the Covered Entity must provide written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available. You are not required to contact next of kin if you do not have contact information.

- In any case deemed by the Covered Entity to require urgency because of possible imminent misuse of unsecured protected health information, the Covered Entity may provide information to individuals by telephone or other means, as appropriate, in addition to the methods listed above.

- For a breach of unsecured protected health information involving more than 500 individuals, a Covered Entity is required to notify prominent media outlets serving the area as soon as possible and no later than 60 days.

Notification to the Secretary of Health and Human Services

Following the discovery of a breach, Covered Entities must notify the Secretary of Health and Human Services.

- For breaches involving 500 or more individuals, the Secretary must be notified immediately (no later than 60 days).
- For breaches involving less than 500 individuals, the Covered Entity may maintain a log of breaches and submit the log annually (calendar year) to the Secretary.

Notification by a Business Associate

Following the discovery of a breach of unsecured PHI, a Business Associate is required to notify the Covered Entity of the breach as soon as possible and no later than 60 days following the discovery, so that the Covered Entity can notify affected individuals. The Business Associate is to provide:

- The identification of the individual(s);
- Any other available information that the Covered Entity is required to include in the notification to the affected individuals.

Since September, 2013, complaints may be filed against Business Associates directly by Covered Entities or others who believe PHI or ePHI breaches have occurred.

Administrative Requirements

Covered Entities are required to:

- Comply with the law;
- Show that all notifications were made as required or that a breach was not made;
- Train members of its workforce on the policies and procedures developed for this rule;
- Provide a process for individuals to make complaints concerning the Covered Entity's policies and procedures;
- Have and apply appropriate sanctions to members of its workforce who fail to comply to the policies and procedures;
- Not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual who files a complaint or exercises any other right under this rule;
- Implement policies and procedures designed to comply with these standards;
- Change its policies and procedures as necessary and appropriate to comply with changes in the law;
- Maintain documentation sufficient to meet its burden of proof under this rule.

Covered Entities may not:

- Require individuals to waive their rights as a condition of the provision of treatment.

Law Enforcement Delay

If a law enforcement official determines that a notification of a breach would impede a criminal investigation or cause damage to national security, the Covered Entity or Business Associate shall delay the notification.

- If the statement is in writing and specifies the time for which the delay is required, the Covered Entity is required to follow the time delay written into the notice.

- If the statement is made orally, the Covered Entity should document the statement, the identity of the official and delay the notification for no longer than 30 days or until a written document is obtained with a different withholding period.

Preemption of State Law

HIPAA regulations apply in every state. There are situations throughout the country where HIPAA conflicts with certain aspects of state law. In those circumstances, state laws that are more stringent than HIPAA regulations take precedence with certain restrictions. A state law is determined to be more stringent when it:

- Prohibits or restricts a use or disclosure that the regulation would permit;
- Grants greater rights of access or amendment to an individual's own PHI;
- Provides for a greater amount of information to be disclosed to an individual upon request;
- Requires more narrowly focused or limited consents or authorization;
- Requires more detailed record keeping; or
- Provides any other greater privacy protection.

The restrictions to the general rule that more stringent state laws take precedence are when the Secretary of HHS determines that the state law or regulation is:

- To prevent fraud and abuse related to the provision of or payment for health care;
- To ensure appropriate state regulation of insurance and health plans to the extent expressly authorized by statute or regulation;
- For state reporting on health care delivery or costs; or
- For purposes of serving a compelling need related to public health, safety, or welfare, or if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served

Compliance and Enforcement

Covered Entities should be prepared to provide accurate documentation of all HIPAA policies, forms, etc. in case a client or anyone else files a complaint with the Office of Civil Rights. These records will be necessary to enable the OCR to determine whether or not you have complied with HIPAA regulations. If a complaint is filed, your responsibility is to cooperate with the investigation in the review of your policies and procedures. You must permit access by OCR representatives during regular business hours to your:

- Books,
- Facilities
- Records,
- Accounts and other sources of information, and
- PHI and ePHI.

This access is to determine if you are in compliance with HIPAA regulations. If OCR determines that you are hiding or destroying information, you must permit access at any time without notice. If you have a complaint filed against you and an audit is planned, you should notify your legal counsel.

Your Employees

Just as you are required to be aware of all HIPAA regulations, any staff you have, including office managers and administrative staff, must know and abide by HIPAA regulations. HIPAA requires that you train your staff members at the time of hiring or in preparation for HIPAA implementation and annually after that. You must also have employees sign documentation of completion of initial and updated training. You should keep records of attendance of all training and assure that all staff are trained and updated.

Your employees should be familiar with the circumstances that allow for the Disclosure of PHI without Authorization. Develop detailed policies outlining each of these uses and disclosures with elements necessary for compliance. Similarly, your employees should have an understanding of the concept of "minimum necessary" when it comes to the disclosure of PHI. If you have administrative staff for billing purposes, ensure that they do not have access to PHI or ePHI, other than what is necessary to do their job. Use passwords and logins to protect ePHI stored in computers. Think of examples where you can apply the concept of minimum necessary. Ensure that your policies include procedures for dealing with infractions and enforce the policies if infractions occur. Make sure staff are aware of the penalties for violations of HIPAA regulations.

Just as you may not threaten a client for making a report, you also may not intimidate, threaten, coerce, discriminate or retaliate against an employee for doing so. Encourage your staff to be on the lookout and report non-compliance with HIPAA. All staff should be encouraged to understand the regulations and make decisions based on that understanding. Employees can choose not to engage in any action they, in good faith, believe to be illegal or contrary to HIPAA regulations. If you are investigated, employees cannot be punished for cooperating with the investigation You must also have appropriate safeguards to protect PHI from either intentional or unintentional disclosure. Train your staff in the importance of confidentiality practices when answering the telephone, handling files, faxing, talking in public places etc. Make sure that computers are secured and password protected.

Train staff on the HIPAA implementation deadlines. Make sure they understand the disclosure rules both before and after the April 14 deadline. If HHS audits you, assure that your staff is aware of their obligation to cooperate with HHS by permitting access to information and exhibiting cooperation in all phases of the investigation.

Patient Rights

The HIPAA Privacy Standards grant new federal rights to patients with respect to health information about them. These include the right to receive a health care provider's Notice of Privacy Practices, and the opportunity to object or opt-out of certain types of communications including disclosures for marketing or fundraising purposes. However, we recommend that PHI or ePHI only be released for TPO purposes. The Privacy Standards also provide individuals the right to access PHI or ePHI, the right to request amendments to PHI or ePHI, and other rights. One of the things HIPAA attempts to do is make it easier for individuals to access their PHI. As such, clients have the right to inspect and copy their PHI and ePHI, in whole or in part, for as long as you maintain the information. There are some special rules set aside for "Psychotherapy Notes" which we have addressed below.

Clients also have the right to have you amend their record for as long as you maintain the information. You must accommodate reasonable requests by clients to receive information about their PHI or ePHI by alternative means or at alternative locations. A client has the right to receive an accounting of disclosures you or your Business Associates make of PHI or ePHI in the six-year period preceding the date on which the accounting is requested. This begins on April 14, 2003, and is not retroactive before that date. There are, however, a number of broad exceptions to the accounting requirement including the following disclosures: to carry out treatment, payment or health care operations; 2) to the individual; and 3) pursuant to a valid authorization as permitted by HIPAA. These exceptions are so broad that, generally, in practice, the clinician must only keep records of any disclosures made for court- ordered purposes or public health reasons.

Finally it is important to note that under HIPAA a client has the right to request that a clinician agree to additional restrictions on uses and disclosures of information that go beyond what the Standards require. Although a clinician is not required to agree to such restrictions, if a clinician does agree, he/she must document and comply with that agreement. As noted earlier, according to HIPAA standards a patient cannot request the restriction of TPO information. Unless the patient is willing to forgo the use of insurance for reimbursement, such information must be provided.

Authorization Forms

Authorization Forms are what most clinical social workers have previously called Release of Information forms. HIPAA standards do not require an Authorization Form be signed whenever PHI or ePHI is released, but we recommend having the patient do so as part of best practices.

The HIPAA standards require that specific information be included in the Authorization form. This includes 1) a definition of the information being disclosed; 2) identification of who will receive the information; 3) the purpose of the disclosure; 3) an expiration date; 4) the right to revoke; and 5) refusal to allow PHI to be disclosed. The Authorization form must also include the patient's acknowledgement of the clinician's NPP, the minimum information necessary principle, and the way that TPO is managed.

Medical Record

The Medical Record must include all of the following information, as applicable:

- Intake information;
- Billing information;
- Formal evaluations;
- Notes of collateral contacts;
- Records obtained from other providers;
- Counseling sessions start and stop times;
- The modalities and frequencies of treatment furnished;
- Medication prescribed, if known; and
- Any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

Psychotherapy Notes

Psychotherapy Notes are specifically defined in the HIPAA Rules and there are additional protections for them. The general rule is that a clinician may not use or disclose Psychotherapy Notes for some purposes, including most treatment, payment and healthcare operations, unless the client's authorization is obtained. Specific exceptions where an authorization is not required include use by the originator of the notes for treatment, supervision and training purposes; uses for defense in a legal action; when needed to avert an imminent threat; and needed by a coroner/medical examiner.

While the clinician is not required to show the patient the Psychotherapy Notes, there is nothing in the Rule that prohibits such a practice. If a clinical social worker wishes to have the protection afforded Psychotherapy Notes, Psychotherapy Notes must be physically separate from the rest of the client's record.

If a clinical social worker decides to maintain separate Psychotherapy Notes, all of the excluded material listed above would be maintained in the primary client file or "Medical Record," while the Psychotherapy Notes would be kept elsewhere. Any summary of diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date. At a minimum, Psychotherapy Notes must be kept in a different part of the client's file. State law regarding mental health records may also apply.

We will now turn to the changes that will allow you to become fully HIPAA compliant, including assessment of current privacy practices, new forms, and new practices which will be needed.

Changes to HIPAA

[N.B.: Information in italics is commentary by the authors on how these changes to HIPAA affect LCSWs currently, or possibly in the future. Not all these changes will affect LCSWs immediately.- L.W.G. and R.K.M.]

Sale of PHI

The HITECH Act prohibits Covered Entities from selling a patient's PHI. However, there are a number of exceptions to this rule, including: (1) public health activities; (2) certain research purposes, (3) treatment of the individual; (4) sale, merger or consolidation of a Covered Entity; (5) services rendered by a Business Associate under a Business Associate Agreement, (6) providing the individual with a copy of his or her PHI; or (7) other reasons determined necessary and appropriate by the Secretary.

Marketing

Under HIPAA, a Covered Entity must obtain a patient's authorization for any use or disclosure of the patient's PHI for the purpose of marketing a product or service to a patient. Two exceptions to this rule are if the communication is: (1) a face-to-face communication made by a covered entity to an individual; or (2) a promotional gift of nominal value provided by the covered entity.

The HITECH Act clarified additional exceptions to the definition of "marketing," including: (1) refill reminders or other communications about a drug or biologic that is currently being prescribed for the individual (if any remuneration is received, it must be reasonable related to the Covered Entity's cost in making the communication); (2) treatment of an individual by a health care provider, including case management or care coordination for the individual, direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; (3) to describe a health-related product or service that is provided by, or included in a plan of benefits of, the covered entity making the communication; or (4) case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions.

For LCSWs, these changes will have minimal direct meaning, as we rarely, if ever, sell patient information or market products to patients. The greater likelihood is that a Business Associate may sell patient information, adding to the importance of our clarifying the responsibilities of any Business Associate to abide by HIPAA requirements and our own policies and procedures.

Fundraising

There has been significant concern among LSCWs about the new requirement that NPPs contain a section on fundraising. This requirement was created as a result of complaints being filed about medical records used for this purpose. This is a rare, if ever, practice by LCSWs, but HIPAA covers the whole of Covered Entities, many of whom, through foundations or Business Associates, engage in fundraising.

The following PHI ePHI may be used for fundraising purposes with patient knowledge, if an LCSW decides to engage in fundraising:

- Demographic information
- Dates of treatment
- Department of treatment (hospitals)
- Treating physician
- Health insurance status
- Outcome information

LCSWs must give patients the right to opt out of any fundraising communications, unless the LCSW's policy is to never release PHI or ePHI for fundraising purposes. Of course, this would be communicated to Business Associates who would be bound by this policy.

Electronic Health Records

Currently, there are no requirements for LCSWs to maintain electronic Health Records (EHRs). However, the possibility that LCSWs may need to develop EHRs in the near future exists; therefore, we are including information on this topic.

The major goal of EHRs is to prevent duplication of needed treatment and have all health records available to all providers, including mental health clinicians, who are treating a given patient. For LCSWs, the information which should be included in the EHR is what is included in the Medical Record.

Another major goal of EHRs is to give the providers a more comprehensive understanding of their patients; they represent a monumental change in the way that health care providers communicate with each other. Interoperable provider communication is moving from being a best practice, to becoming a requirement for reimbursement. However, as noted above, LCSWs are not required at this time to include their records in EHRs at this time.

Personal Health Records

There is another major shift in the way that patients' records are kept, i.e., the creation of a type of EHR that an individual patient controls, called Personal Health Records (PHRs). Examples of PHR systems include Google Health and Microsoft Health Vault.

PHRs are intended to give the patient more information about their health care and more self-determination regarding the health care treatment(s) that he or she receives. PHRs represent a revolutionary change from the past, when doctors and other health care providers were considered experts whose control of health care decision-making was absolute. Now patients will be expected to have more understanding of the health care treatment they need and more responsibility for the choices that they make in collaboration with their doctor or clinician. This principle is not a major change for LCSWs who have always seen patient self-determination, including self-determination about participation in mental health treatment, as a given.

The implementation of Personal Health Records is voluntary at this point in time and will not be required, though the principle is a fundamental part of HITECH changes. LCSWs are not required to maintain records in PHRs at this time.

The HITECH Act – Incentivizing EHR Adoption

In order to accelerate the pace of EHR adoption, Congress passed the Health Information Technology for Economic and Clinical Health (HITECH) Act in March, 2010, which was part of the American Recovery and Reinvestment Act (ARRA). The HITECH Act contains Medicare and Medicaid "incentives", or financial underwriting, for providers who adopt "certified" EHRs (see below) and use such technology in a "meaningful way," also called "meaningful use" (see below).

Currently LCSWs and psychologists are not included as "eligible professionals" who may receive incentive payments, but legislation is pending to make LCSWs and psychologists eligible providers. Federal bills pending in House of Representatives and the Senate (H.R. 5040/S. 3709) would extend Medicare and Medicaid incentive payments for the adoption and meaningful use of health information technology to the currently ineligible behavioral health providers and facilities.

The Medicaid incentives are also spread out over a period of six years, but providers have until 2016 to begin the meaningful use of an EHR system.

Although licensed clinical social workers do not qualify as "eligible professionals" for the HITECH Act incentives, CSWA and other behavioral health groups are supporting legislation that would extend the incentives to licensed clinical social workers and other mental health and substance abuse providers and facilities. Beginning in 2015, Medicare reimbursementswill be reduced for eligible providers who fail to meaningfully use certified EHRs, currently not applicable to LCSWs.

Certification

In order to receive Medicare or Medicaid incentives under the HITECH Act, providers must use a "certified" EHR system. Under the Office of National Coordinator for Health Information Technology (ONC) criteria, certain organizations will be designated by the ONC as Authorized Testing and Certification Bodies (ATCBs). ATCBs are responsible for testing EHR systems to determine whether they meet minimum functional requirements. To date, ONC has designated five organizations as ATCBs, but more are soon to follow. Providers should ensure that the EHR systems that they purchase from vendors have been properly certified by an ATCB. Currently LCSWs are not required to use certified electronic health records, but this may change in the future; knowledge of the use of electronic health records is considered a best practice.

Meaningful Use

In addition to the requirement of using "certified" EHR systems, providers will receive Medicare and Medicaid incentive payments only if they "meaningfully use" the EHR technology. The definition of meaningful use involves three different stages that providers have to comply with by certain deadlines; only Stage 1 standards are currently in place. Each subsequent stage increases the requirements on providers to ensure that the EHR system is fully integrated into business operations.

There are two primary ways that Meaningful Use is defined currently: "Stage 1" objectives and "A la Carte" objectives for Stage 1. For example, to achieve compliance with Stage 1, providers will have to meet all appropriate objectives that focus on improving quality, safety, efficiency, engaging patients and families in health care, improving care coordination, and improving public health. Only five "A la Carte" objectives will need to be implemented to meet meaningful use standards. All Stage 1 and A la Carte objectives which potentially apply to LCSWs are italicized below. Currently LCSWs are not required to use certified electronic health records, but this may change in the future; knowledge of the use of EHRs is considered a best practice.

Stage 1 objectives include the following:

- Use computerized provider order entry (CPOE) for medication orders
- Implement drug-drug and drug-allergy interaction check
- Maintain an up-to-date problem list of current and active diagnoses
- Generate and transmit permissible prescriptions electronically (eRx)
- Maintain active medication list
- Maintain active medication allergy list
- Record patient demographics (sex, race, ethnicity, date of birth, gender, preferred language, and in the case of hospitals, date and preliminary cause of death in the event of mortality)
- Record vital signs and chart changes (height, weight, blood pressure, body mass index, growth charts for children)
- Record smoking status for patients 13 years of age or older
- Report ambulatory clinical quality measures to CMS (Medicare) or states (Medicaid)
- Implement one clinical decision support rule and ability to track compliance with the rule
- On request, provide patients with an electronic copy of their health information (including diagnostic test results, problem list, medication list, medication allergies, and for hospitals, discharge summary and procedures)
- For individual professionals , provide patients with clinical summaries for each office visit; for hospitals, provide an electronic copy of hospital discharge instructions on request
- Implement capability to electronically exchange key clinical information among providers and patient-authorized entities
- Implement technical systems to protect privacy and security of patient data in the EHR

"A la carte" objectives for Stage 1 (provider must implement five to meet Meaningful Use standard):

- Implement drug formulary checks
- Incorporate clinical laboratory test results into EHR as structured data
- Generate lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, or outreach
- Send reminders to patients per patient preference for preventive/follow-up care
- Provide patients with timely electronic access to their health information within 4 business days of the information being available to the EP
- Use EHR technology to identify patient-specific education resources and provide to the patient as appropriate
- Perform medical reconciliation between care settings
- Provide summary of care record for patients referred or transitioned to another provider or setting
- Submit electronic immunization data to immunization registries or immunization information systems
- Submit electronic surveillance data to public health agencies

In order for providers to receive incentives in 2012, they will have to achieve Stage 1 compliance by their first and second payment years (2012 and 2013).

To ensure that the monetary incentives of the HITECH Act are used in accordance with the HITECH Incentives, Congress has delegated oversight authority to the following federal agencies: (1) the Office of the National Coordinator (ONC), which is responsible for drafting certification criteria to ensure that EHR systems meet basic functionality requirements, and the Centers for Medicare & Medicaid Services, which is responsible for drafting guidelines that define what it means for a provider to "meaningfully use" an EHR System.

Mental Health Records in EHRs/PHRs

The inclusion of mental health records in EHRs/PHRs may be a problematic issue for LCSWs. While CSWA supports the inclusion of mental health information in records in which privacy has been clearly established, there are concerns about the ability of ONC, ATCB, and other governmental entities to guarantee the privacy of mental health records in EHR systems within the HITECH Act timelines that now exist, i.e., Stage 1 starting by January, 2011 to receive the maximum incentive payments.

On the other hand, LCSWs who would like to purchase an EHR system may need the HITECH Act incentives in order to afford the purchase. The ONC has designed the payments to cover the average five-year start-up cost for EHR Systems, which is $44,000. This would be a substantial burden for most LCSWs without the HITECH Act incentives. The Murphy Bill includes funding for mental health EHR systems which could be passed this year.

Health Homes/Medical Homes and ACOs – Integrated Care

Another aspect of the use of EHRs is the creation of virtual or actual "Health Homes," sometimes called "Medical Homes." The intent is to have ongoing communication through EHRs between all practitioners for a given patient and to provide patients with access to all information about his or her medical conditions through EHR/PHR technology. Funding for Health Homes is capitated, leading to choices about treatment covered. The primary area where Health Homes are being implemented at this time is in Medicaid programs.

Accountable Care Organizations (ACOs) are another kind of integrated care which differ from Health Homes in having a profit and loss component built in, i.e., reimbursement rates are affected by the overall profits of the ACO. ACOs are overseen by the ONC and must have at least 5000 enrollees. The role of EHRs remain the same, i.e., to have a consolidated record for each patient available to all providers involved with a patient and the patient.

The HITECH Act will play an important role in helping to facilitate the adoption of EHRs that are essential to medical homes. Again, there is cause for concern because the privacy of mental health information might not be able to be guaranteed in all systems, and patients could have access to their own records without adequate explanation.

ICD-10 Implementation

The Department of Health and Human Services (HHS) has mandated the replacement of the ICD-9-CM code sets used to report health care diagnoses and procedures with ICD-10 code sets, effective Oct. 1, 2014.

ICD-10 implementation will radically change the way diagnostic coding is currently done; the code-set will grow from its current 17,000 codes to more than 141,000, and the format is new with seven alpha-numeric codes instead of five numeric digits. These dramatic changes, and others, will require very significant changes to the way that LCSWs identify diagnostic codes. CSWA will have a training on the changes to diagnostic codes later this year. Anyone who has the DSM-5 will note that there are two codes for each diagnostic category. The first is the ICD-9 codes currently in use. The second is the ICD-10 code that will replace the code on October 1, 2014.

Developing HIPAA Compliant Practices

There are seven major changes that Covered Entities will need to consider and/or implement that may not be part of your current standard practices to become compliant with HIPAA Privacy and Security Rules. These include:

1. Developing a Notice of Privacy Practices explaining the ways PHI and ePHI are protected in principal;

2. Devising "reasonable" ways of protecting information sent electronically, or security practices, including conducting a Risk Assessment and Risk Management Plan (see Matrix below);

3. Appointing a privacy and security officer (a sole practitioner is also the privacy and security officer) and developing a document on Privacy Practices or how PHI is actually protected and/or disclosed in practice based on the "minimum necessary" disclosure of information;

4. Developing Business Associate Contracts which allows information to be shared by a Covered Entity and a non-Covered Entity;

5. Creating a HIPAA-compliant Authorization Form for the disclosure of PHI and ePHI;

6. Keeping two sets of records should be considered, one containing relevant disclosable PHI or ePHI about a case, and the other being Psychotherapy Notes. In addition, you will want to conduct an internal review of your current privacy and security practices. Many clinicians may be complying with HIPAA regulations in part but need to adjust their privacy and security procedures to fully comply with HIPAA regulations. The GAP Internal Review and Risk Management Assessment will be described below.

7. Having clear breach policies to notify patients if their PHI or ePHI is disclosed without prior approval or for TPO purposes by you or your Business Associate.

Developing and Implementing a Notice of Privacy Practices (NPP)

The privacy requirements of HIPAA provide new patients with a Notice of Privacy Practices (NPP) which details the ways you protect PHI and under what conditions you will release information about them without getting a signed Authorization form. A signed statement that the patient received the NPP must be kept on file at your office. If you practice in a state that requires a Disclosure Statement be given to patients at the first meeting, you may want to incorporate NPP requirements into the Disclosure Statement. Details of what must be included in the NPP can be found below.

Business Associates Contract

This document applies to relationships between a practitioner and a non-Covered Entity such as an administrator, collection agency, accountant, secretary, etc. This document guarantees that there is agreement by the Business Associate to conform to the Privacy Practices of the clinician.

Security Practices

It is prudent to take steps to protect all paper and electronic materials. HHS states that "reasonable attempts" to protect all forms of PHI should be taken. At this point in time, "reasonable attempts" include having paper records in locked files; sending electronic information that is not de-identified (see above) on a secure server such as WebMD, using a password computer only, checking for computer viruses every few days, or getting an encryption program such as PGP (which must be shared by anyone to whom you send PHI information electronically). In addition, all records should be reviewed and stored offsite or destroyed regularly. Finally, a Risk Management Assessment and Risk Management Plan must be developed.

Summary of Changes to Clinical Practice

Clinicians who do not use insurance or send information electronically to billing services may feel that the HIPAA Standards do not apply to them. However, these Standards are likely to become the de facto standard for all mental health clinicians, whether they are 'Covered Entities' or not. Below are listed the areas of HIPAA standards that differ from standard practice that all mental health clinicians may want to consider:

1. **Electronic Transmission of Patient Information** – clinicians must be HIPAA-compliant BEFORE any patient information is sent electronically (by computer, computer fax, or telephone key pad), This means that clinicians have created their own privacy Policies and Procedures; their Notice of Privacy Practices; their Business Associate Agreement; designate a Privacy Officer; 4) keep all records, paper and electronic, secured, i.e., locked file cabinets and password and/or encrypted computers; 5) develop Authorization and Revocation of Authorization Forms to allow release of protected health information.

2. **Disclosure Statements (NPP - Notice of Privacy Practices)** – while a handful of states already require a Disclosure Statement which details the clinician's privacy practices, the NPP makes this a requirement that includes specific information about when a clinician will or will not release patient information.

3. **Contracts with Business Associates (BAA - Business Associate Agreement)** – while some prudent clinicians may already have contracts with non-clinicians who have access to patient material (PHI), the majority of clinicians do not. HIPAA standards will require all non-clinicians – "Business Associates" – who have access to PHI to have a contract with the clinician on how and when they can release the PHI.

4. **Psychotherapy Notes Protection** – if a clinician wishes to have the protections the "Psychotherapy Notes" section of HIPAA standards offers, a separate record will have to be maintained from the record that contains TPO (treatment, payment and health care operations) information.

5. **Secure Faxes** – to assure faxed material is going to a fax machine where privacy can be maintained, a clinician should ask the recipient if the receiving fax is a "secure" or "protected" fax machine.

6. **Privacy GAP Analysis** – for clinicians who wish to be HIPAA compliant (and all prudent clinicians should work toward this goal), a Privacy GAP analysis of current privacy practices should be done to assure all areas of compliance are being addressed.

7. **Security Risk Assessment** – for clinicians who wish to be HIPAA compliant (and all prudent clinicians should work toward this goal), a Security GAP analysis of current security practices should be done to assure all areas of compliance are being addressed.

8. **Risk Management Plan** – development of a Security plan to make sure all HIPAA Security Standards are in place.

9. **Back up Mechanisms** – all ePHI must be 'backed up' on a disc or CD , or at an encrypted external website.

10. **Regular Changes to Passwords** – computer passwords must be changed regularly to comply with HIPAA Security Standards.

The following material will take you through the internal review of your current privacy and security practices and assess what does and does not conform to HIPAA requirements. We will then help you develop an Action Plan and Risk Management Assessment for how to implement the new practices and procedures necessary to comply with HIPAA rules.

[This page intentionally left blank.]

Action Plan

Becoming HIPAA Compliant

In order to understand the larger picture of HIPAA we encourage you to go to the websites listed below and become more familiar with the many facets of HIPAA. The list of websites is not an exhaustive list, but will provide you with good accurate information about all aspects of the regulation. Many questions may also be answered by simply reading the regulations.

An indexed copy of the regulations is available on the compact disc included with some versions of this manual or at http://www.hhs.gov/ocr/hipaa. In addition, other websites that carry up-to-date information about HIPAA include: http://aspe.hhs.gov/admnsimp/; http:// snip.wedi.org/; http://www.hipaadvisory.com/; http://www.nchica.org/HIPAAResources/ regulations.htm.

The privacy and security regulations impose extensive and specific documentation requirements on Covered Entities. For example, a Covered Entity must retain signed authorizations, copies of the notices of privacy practices, and any agreements with patients restricting disclosure of PHI. In addition to meeting these specific requirements, the Covered Entity should retain documentation to show that reasonable steps were taken to meet generalized and scalable standards imposed by HIPAA. Covered Entities should also document staff training, adoption of policies and procedures, and other efforts to comply with HIPAA. Two concepts that are important to understand are the ones of reasonableness and scalability. The federal government understands that HIPAA standards cannot cover all the situations that may arise in a complex health care system. What they ask is that you take “reasonable steps” to ensure privacy and security for protected health information. Since reasonableness has yet to be defined due to the newness of the regulation, we believe that if a clinician takes precautions and can provide a rationale for an action, no sanctions will be taken against that clinician. Scalability means that large, complex health care organizations will need to have large, complex policies and procedures to protect the massive amount of protected health information they possess. Likewise, small, individual practitioners with much less complex practices need only basic policies and procedures in place to accommodate HIPAA standards. As such, we have provided only those policies and procedures that we feel a small group or solo practitioner needs to comply with HIPAA.

Appoint and Train a Privacy Officer

All Covered Entities must designate a privacy official who is responsible for the development and implementation of HIPAA policies and procedures as well as a contact person to receive complaints and provide further information about the Covered Entity’s privacy practices.

Does this mean you must hire someone to serve as a privacy official? No. For solo practices/small offices, the privacy official may be the office manager, or the clinician him/herself. The requirement is that someone must be designated as the contact person with respect to HIPAA compliance. The designated person should be trained in the requirements imposed by the Privacy Standards, and empowered to apply and enforce such requirements in your practice.

Conduct an Internal Assessment

Once a privacy officer has been designated and trained, the essential next step is to conduct an internal assessment of existing policies, procedures, and practices for collecting and handling medical records and other patient information to determine where the gaps may be in a practice's ability to meet HIPAA standards. The following questions need to be answered:

- What information is collected from clients?
- Where is it stored?
- Who has access to it?
- What forms are currently used to obtain consent and authorization for necessary disclosures?
- With what third parties do you share protected health information?

Next the following questions must be asked and answered in order to identify risk areas and set priorities for further action. The following checklist may assist with your internal assessment efforts:

- **How are paper records containing PHI maintained?**
  Location:
  Security mechanisms:

- **How are electronic records containing ePHI maintained?**
  Location:
  Security mechanisms:

- **Who has access to paper or electronic records containing PHI or ePHI (list all individuals or organizations)?**
  For all the individuals listed above, indicate relationship (e.g. employee, contractor, etc.) and reason for permitting access.

- **Who receives PHI or ePHI from you (list all individuals or organizations)?**
  For all individuals listed above, indicate relationship and reason for disclosure.

- **Who has the right to modify or change PHI or ePHI in your practice?**

- **How is PHI or ePHI disposed of or destroyed?**

- **What policies (if any) do you currently have in place related to the confidentiality or use and disclosure of patient information?**

Once you have completed the process of documenting how PHI and ePHI flows into, within, and out of your office, you will be in a much better position to determine the steps you will need to take to close the gaps between your current practices and the HIPAA Privacy and Security Standards.

Prepare a Notice of Privacy Practices

To assure that clients know their rights, HIPAA requires that you provide clients a Notice of Privacy Practices (NPP) at the time of the first session, and maintain documentation that you provided the NPP. The NPP represents your public statement regarding how you will handle your client's health information. HIPAA not only requires that you post and provide this document to your clients, but also that you comply with its terms. Although you may choose to use a form such as the one provided in this Manual and on Disc to develop your NPP, it is critical that you take time to thoroughly review and understand the terms of your NPP, and make any changes in order to ensure the notice is consistent with your current practices and state law in your jurisdiction.

We have provided a sample Notice of Privacy Practices in this Manual and on Disc. We have provided a sample that has both required and optional parts. Most of the optional parts are less stringent than practices we suggest, yet are compliant with HIPAA regulations.

Business Associates

Business Associates are individuals or organizations that are themselves not Covered Entities but who may have access to your PHI. Disclosures of PHI may be made to Business Associates only when a Business Associate Contract is in place.

Go through your weekly, monthly and yearly routines and determine who has access to your PHI and in what manner that is disclosed.

Be sure to have those who you identify as Business Associates sign the Business Associate Contract as soon as you become a Covered Entity.

We have included two sample Business Associate Agreements in this manual. The one entitled Business Associate Agreement is to be used when you do not already have a written agreement in place with a Business Associate. Section 2.1 of the Business Associate Agreement has a place for you to list the duties for which you are hiring someone. For example, if you have someone who does your billing and you have never formalized your arrangement with a written agreement, you would put (where it says [list purposes]) a description of the biller's reason for reviewing your records, e.g. "Compiling charges, sending out bills, and maintaining records and copies of such bills."

The second Business Associate Agreement is entitled Business Associate Amendment to Agreement. This is to be used when you do have an existing written agreement with a Business Associate. You can keep the existing agreement and add this as an amendment to that agreement. The reference to the original agreement is addressed in the first four lines of the amendment.

Breach Notification Timeline:

- Covered Entity must notify patients within 60 days of breach discovery.
- Business Associate must notify Covered Entity within 60 days of breach discovery.
- Covered Entity must notify HHS of all breaches within 60 days of the end of each calendar year through the HHS web site

If the breach involves 500 or more individuals, the Covered Entity must also:

- Notify HHS within 60 days of breach discovery, including breaches by business associates and subcontractors; and

- Notify appropriate media outlets within 60 days of breach discovery.

Adopt Policies & Procedures That Apply HIPAA Regulations to Your Practice

The need to write and adopt policies is a somewhat foreign concept for most individual mental health practitioners. However, for purposes of HIPAA compliance it is a necessary step to take. The policies and procedures we have provided are a guideline and will still require you to do some work. They are compliant with federal HIPAA regulations, but do not include accommodations to state laws and to individual practice styles. The parts you will need to provide are those parts that pertain to your state and your individual practice.

HIPAA sets minimum requirements for privacy and security. Some state laws go beyond these minimum requirements. In those situations, the law that is more "stringent" applies. Furthermore, you can adopt individual practices that are more stringent than either or both federal and state laws. Take the time to review and modify, as appropriate, the policies and procedures. The compact disc included in some versions of this manual allows you to customize the policies and procedures to fit your state and practice. Sentences that appear in italics are optional and not required by HIPAA but are ones we suggest for appropriate, ethical practices. You may add privacy practices that you will adhere to as long as they either allow clients more access to their record or are more restrictive as to releases of information.

One note of caution, if you are going to write a policy that is different than those suggested, be sure that you can always adhere to that policy. You will place yourself at more risk for a complaint if you have a written policy that you do not adhere to, than if you have a less restrictive policy that you always adhere to.

Finally, since your Notice of Privacy Practices is your public statement about your policies, make sure that any changes you make in your NPP are reflected in your Policies and Procedures and vice versa. Furthermore, if you do make changes in your NPP, you are required to post the new NPP in your waiting room and on your website if you have one.

Educate and Train Employees

HIPAA requires that you train your staff members at the time of hiring or in preparation for HIPAA implementation and annually thereafter. Have employees sign documentation of completion of initial and updated training. You should keep records of attendance of all training and assure that all staff are trained and updated. See Volume 1 for further elaboration on training requirements for employees.

FORMS

(All Forms in this Manual were prepared with the assistance of Ogden Murphy Wallace law firm, Seattle, Washington, but should not be considered legal consultation.)

This section contains the following forms:

1. **Privacy and Security Policies and Procedures**

2. **Notice of Privacy Practices** (To be given to all clients); Acknowledgement of Receipt of Notice of Privacy Practices - must be signed by patient and clinicians at first meeting and kept as part of the patient's record.

   Acknowledgement of Receipt of Notice of Privacy Practices

3. **Business Associate Agreement** – for use with anyone who has access to your PHI who is not themselves a Covered Entity

   Business Associate Agreement Amendment – for use when you already have a BAA agreement in place and want to modify that agreement without re-writing the entire agreement

4. **Authorization to Release Health Care Information** – for use in all situations that require client authorization to release information

5. **Revocation of Consent for Use and Disclosure of Health Care Information** – to revoke disclosure of information which either requires client authorization, or is covered by TPO exceptions.

These forms are available on the CD in Microsoft Word format so that you can modify them as necessary to suit your practice.

[This page intentionally left blank.]

Policies and Procedures

These Policies and Procedures are educational only and do not constitute legal advice. They cover only federal law, not state law

Note: Sentences that appear in italics are optional and not required by HIPAA. They are included as examples of policies we feel are consistent with good clinical practice.

Applicability and Effective Date

Having determined that I am a Covered Entity as a "health care provider who transmits any health information in electronic form in connection with a covered transaction" the following Policies and Procedures are in force in my practice: The information contained in this Manual will be in effect beginning April 14, 2003, or at such time that I become a Covered Entity.

Uses and Disclosures of Protected Health Information

1. Permissible Uses and Disclosures without Written Authorization

   I may use and disclose PHI and ePHI without written authorization, excluding Psychotherapy Notes, for certain purposes as described below.

   1. Treatment: I may use and disclose PHI and ePHI in order to provide treatment to clients.

   2. Payment: I may use or disclose PHI or ePHI so that services are appropriately billed to, and payment is collected from, health plans.

   3. Health care Operations: I may use and disclose PHI or ePHI in connection with health care operations, including quality improvement activities, training programs, accreditation, certification, licensing or credentialing activities.

   4. Required or Permitted by Law: I may use or disclose PHI when I am required or permitted to do so by law. For example, I may disclose PHI to appropriate authorities if I reasonably believe that a client is a possible victim of abuse, neglect, or domestic violence or the possible victim of other crimes. In addition, I may disclose PHI to the extent necessary to avert a serious threat to the health or safety of a client or the health or safety of others. Other disclosures permitted or required by law include the following: disclosures for public health activities; health oversight activities including disclosures to state or federal agencies authorized to access PHI or ePHI; disclosures to judicial and law enforcement officials in response to a court order or other lawful process; disclosures for research when approved by an institutional review board; and disclosures to military or national security agencies, coroners, medical examiners, and correctional institutions or otherwise as authorized by law.

Note: HIPAA allows you to do many things that we have not included here. These include disclosures for purposes of reminding clients of their appointments, sending them information about treatment alternatives or other health related services, disclosures to family members or other persons involved in a client's care or in the event you intend to contact a client for fund raising purposes. If you intend to do any of these things, you must include these disclosures in both your NPP and policies and procedures. You must also include an explanation of the client's right to object to such disclosures. In addition, the foregoing descriptions of permissible uses and disclosures must be modified to the extent state law is more protective of client health information (e.g., "State law requires me to obtain your authorization to disclose your health information for payment purposes."). Finally, you may choose to modify the provisions in this section to reflect your individual practices that may be more restrictive than what federal and state law allow.

5. Records of Disclosure. Records of disclosure of PHI or ePHI without client authorization will be maintained in the case record as required by HIPAA standards.

   Records of disclosure will include:

   - A description of the information to be disclosed;
   - Who (individual or organization) is making the request;
   - Expiration date of the request;
   - A statement that the individual has the right to revoke the request;
   - A statement that information may be subject to re-disclosure by the receiving party;
   - Signature of the client or their representative and date;
   - If signed by a representative, a description of their authority to make the disclosure.

   Records of disclosure will be maintained for at least six years from April 14, 2003. (Note: The six-year requirement is just for the records of disclosure, not for the length of time you keep your clinical records. HIPAA does not address how long you keep your records. Refer to state law for length of time you are required to keep records.)

2. Uses and Disclosures Requiring Written Authorization

   1. **Psychotherapy Notes:** Notes documenting the contents of a counseling session ("Psychotherapy Notes") will not be used or disclosed without written client authorization.

      Note: HIPAA requires Psychotherapy Notes to be "separated from the rest of the individual's medical record." In addition, if you operate a federally assisted substance abuse program, or obtain HIV/AIDS testing, or other highly sensitive information protected by state law, applicable authorization requirements should be added here.

   2. **Marketing Communications:** PHI and ePHI will not be used for marketing purposes without written authorization.

   3. **Other Uses and Disclosures:** Uses and disclosures other than those described in Section A above will only be made with written client authorization. Clients may revoke such authorizations at any time.

Notice of Privacy Practices

A. Every attempt will be made in the first session to explain my Privacy Policy, address any restrictions to PHI and obtain a signature confirming receipt of NPP. In those situations where a signature is not possible, I will document my attempts to obtain the signature and the reasons for not doing so.

B. Existing clients will receive my Notice of Privacy Practices (NPP) immediately.

   1. A copy of my NPP will be posted in my waiting room and on my website (if applicable) and updated as policies change. Any client or potential client may have access to a written copy of my Privacy Policy.

C. I reserve the right to make changes in my Privacy Policies and Procedures. Language supporting this right will appear in my NPP. In those situations where changes are made to my Privacy Policies and Procedures, I will post those changes in my waiting room and on my website (if applicable).

D. I will obtain a written consent from all clients to release any and all information including TPO except when required by law.

Access to Protected Health Information

A. Right to Inspect and Copy.

Clients may request access to their medical record and billing records maintained by me in order to review and/or request copies of the records. All requests for access must be made in writing. Under limited circumstances, I may deny access to those records. I may charge a fee for the costs of copying and sending any records requested. [Note: State law may regulate such charges]. A parent or legal guardian of a minor will not have access to certain portions of the minor's medical record. [Note: Examples should be included consistent with state law (e.g., records related to mental health, drug treatment, or family planning services)]. Access will be granted within a reasonable time frame and no later than 30 days. [Note: State law may vary on this.] In those situations where I determine that access to their PHI or ePHI would be harmful to the client, I will restrict the client's access to the record. The client may appeal this decision to a neutral third party agreed upon by both the client and me. The decision of that party will be binding. [Note: This provision needs to be checked against state law.]

B. Right to Request Amendment.

Clients have the right to amend their record by including a statement in the case file. The original documentation will remain in the file alongside the amendment. All client requests to access case records will be recorded in their file. The client's request must be in writing and must explain why the information should be amended. I may deny requests under certain circumstances, but I will accommodate any reasonable written request to receive PHI or ePHI by alternative means of communication or at alternative locations.

C. **Minimum Necessary.** With the exception of release of information for treatment purposes, any disclosure of PHI or ePHI will provide only the minimum necessary information to comply with the request.

D. **Security of Records.** Appropriate safeguards will be taken to protect the security of PHI and ePHI and reasonably protect it from intentional or unintentional disclosures.

E. **Right to Request Restrictions.** Clients have the right to request a restriction on PHI or ePHI used for disclosure for treatment, payment or health care operations. Clients must request any such restrictions in writing addressed to the Privacy Officer. I am not required to agree to any restrictions clients may request.

F. **Right to Obtain Notice.** Clients have the right to obtain a paper copy of my NPP by submitting a request to the Privacy Officer.

G. **Questions and Complaints.** Clients who require further information about their privacy rights or have concerns that I have violated their privacy rights may contact the Privacy Officer. Clients may also file written complaints with the Director, Office for Civil Rights of the U.S. Department of Health and Human Services.

Business Associates

A. It is my policy to obtain a Business Associate Contract with any individual or organization who has access to PHI or ePHI in my possession and who is not a Covered Entity under HIPAA or a member of my workforce.

B. All Business Associate Contracts will include language that reasonably assures that the Business Associate will appropriately safeguard and limit their use and disclosure of PHI or ePHI that I disclose to them. In the event I learn of a breach of the Business Associate Contract by the Business Associate, I will immediately take reasonable steps to correct the problem, including termination of the contract with the Business Associate and reporting to the Secretary of the Department of Health and Human Services.

C. Business Associate Contracts will be in place on or before April 14, 2003 or at such time that I become a Covered Entity.

D. Business Associates will be held liable directly for unauthorized disclosures of PHI or ePHI and subject to enforcement sanctions.

Administrative Requirements — Privacy Official, Complaints and Grievances

A. _____ is the designated privacy officer and contact person for my practice. Questions and concerns about violations of HIPAA requirements can first be directed to me.

B. In the event a breach of confidentiality is reported, I will review the complaint and compare the action I took against HIPAA regulations. In this process I will take reasonable steps to obtain expert opinion and review of my practice to determine if a breach has occurred. If I find that a breach has occurred I will take immediate steps to come into compliance with HIPAA regulations.

C. Clients will be informed in my NPP of the proper procedure for filing a complaint. At no time will I intimidate, threaten, coerce, discriminate or retaliate against anyone making a complaint against me, nor will clients be asked to waive their rights to receive treatment for filing a complaint against my practice.

D. As changes in HIPAA regulations are implemented, I will update my policies, practices and notices to comply with the new regulations. Changes will be posted in my waiting room and on my website.

E. All policies pertaining to HIPAA will be retained by my practice for at least six years from the date they are written or the date they are in effect, whichever is later, even if policies and procedures change.

Preemption of State Law

A. I will comply with all state laws pertaining to my practice. In the event that a state law conflicts with HIPAA regulations, I will adhere to the regulation or law that offers clients more stringent protection of PHI or ePHI.

Policies Pertaining to Employees

A. All employees will be trained in the use and disclosure of PHI, with and without authorization, at the time of hiring and annually thereafter. Employees will sign documentation of completion of training.

B. All employees will sign a confidentiality agreement.

C. All employees will be trained to understand the concept of minimum necessary in disclosure of PHI or ePHI. Employees will be given access only to that PHI or ePHI necessary to complete their job duties. Any employee who violates these policies and procedures will be subject to disciplinary action up to and including termination of employment.

D. Employees are encouraged to report any potential conflict between HIPAA regulations and practice procedures. No employee will be punished for reporting infractions. Employees are not required to participate in a practice that they feel, in good faith, is illegal.

E. Employees will be trained in security awareness.

F. Policy and Procedure Manuals will be available to all staff. All previous policy manuals will be available to employees for at least six years from the date of creation or date when the policy was last in effect, whichever is later.

G. All employees will be trained in HIPAA implementation timelines.

H. Employees are encouraged to respond to and cooperate with requests from DHHS for information. Employees will be trained in the procedures for responding to an investigation.

Breach Notification Policy

In the event of a breach of unsecured protected health information it is my policy to:

A. Conduct an assessment to determine whether there is a low probability that the PHI was compromised. I will retain documentation of the assessment and response to the breach, including the rationale for a decision not to notify the client.

B. If I determine that there is not a low probability that the PHI was compromised, I will:

1. Notify each individual whose unsecured protected health information has been, or believed to have been, accessed, acquired, used, or disclosed as a result of a breach as soon as possible and no later than 60 days from the time the breach is discovered.

2. Include in the notification a description of what happened, the date of the breach, what information was released, steps I am taking to investigate the breach and minimize harm to the individual(s), and steps the individuals can take to protect themselves from harm. I will also provide contact procedures for individuals to ask questions or learn additional information.

3. Notify the individual in writing, by first class mail or by electronic mail if given permission.

    a. If I do not have current contact information and less than 10 individuals are involved, I will make every effort to find current contact information and provide notification by whatever means I am able to find.

    b. If I do not have current contact information and 10 or more individuals are involved, I will develop a substitute method of notification that conforms to the Breach Notification Rule (45 CFR Parts 160 and 164)

c. If the breach involves 500 or more individuals, I will inform appropriate media outlets and the Secretary of HHS.

d. I will maintain a log of breaches of less than 500 individuals and report those annually to the Secretary of HHS.

C. Honor requests by law enforcement official(s) to delay notification of a breach due to impediment of a criminal investigation or that may cause damage to national security.

D. Adhere to all administrative requirements.

[This page intentionally left blank.]

[LCSW Name and Address]
NOTICE OF PRIVACY PRACTICES

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

I am required by law to maintain the privacy of your health information. I am also required to give you this Notice about my privacy practices, legal obligations, and your rights concerning your health information ("Protected Health Information" or "PHI"). I will follow the privacy practices that are described in this Notice. If I amend this Notice, I will provide you with the amended Notice for your information and signature.

For more information about my privacy practices, or for additional copies of this Notice, please let me know your questions as soon as they arise.

I. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

A. **Permissible Uses and Disclosures Without My Written Authorization.** I may use and disclose your PHI without your written authorization for certain purposes as described below. The examples provided in each category are not meant to be exhaustive, but instead are meant to describe the types of uses and disclosures of your mental health information that are legally permissible.

1. **Treatment:** I may use and disclose your PHI to other clinicians involved in your care in order to better provide integrated treatment to you. For example, I may discuss your diagnosis and treatment plan with your psychiatrist or nurse practitioner. In addition, I may disclose your PHI to other health care providers in order to provide you with appropriate care and continued treatment.

2. **Payment:** I may use or disclose your PHI for the purposes of determining coverage, billing, claims management, and reimbursement. For example, a bill sent to your health insurer may include some information about our work together so that the insurer will pay for the treatment. I may also inform your health plan about a treatment you are going to receive in order to determine whether the plan will cover the treatment.

3. **Health Care Operations:** I may use and disclose your PHI in connection with health care operations, including quality improvement activities, training programs, accreditation, certification, licensing or credentialing activities. For, example, I may disclose disguised information about our work for training purposes.

4. **Required or Permitted by Law:** I may use or disclose your PHI when I am required or permitted to do so by law. For example, I may disclose your PHI to appropriate authorities if I reasonably believe that you are a possible victim of abuse, neglect, domestic violence, or the possible victim of other crimes. In addition I may disclose your PHI to the extent necessary to avert a serious threat to your health or safety or the health or safety of others. Other disclosures permitted or required by law include the following: disclosures for public health activities; health oversight activities including disclosures to state or federal agencies authorized to access your PHI; disclosures to judicial and law enforcement officials in response

to a court order or other lawful process; disclosures for research when approved by an institutional review board; disclosures for workers' compensation claims, and disclosures to military or national security agencies, coroners, medical examiners, and correctional institutions as authorized by law.

B. Permissible Uses and Disclosures That May Be Made Without My Authorization, But For Which You Have An Opportunity to Object.

1. **Fundraising:** I may use your PHI to contact you in an effort to offer you new services. I may also disclose PHI to any foundation with which I am connected so that the foundation may contact you in an effort to raise money for its operations. Any fundraising communications with you will include a description of how you may opt out of receiving any further fundraising communications.

2. **Family and Other Persons Involved in Your Care.** I may use or disclose your PHI to notify, or assist in the notification of (including identifying or locating) your personal representative, or another person responsible for your care, location, general condition, or death. If you are present, then I will provide you with an opportunity to object prior to such uses or disclosures. In the event of your incapacity or emergency circumstances, I will disclose your PHI consistent with your prior expressed preference, and in your best interest as determined by my professional judgment. I will also use my professional judgment and my experience to make reasonable inferences of your best interest in allowing another person access to your PHI regarding your treatment with me.

3. **Disaster Relief Efforts.** I may use or disclose your PHI to a public or private entity authorized by law or its charter to assist in disaster relief efforts for the purpose of coordinating notification of family members of your location, general condition, or death.

C. **Uses and Disclosures Requiring Your Written Authorization.**

1. **Psychotherapy Notes.** I will not disclose the records of our work that I keep separate from the medical record for my personal use, known as psychotherapy notes, except as permitted by law.

2. **Marketing Communications; Sale of PHI.** I must obtain your written authorization prior to using or disclosing your PHI for marketing or the sale of your PHI, consistent with the related definitions and exceptions set forth in HIPAA.

3. **Other Uses and Disclosures.** Uses and disclosures other than those described in this Notice will only be made with your written authorization. For example, you will need to sign an authorization form before I can send your PHI to your life insurance company or to your attorney. You may revoke any such authorization at any time by providing me with written notification of such revocation.

II. MY INDIVIDUAL RIGHTS

A. **Right to Inspect and Copy.** You may request access to your medical records and billing records maintained by me in order to inspect and request copies of the records. All requests for access must be made in writing. Under limited circumstances, I may deny access to your records. I may charge a fee for the costs of copying and sending you any records requested.

B. **Right to Alternative Communications.** You may request, and I will accommodate, any reasonable written request for you to receive your PHI by alternative means of communication or at alternative locations.

C. **Right to Request Restrictions.** You have the right to request a restriction on your PHI that I use or disclose for treatment, payment or health care operations. You must request any such restriction in writing addressed to **[LCSW Name and Contact Information]**. I am not required to agree to any such restriction you may request, except if your request is to restrict disclosing your PHI to a health plan for the purpose of carrying out payment or health care operations, the disclosure is not otherwise required by law, and the PHI pertains solely to a health care item or service which has been paid in full by you or another person or entity on your behalf.

D. **Right to Accounting of Disclosures.** Upon written request, you may obtain an accounting of disclosures of your PHI made by me in the last six years, subject to certain restrictions and limitations.

E. **Right to Request Amendment:** You have the right to request that I amend your PHI. Your request must be in writing, and should explain why the information should be amended. I may deny your request under certain circumstances.

F. **Right to Obtain Notice.** You have the right to obtain a paper copy of this Notice by submitting a request to **[LCSW Name and Address]** at any time.

G. **Right to Receive Notification of a Breach.** I am required to notify you if I discover a breach of your unsecured PHI, according to requirements under federal law.

H. **Questions and Complaints.** If you desire further information about your privacy rights, or are concerned that I have violated your privacy rights, please contact me at **[LCSW Phone Number]**. You may also file a written complaint with the Director, Office for Civil Rights of the U.S. Department of Health and Human Services. I will not retaliate against you if you file a complaint.

III. EFFECTIVE DATE AND CHANGES TO THIS NOTICE

A. Effective Date. This Notice is effective on _____.

B. Changes to this Notice. I may change the terms of this Notice at any time. If I change this Notice, I may make the new notice terms effective for all PHI that I maintain, including any information created or received prior to issuing the new notice. If I change this Notice, I will post the revised notice in the waiting area of my office and on my website at [**website address**]. You may also obtain any revised notice by asking me directly.

[LCSW Name and Address]
ACKNOWLEDGEMENT OF RECEIPT OF NOTICE OF PRIVACY PRACTICES

By my signature below I, _____, acknowledge that I received a copy of her Notice of Privacy Practices.

_____
Printed name of client

_____ _____
Signature of client Date

_____ _____
Signature of LCSW Date

If this acknowledgment is signed by a personal representative on behalf of the client, complete the following:

Personal Representative's Name: _____

Relationship to Client: _____

For Office Use Only

I attempted to obtain written acknowledgement of receipt of our Notice of Privacy Practices, but acknowledgement could not be obtained because:

3. Individual refused to sign
4. Communications barriers prohibited obtaining the acknowledgement
5. An emergency situation prevented us from obtaining acknowledgement
6. Other (Please Specify)

This form will be retained in your medical record
by the Miller Nash Law Firm

[LCSW Name and Address]
BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into by and between [Name of Entity] ("Covered Entity") and _____, ("Business Associate"), effective as of the ___ day of _____, 20__ ("Effective Date").

RECITALS

WHEREAS, the parties contemplate one (1) or more arrangements (collectively, the "Arrangement") whereby Business Associate provides services to Covered Entity, and Business Associate creates, receives, maintains, transmits, or has access to Protected Health Information in order to provide those services;

WHEREAS, Covered Entity is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and regulations promulgated thereunder, including the Standards for Privacy and for Security of Individually Identifiable Health Information codified at 45 Code of Federal Regulations ("CFR") Parts 160, 162, and 164 ("Privacy Regulations" and "Security Regulations");

WHEREAS, the Privacy Regulations and Security Regulations require Covered Entity to enter into a contract with Business Associate in order to mandate certain protections for the privacy and security of Protected Health Information, and those Regulations prohibit the disclosure or use of Protected Health Information by or to Business Associate if such a contract is not in place;

AGREEMENT

NOW, THEREFORE, in consideration of the foregoing, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

DEFINITIONS

"Designated Record Set" shall mean a group of records maintained by or for Covered Entity that is (a) the medical records and billing records about individuals maintained by or for Covered Entity; (b) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (c) used, in whole or in part, by or for Covered Entity to make decisions about individuals. As used herein, the term "Record" means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for Covered Entity.

"Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of, access to, or divulging in any other manner, of Protected Health Information outside Business Associate's internal operations, or to persons other than Business Associate's own employees engaged in internal operations.

"Protected Health Information" or "PHI" means information, including demographic information, that (a) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; (b) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual); (c) is received by Business Associate from or on behalf of Covered Entity, or is created, received, maintained, or transmitted by Business Associate, or is made accessible to Business Associate by Covered Entity; and (d) is transmitted or maintained in any form or medium.

"Electronic Protected Health Information" or "EPHI" means the subset of PHI that is transmitted by electronic media or maintained in electronic media.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations of an information system.

"Use" or "Uses" mean, with respect to PHI, the sharing, employment, application, utilization, examination, or analysis of such information within Business Associate's internal operations.

Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those in 45 CFR 160, 162, and 164.

OBLIGATIONS OF BUSINESS ASSOCIATE

Permitted Uses and Disclosures of PHI. Except as otherwise limited in this Agreement, Business Associate may Use and Disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the written documents describing the Arrangement, provided that such Use or Disclosure of PHI would not violate the Privacy Regulations or Security Regulations if done by Covered Entity. Business Associate agrees not to Use or Disclose PHI other than as permitted or required by this Agreement, or as required by law.

Adequate Safeguards for PHI. Business Associate warrants that it shall implement and maintain appropriate safeguards to prevent the Use or Disclosure of PHI in any manner other than as permitted by this Agreement or as required by law.

Adequate Safeguards for EPHI. Business Associate warrants that it shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any EPHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate further warrants that it shall comply with the HIPAA Security Regulations, where applicable, with respect to EPHI to prevent the use or disclosure of EPHI other than as provided for by this Agreement.

Reporting Non-Permitted Use, Disclosure, or Breach.

Business Associate shall immediately in writing notify Covered Entity of any Use or Disclosure of PHI not provided for by this Agreement of which Business Associate becomes aware.

Business Associate shall report to Covered Entity any Security Incident of which it becomes aware as follows: (a) reports of successful unauthorized access shall be made immediately; and (b) reports of attempted unauthorized access shall be made in a reasonable time and manner considering the nature of the information to be reported.

Business Associate shall report to Covered Entity a breach of Unsecured Protected Health Information without unreasonable delay, but not later than five (5) days, following Business Associate's discovery of such breach, where such report will include the identification of each individual whose Unsecured PHI has been or is reasonably believed to have been breached and other information as requested by Covered Entity. For purposes of the foregoing obligation, "breach" shall mean the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Regulations which compromises the security or privacy of such information, as further defined in 45 CFR Section 164.402.

Availability of Internal Practices, Books and Records to Government Agencies. Business Associate agrees to make its internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by Business Associate on behalf of Covered Entity available to the Secretary of the federal Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy Regulations. Business Associate shall immediately in writing notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

Access to and Amendment of PHI. Within ten (10) days of receiving a request from Covered Entity for access to PHI about an individual contained in a Designated Record Set, Business Associate shall: (a) make the PHI specified by Covered Entity available to the individual(s) identified by Covered Entity as being entitled to access and copy that PHI, and (b) make PHI available to Covered Entity for amendment purposes and incorporating such amendments into the PHI. Business Associate shall provide such access and incorporate such amendments within the time and in the manner specified by Covered Entity.

Accounting of Disclosures. In accordance with 45 CFR 164.528, and Section 13405(c) of Title XII, Subtitle D of the Health Information Technology for Economic and Clinical Health ("HITECH") Act, codified at 42 U.S.C. § 17932, Business Associate agrees to: (a) document Disclosures of PHI and information related to such Disclosures; (b) provide such documentation to Covered Entity in a time and manner designated by Covered Entity; and (c) permit Covered Entity to respond to a request by an individual for an accounting of Disclosures of PHI. Within ten (10) days of receiving a request from Covered Entity, Business Associate shall provide to Covered Entity an accounting, as referenced in 45 CFR 164.528, of each Disclosure of PHI made by Business Associate or its employees, agents, representatives, or subcontractors.

Any accounting provided by Business Associate under this Section 0 shall include: (a) the date of Disclosure; (b) the name, and address, if known, of the entity or person who received the PHI; (c) a brief description of Disclosed PHI; and (d) a brief statement of the purpose of Disclosure. For each Disclosure that could require an accounting under this Section 0, Business Associate shall document the information specified in (a) through (d), above, and shall securely retain this documentation for six (6) years from the date of Disclosure.

Use of Subcontractors and Agents. Business Associate may disclose PHI to a subcontractor, and may allow the subcontractor to create, receive, maintain, or transmit PHI on its behalf, provided by Business Associate obtains satisfactory assurances that the subcontractor will appropriately safeguard the information. Without limiting the generality of the foregoing, Business Associate shall require each of its subcontractors that create, receive, maintain, or transmit PHI on behalf of Business Associate to execute a written agreement obligating the subcontractor to comply with all terms of this Agreement and to agree to the same restrictions and conditions that apply to Business Associate with respect to the PHI.

Business Associate shall not be in compliance with the Privacy Regulations if Business Associate knew of a pattern of activity or practice of a subcontractor that constituted a material breach or violation of the subcontractor's obligation under the written agreement with Business Associate, unless Business Associate took reasonable steps to cure the breach or end the violation, and if such steps were unsuccessful, terminate the contract, if feasible.

Agreement to Mitigate. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement, and to promptly communicate to Covered Entity any actions taken pursuant to this paragraph.

Business Associate Practices, Policies and Procedures. Business Associate's privacy and security policies and practices shall meet current standards set by applicable state and federal law for the protection of PHI including, without limitation, user authentication, data encryption, monitoring and recording of database access, internal privacy standards and a compliance plan, all designed to provide assurances that the requirements of this Agreement are met.

Compliance with Covered Entity Obligations. To the extent Business Associate carries out Covered Entity's obligations under the Privacy Regulations and Security Regulations, Business Associate shall comply with the requirements of such regulations that apply to Covered Entity in the performance of such obligations.

HITECH Act Compliance. Business Associate will comply with the requirements of the HITECH Act, codified at 42 U.S.C. §§ 17921–17954, which are applicable to business associates, and will comply with all regulations issued by the Department of Health and Human Services (HHS) to implement these referenced statutes, as of the date by which business associates are required to comply with such referenced statutes and HHS regulations. Further, Business Associate will comply with Section 13402 of the HITECH Act, codified at 42 U.S.C. § 17932, and will comply with all regulations issued by HHS to implement this statute, as of the date by which business associates are required to comply with such referenced statutes and HHS regulations. Business Associate agrees to indemnify Covered Entity for any and all costs and expenses incurred by Covered Entity which are directly or indirectly caused by Business Associate's failure to comply with the HITECH Act and the HITECH Act's implementing regulations including, without limitation, penalties imposed and expenses incurred related to notifying individuals of a breach caused by Business Associate or its subcontractors in compliance with the HIPAA breach notification requirements set forth at 42 U.S.C. §17932..

ADDITIONAL PERMITTED USES

Except as otherwise limited in this Agreement or the Arrangement, Business Associate may use PHI for the following additional purposes:

Use of Information for Management, Administration and Legal Responsibilities. Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

Disclosure of Information for Management, Administration and Legal Responsibilities. Business Associate may Disclose PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate if the Disclosure is required by law, or Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will be held confidentially and Used or further Disclosed only as required by law or for the purpose of which it was Disclosed, and the person notifies Business Associate of any instances of which it is aware where confidentiality of the information has been breached.

TERM AND TERMINATION

Term and Termination. This Agreement shall commence as of the Effective Date and shall continue in effect unless and until terminated by Covered Entity under this Section 0. Covered Entity may terminate this Agreement, without cause or penalty, on five (5) days' prior written notice to Business Associate. In addition, this Agreement may be terminated by Covered Entity immediately and without penalty upon written notice by Covered Entity to Business Associate if Covered Entity determines, in its sole discretion, that Business Associate has violated any material term of this Agreement. Business Associate's obligations under Sections 0, 0, 0, 0, 0, 0, 0, and 0 of this Agreement shall survive the termination of this Agreement.

Disposition of PHI upon Termination. Upon termination of this Agreement, Business Associate shall either return or destroy, in Covered Entity's sole discretion and in accordance with any instructions by Covered Entity, all PHI maintained in any form by Business Associate or its agents and subcontractors, and shall retain no copies of such PHI unless directed to do so by Covered Entity. However, if Covered Entity determines that neither return nor destruction of PHI is feasible, Business Associate may retain PHI provided that Business Associate: (a) continues to comply with the provisions of this Agreement for as long as it retains PHI, and (b) limits further Uses and Disclosures of PHI to those purposes that make the return or destruction of PHI infeasible.

GENERAL TERMS

No Third Party Beneficiaries. There are no third party beneficiaries to this Agreement.

Relationship to Agreement Provisions. In the event that a provision of this Agreement is contrary to a provision of any other agreement between the parties, the provisions of this Agreement shall control.

Indemnification. Business Associate will indemnify, hold harmless and defend Covered Entity from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of, or in connection with (a) any misrepresentation, breach, or non-fulfillment of any undertaking on the part of Business Associate under this Agreement; (b) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization, arising out of or in any way connected with Business Associate's obligations under this Agreement; and (c) a breach of unsecured PHI caused by Business Associate or its subcontractors or agents. Without limiting the generality of the foregoing, Business Associate agrees to indemnify Covered Entity for any and all costs and expenses incurred as a result or arising directly or indirectly out of the Covered Entity's compliance with the HIPAA breach notification requirements set forth at 42 U.S.C. § 17932.

Insurance. Business Associate shall obtain and maintain during the term of this Agreement and at any time in which it retains PHI, privacy and security liability insurance covering common law claims, breach notification expenses, data theft, and coverage related to the violation of state or federal information privacy and security laws or regulations. The policy limits for such coverage shall not be less than $1,000,000 per claim, and $5,000,000 in the aggregate. Such insurance shall name the Covered Entity as an additional named insured. A copy of such policy or a certificate evidencing the policy shall be provided to the Covered Entity upon written request.

Data Ownership. Business Associate acknowledges and agrees that Covered Entity owns all rights, interests, and title in and to its data, including all PHI, and title shall remain vested in Covered Entity at all times.

Legal Compliance; Amendment. The parties hereto shall comply with applicable laws and regulations governing their relationship, including, without limitation, the Privacy Regulations, the Security Regulations, and any other federal or state laws or regulations governing the privacy, confidentiality, or security of patient health information, including without limitation, the Washington Uniform Healthcare Information Act, RCW Ch. 70.02. If a provision of this Agreement is held invalid under any applicable law, such invalidity will not affect any other provision of this Agreement that can be given effect without the invalid provision. Further, all terms and conditions of this Agreement will be deemed enforceable to the fullest extent permissible under applicable law, and, when necessary, the court is requested to reform any and all terms or conditions to give them such effect. Business Associate shall comply with applicable state and federal statutes and regulations as of the date by which business associates are required to comply with applicable statutes and regulations. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Regulations, the Security Regulations, the HITECH Act, RCW ch. 70.02 and other federal or state laws or regulations governing the privacy, confidentiality or security of PHI. Upon request by Covered Entity, Business Associate agrees to promptly enter into negotiations with Covered Entity concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of the Privacy Regulations, Security Regulations, or other applicable laws. Covered Entity may terminate this Agreement upon thirty (30) days written notice to Business Associate in the event: (a) Business Associate does not promptly enter into negotiations to

amend this Agreement when requested by Covered Entity pursuant to this Section, or (b) Business Associate does not enter into an amendment of this Agreement providing assurances regarding the safeguarding of PHI that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of the Privacy Regulations, Security Regulations, or other applicable laws.

Independent Contractor. Business Associate and Covered Entity are and shall be independent contractors to one another, and nothing herein shall be deemed to cause this Agreement to create an agency, partnership, or joint venture between the parties. No acts performed or words spoken by either party with respect to any third party shall be binding upon the other. Any and all obligations incurred by either party in connection with the performance of any of its obligations hereunder shall be solely at that party's own risk, and the other shall not be obligated in any way therefore except as specifically provided for herein to the contrary. Each party agrees that it shall not represent itself as the agent or legal representative of the other for any purpose whatsoever.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement effective as of the Effective Date.

Business Associate:	**Covered Entity:**
_____	_____
By: _____	By: _____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Dated: _____	Dated: _____

[LCSW Name and Address]
Business Associate Amendment to Agreement

By agreement of the parties, _____ ("Covered Entity") and _____("Business Associate"), whose signatures have been affixed below, the _____ Agreement for _____ Services, dated, 20__, ("Agreement"), is hereby amended as set forth herein ("Amendment"). This Amendment is effective as of, 20__ or such earlier date as this Amendment is fully signed by the parties ("Effective Date").

RECITALS

WHEREAS, the parties have executed an agreement whereby Business Associate provides services to Covered Entity, and Business Associate receives, has access to or creates Protected Health Information in order to provide those services ("Agreement");

WHEREAS, Covered Entity is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and regulations promulgated thereunder, including the Standards for Privacy of Individually Identifiable Health Information codified at 45 Code of Federal Regulations Parts 160 and 164 ("Privacy Regulations");

WHEREAS, the Privacy Regulations require Covered Entity to enter into a contract with Business Associate in order to mandate certain protections for the privacy and security of Protected Health Information or electronic Protected Health Information, and those Regulations prohibit the disclosure to or use of Protected Health Information or electronic Protected Health Information by Business Associate if such a contract is not in place;

NOW, THEREFORE, in consideration of the foregoing, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

DEFINITIONS

2.1 "Disclose" and "Disclosure" mean, with respect to Protected Health Information, the release, transfer, provision of access to, or divulging in any other manner of Protected Health Information or electronic Protected Health Information outside Business Associate's internal operations or to other than its employees.

2.2 "Protected Health Information" or "PHI" and electronic Protected Health Information or "ePHI" means information, including demographic information, that (i) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual, or the past, present or future payment for the provision of health care to an individual; (ii) identifies the individual (or for which there is a reasonable basis for believing that the information can be used to identify the individual); and (iii) is received by Business Associate from or on behalf of Covered Entity, or is created by Business Associate, or is made accessible to Business Associate by Covered Entity.

2.3 "Services" has the same meaning as in the Agreement.

2.4 "Use" or "Uses" mean, with respect to Protected Health Information, the sharing, employment, application, utilization, examination or analysis of such information within Business Associate's internal operations.

2.5 Terms used, but not otherwise defined, in this Amendment shall have the same meaning as those in 45 CFR 160.103 and 164.501.

OBLIGATIONS OF BUSINESS ASSOCIATE

(1) Permitted Uses and Disclosures of PHI and ePHI. Business Associate may Use and Disclose PHI and ePHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Agreement provided that such use or disclosure would not violate the Privacy Regulations if done by the Covered Entity. Business Associate agrees not to use or further disclose PHI other than as permitted or required by the Agreement, this Amendment, or as required by law.

(2) Adequate Safeguards for PHI and ePHI. Business Associate warrants that it shall implement and maintain appropriate safeguards to prevent the Use or Disclosure of PHI and ePHI in any manner other than as permitted by the Agreement and this Amendment.

(3) Reporting Non-Permitted Use or Disclosure. Business Associate shall immediately in writing notify Covered Entity of each Use or Disclosure, of which it becomes aware, that is made by Business Associate, its employees, representatives, agents or subcontractors that is not specifically permitted by this Amendment.

(4) Availability of Internal Practices, Books and Records to Government Agencies. Business Associate agrees to make its internal practices, books and records relating to the Use and Disclosure of PHI available to the Secretary of the federal Department of Health and Human Services for purposes of determining Covered Entity's compliance with the Privacy Regulations. Business Associate shall immediately notify Covered Entity of any requests made by the Secretary and provide Covered Entity with copies of any documents produced in response to such request.

(5) Access to and Amendment of PHI and ePHI. Within ten (10) days of receiving a request from the Covered Entity, Business Associate shall: (a) make the PHI or ePHI specified by Covered Entity available to the individual(s) identified by Covered Entity as being entitled to access and copy that PHI or ePHI, and (b) make PHI or ePHI available to Covered Entity for the purpose of amendment and incorporating such amendments into the PHI or ePHI. Business Associate shall provide such access and incorporate such amendments within the time and in the manner specified by Covered Entity.

(6) Accounting of Disclosures. Within ten (10) days of receiving a request from the Covered Entity, Business Associate shall provide to Covered Entity an accounting of each Disclosure of PHI or ePHI made by Business Associate or its employees, agents, representatives or subcontractors. Business Associate is not required to provide an accounting of Disclosures that are necessary to perform the Services when such Disclosures are for the purposes of the Covered Entity's treatment, payment or health care operations. Any accounting provided by Business Associate under this Section 2.6 shall include:

(a) the date of the Disclosure; (b) the name, and address if known, of the entity or person who received the PHI or ePHI; (c) a brief description of the PHI or ePHI disclosed; and (d) a brief statement of the purpose of the Disclosure. For each Disclosure that could require an accounting under this Section 2.6, Business Associate shall document the information specified in (a) through (d), above, and shall securely retain this documentation for six (6) years from the date of the Disclosure.

(7) Term and Termination. The term of this Amendment shall be the same as the term of the Agreement. In addition to and notwithstanding the termination provisions set forth in the Agreement, both this Amendment and the Agreement may be terminated by Covered Entity immediately and without penalty upon written notice by Covered Form: Business Associate Amendment to Agreement Entity to Business Associate if Covered Entity determines, in its sole discretion, that Business Associate has violated any material term of this Agreement, as amended. Business Associate's obligations under Sections 2.3, 2.4, 2.5, 2.6, 2.8, and 2.10 of this Amendment shall survive the termination or expiration of the Agreement.

(8) Disposition of PHI or ePHI upon Termination or Expiration. Upon termination or expiration of the Agreement and this Amendment, Business Associate shall either return or destroy, in Covered Entity's sole discretion and in accordance with any instructions by Covered Entity, all PHI or ePHI in the possession or control of Business Associate or its agents and subcontractors. However, if Covered Entity determines that neither return nor destruction of PHI or ePHI is feasible, Business Associate may retain PHI provided that Business Associate (a) continues to comply with the provisions of this Amendment for as long as it retains PHI or ePHI, and (b) limits further Uses and Disclosures of PHI or ePHI to those purposes that make the return or destruction of PHI or ePHI infeasible.

(9) No Third Party Beneficiaries. There are no third party beneficiaries to this Agreement.

(10) Use of Subcontractors and Agents. Business Associate shall require each of its agents and subcontractors that receive PHI from Business Associate to execute a written agreement obligating the agent or subcontractor to comply with all the terms of this Amendment.

(11) Relationship to Agreement Provisions. In the event that a provision of this Amendment is contrary to a provision of the Agreement, the provision of this Amendment shall control. Otherwise, this Amendment shall be construed under, and in accordance with, the terms of the Agreement.

(12) Indemnification. Business Associate will indemnify, hold harmless and defend Covered Entity from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result or arising directly or indirectly out of or in connection with (a) any misrepresentation, breach or non-fulfillment of any undertaking on the part of Business Associate under this Amendment; and (b) any claims, demands, awards, judgments, actions and proceedings made by any person or organization, arising out of or in any way connected with Business Associate's obligations under this Amendment.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement effective as of the date stated above.

Business Associate:

_____

By: _____

Title: _____

Date: _____

Business Associate:

_____

By: _____

Title: _____

Date: _____

[This page intentionally left blank.]

[LCSW Name and Address]
Authorization to Release Health Care Information

Client name: _____ Date of birth: _____

SSN: _____ Previous name: _____

Please release health care information to:

Name and Organization: _____

Address: _____

City, State: _____ Zip Code: _____

Release the following information:

- Health care information relating to the following treatment or condition:

  _____

- Health care information for the date(s): _____
- All health care information: _____
- Other: _____

This authorization ends:

- in 90 days; or
- when the following occurs (but not longer than 90 days): _____

I may cancel this authorization in writing as allowed by law. This would not affect any actions already taken based upon my original request. There are three ways to cancel this authorization:

(1) Sign and date a revocation form. This form is available from (clinician); or
(2) Write, sign and date a letter to the (clinician clinician) to cancel the authorization; or
(3) Sign, date and write "CANCEL" on this original form

Once the (clinician) gives out the information, the (clinician) has no control over it. The recipient might re-disclose it. Privacy laws may no longer protect it.

I also agree to the release of health care information regarding testing, diagnosis, and/or treatment for: HIV (AIDS virus), Sexually transmitted diseases, Psychiatric disorders/mental health, or Drug and/or alcohol use.

_____ _____ _____
Patient or legally authorized individual signature Date Time

Relationship to patient if signed on behalf of the patient by parent, legal guardian, personal representative, etc.: _____

[This page intentionally left blank.]

Revocation of Consent for Use and Disclosure of Health Care Information

Client name: _____ Date of birth: _____

SSN: _____ Previous name: _____

I no longer want (clinician) to use and disclose health care information about me for treatment, billing and payment, and health care operations.

I understand that:

- This request applies after I sign this document.
- (Clinician) may have already taken action based upon my earlier permission.
- (Clinician) is allowed, by law, to use and disclose my health care information to complete treatment, billing and payment, and health care operations already in progress. I agreed to this when I signed the "Consent for Use and Disclosure of Health Care Information."
- (Clinician) is allowed or required by law to release health care information without my permission under certain situations.
- (Clinician) does not have to provide any further health care services to me.

_____ _____ _____
Client or legally authorized individual signature Date Time

Relationship to patient if signed on behalf of the patient by parent, legal guardian, personal representative, etc.: _____

Signature: _____ Date: _____

[This page intentionally left blank.]

APPENDICES

This section contains the following Appendices:

[This page intentionally left blank.]

Appendix 1: Frequently Asked Questions (FAQs) about the HIPAA Privacy and Security Standards (September, 2008)

1. **Generally what do the HIPAA Privacy and Security Standards require clinicians to do?**

   Clinicians must 1) Notify patients of their privacy rights with the Notice of Privacy Practice (NPP); 2) Develop privacy policies; 3) Designate a Privacy Officer; 4) Keep all records, paper and electronic, secured, i.e., locked file cabinets and password and/ or encrypted computers; 5) Develop Authorization Forms and Business Associate Agreements; and 6) Complete a Risk Assessment and Risk Management Plan; and 7) Notify patients if any PHI or ePHI is disclosed without authorization by the clinician or a Business Associate.

2. **Which clinicians must become HIPAA compliant?**

   The HIPAA Privacy and Security Standards regulate only "Covered Entities". Clinicians are Covered Entities under HIPAA only if they conduct any HIPAA covered transactions (see definition below) electronically. If a clinician does not conduct one of the covered transactions electronically, technically he or she does not need to be in compliance with HIPAA standards. However, it is advisable for all clinicians to become familiar with HIPAA standards as they are likely to become the basis for standard practice in all areas of health information confidentiality.

3. **When do clinicians need to be HIPAA compliant with the Privacy and Security Standards?**
   Any clinician who is, or becomes, a Covered Entity by completing a covered transaction must be in compliance with the HIPAA Privacy and Security Standards.

4. **What is a "Covered Entity"?**

   A Covered Entity is any health plan, health care clearinghouse or any health care provider who conducts HIPAA covered transactions in electronic form.

5. **What is Protected Health Information (PHI) and electronic Protected Health Information (ePHI)?**

   Protected Health Information (PHI) is health information that is identifiable to a specific individual and that is maintained or transmitted by a Covered Entity in any form, whether in oral, paper, or electronic form and subject to the HIPAA Privacy Standards. Electronic Protected Health Information (ePHI) which is stored electronically is therefore subject to the HIPAA Security Standards.

6. What are "covered transactions"?

A covered transaction is any computer-to-computer or computer-to-fax transmission of healthcare claims, payment and remittance, benefit information, or health plan eligibility information. There are eight covered transactions in all. The covered transactions most commonly used by clinicians include:

- *Health Care Claims (request for reimbursement by a provider to a health plan for health care services);*
- *Eligibility for Treatment (request for information by a provider to a health plan about eligibility, coverage limits, and/or benefits in a health plan for a client or potential client);*
- *Authorization for Treatment (request made to a health plan for authorization of mental health treatment by a mental health provider); and*
- *Health Care Claims Status (request by a mental health provider to a health care plan).*

7. What does "minimum necessary" mean in disclosing PHI or ePHI?

"Minimum necessary" is a description of the principle behind all disclosures of PHI without an authorization to do so. This means that the information disclosed is the "minimum necessary" for the specific disclosure, i.e., information being disclosed for payment purposes does not require information about the treatment progress. The major exception to the "minimum necessary" principle is when the treatment itself is being discussed, i.e., in supervision or consultation. Minimum necessary does not apply to releases with proper authorization to release PHI or ePHI.

8. What is a "Business Associate"?

Stated generally, a Business Associate is a person or entity who performs certain functions or activities that involve the disclosure of PHI or ePHI. Employees or volunteers serving at the direction of a clinician are not considered Business Associates. Examples of Business Associates are a third-party billing company, an accountant, or a transcription service that transcribes information for a clinician.

9. What is the "Notice of Privacy Practices" (NPP)?

The Notice of Privacy Practices informs a patient about the privacy practices of the clinician. The NPP must include information about how the clinician may disclose PHI about the patient; the rights of the patient to have access to the record; who is responsible for the development and implementation of the NPP; and the right of the patient to correct the record, among other information. The patient must sign the NPP at the first date of service except in emergency situations.

10. What are "Psychotherapy Notes"?

The HIPAA Privacy Standards define Psychotherapy Notes as notes recorded by a mental health professional documenting or analyzing the contents of conversation during a counseling session and that are separated from the rest of the individual's medical record. Records meeting the definition of psychotherapy notes maintain additional protection under the Privacy Standards. Disclosures of psychotherapy notes to third parties require prior patient authorization.

11. Can patient information be disclosed for marketing purposes?

Patient information cannot be disclosed for marketing purposes without an Authorization form signed by the patient. The Privacy Standards contain a detailed definition of the term "marketing", which contains a number of significant exceptions. These exceptions permit communications by a health care provider about his or her own services and those related to the treatment of the individual. Use of health information for other communications that encourage the purchase of a product or service, or the sale of information to a third party for marketing purposes clearly falls within the definition of marketing and is not permitted without prior patient authorization.

12. What is TPO (Treatment, Payment, and Health Care Operations)?

Treatment, Payment, and Health Care Operates, are terms in the HIPAA Privacy Standards which define the general scope of permissible uses and disclosures of health information that may be made without a specific authorization from the patient. Specifically, these terms are defined as follows:

- *"Treatment" – for purposes of coordinating or consulting on a patient's treatment or referring a patient for treatment;*
- *"Payment" – for purposes of obtaining reimbursement for treatment provided, collections, utilization review activities, or determining eligibility; and*
- *"Health Care Operations" – for purposes of conducting administrative, legal or other functions necessary to support treatment and payment including audits, quality assessment, or assessment of benefit plans.*

There are certain types of highly confidential information such as psychotherapy notes (see definition above) and drug treatment information that require prior authorization from the patient, even if the disclosure is for purposes of TPO. Also note that although a formal authorization may not be required for uses and disclosures of information that fall within the scope of TPO, clinicians must comply with the requirements for distribution of a Notice of Privacy Practice.

13. What is Electronic Data Interchange (EDI)?

Electronic data interchange (EDI) is any computer-to-computer transmission of routine business information using publicly available standards. The HIPAA EDI standards will permit clinicians to exchange data electronically and process the information on computers with less human interaction.

14. Are telephone calls and faxes about patients considered to be communications in "electronic form"?

Telephone calls and paper faxes are not considered to be communications in "electronic form" for purposes of determining whether a health care provider is a "Covered Entity" under HIPAA (see above). However, regulators appear to be treating faxes sent by computer as communications in electronic form and thus, to the extent a clinician engages in one of the covered transactions by such means, such clinician is probably a Covered Entity.

15. Are special kinds of software necessary to comply with the HIPAA Privacy Standards?

No. The Privacy Standards do not specifically require special software in order to achieve compliance. However, the Privacy Standards do require Covered Entities to have in place "appropriate administrative, technical, and physical safeguards to protect the privacy of health information." Each clinician must apply this general standard to his or her own particular work environment. Simple steps such as utilizing the password or encryption features built into existing software and operating systems may be sufficient. In other cases, particularly where patient information is transferred via the Internet, more elaborate measures may need to be taken in order to meet the "appropriate safeguards" standard. Such measures may include acquisition and installation of firewalls, anti-virus software, or other mechanisms to protect patient data.

16. What effect will HIPAA Standards have on privacy standards in general?

The impact of HIPAA Standards on what will be considered reasonable privacy practices cannot be underestimated. HIPAA Standards will become expected practice for all clinicians, whether they are HIPAA compliant or not.

17. What are the penalties for HIPAA violations?

Civil penalties are $100 for each violation up to $25,000 per year. Criminal penalties are up to $250,000 in fines and up to 10 years in jail.

18. What Federal agency has oversight of HIPAA standards and receives complaints?

The Department of Health and Human Services (HHS) has overall responsibility for implementation of HIPAA Privacy Standards. The Office of Civil Rights (within HHS) maintains the enforcement responsibility. The Transaction and Code Set Standards fall under the Center for Medicare and Medicaid Services (CMS).

19. Are the Security Standards and Privacy Standards the same in the kinds of communications they cover?

No. The Security Standards apply only to electronic transmissions or data storage of electronic Protected Health Information (ePHI). The Privacy Standards apply to verbal, written and electronic transmission of Protected Health Information (PHI).

20. Do I have to comply with Security Standards if I am not a Covered Entity (CE)?

No. The Security Standards apply only to clinicians who are Covered Entities, i.e., who have sent Protected Health Information electronically at least once.

21. What is the purpose of the Security Standards?

To maintain the confidentiality of ePHI; to prevent changes to ePHI, i.e., maintain the integrity of the electronic data); to maintain availability to ePHI; to prevent unidentified electronic access to ePHI; and to prevent physical access by unidentified personnel to areas and computers holding ePHI.

22. Is "encryption" required to protect any ePHI that is transmitted?

No. Encryption is a computer program that disguises all ePHI that was originally required as part of the Security Standards but is optional at this time. Both the sender and receiver must have the same program to use encryption. Some insurers may use encryption and supply providers with the program they use.

23. What kinds of security procedures are used by insurers for protecting ePHI if encryption is not?

Most insurers are beginning to use "secure servers" which allow the insurer and the provider to log on to a secure website with passwords and exchange information there, e.g., Office Ally.

24. What is the difference between "required" and "addressable" areas of the Security Standards?

"Required" areas must be covered in the Risk Management Plan; "addressable" areas may be covered in the Risk Management Plan, but are optional.

25. What is a Risk Assessment?

A Risk Assessment is an evaluation of 39 required and 4 optional items which are identified in the Security Standards.

26. What is a Risk Management Plan and is it necessary to have one to be compliant?

A Risk Management Plan is the documentation of how required Security Standards will be implemented. All Covered Entities need to have conducted a Risk Assessment and develop a Risk Management Plan to be compliant with HIPAA Security Standards.

27. Is external auditing of the Risk Management Plan necessary?

No, but it may be conducted by qualified reviewers if desired. A "certification" will not remove responsibility for compliance from the CE.

28. **Is it necessary to 'back up' all ePHI on disc or CD to be compliant with HIPAA Security Standards?**
Yes.

29. **If ePHI is lost due to theft or natural disaster, is that considered a violation of the Security Standards?**

Yes, if reasonable precautions according to the Security Standards have not been followed.

30. **Is an 'audit trail' required when to disclose ePHI?**

No, but a record of all disclosed ePHI is required. An audit trail would be considered a best practice.

31. **Are a firewall, passcode (i.e., password), and other computer security systems needed to be compliant with the Security Standards?**

Yes.

32. **Is it necessary to regularly change computer passwords to be compliant with Security Standards?**
Yes.

33. **What are the civil and criminal penalties for violating the Security Standards?**

The civil penalties are up to $25,000 per year for every violation with a $1.5 million dollar cap for identical violations. The criminal penalties for purposeful violations are up to 10 years in prison and $250,000.

34. **How many times does a provider need to send ePHI electronically, when it is a covered transaction, to be considered a Covered Entity? What forms of transmission are considered covered transactions?**

If a provider sends ePHI which is a covered transaction electronically once, the provider is a Covered Entity. Covered transactions include computer to computer transmissions; computer fax to computer or paper fax transmissions, and key pad telephone transmissions. Covered transactions do not include paper to paper faxes or voice mail transmissions.

35. **What happens if a Covered Entity loses ePHI through computer error or inadequate security procedures?**

The Covered Entity is responsible for the security of all ePHI and may be found in violation of HIPAA Security Standards.

36. **Does a provider need to guarantee the confidentiality of a paper to paper fax?**

While the Security Standards do not specifically address this issue, they do require that ePHI be kept confidential. Also note that the Privacy Standards apply to all forms of PHI. Therefore, a Covered Entity should ensure the privacy of PHI sent on paper to paper faxes.

37. What are the security risks a Covered Entity should consider in doing a Risk Assessment?

A Risk Analysis should include risks to the computer systems containing ePHI, and all PHI generated in paper or electronic form from computer systems, which may be unintentional or intentional. The risks considered include administrative, technical and physical risks to the confidentiality and integrity of ePHI.

38. Is a Covered Entity required to notify a patient if any PHI or ePHI is released without authorization?

Yes, unless the Covered Entity can show that there is a low probability that the PHI or ePHI has been compromised. Otherwise, a letter must be sent to the patient which explains all the information that was disclosed without authorization, when it was disclosed and to whom.

39. Is a Covered Entity required to notify a patient if any PHI or ePHI is released without authorization by a Business Associate?

Yes, unless the Covered Entity can show that there is a low probability that the PHI or ePHI has been compromised. Otherwise, a letter must be sent to the patient which explains all the information that was disclosed without authorization, when it was disclosed and to whom.

[This page intentionally left blank.]

Appendix 2: "Confidentiality" Section from Clinical Social Work Association's Code of Ethics (1997 Edition)

Confidentiality

Clinical social workers have a primary obligation to maintain the privacy of both current and former clients, whether living or deceased, and to maintain the confidentiality of material that has been transmitted to them in any of their professional roles. Exceptions to this responsibility will occur only when there are overriding legal or professional reasons and, whenever possible, with the informed consent of the client(s).

(a) Clinical social workers discuss fully with clients both the nature of confidentiality, and potential limits to confidentiality that may arise during the course of their work. Confidential information should only be released, whenever possible, with the written permission of the client(s). As part of the process of obtaining such a release, the clinical social worker should inform client(s) about the nature of the information being sought, the purpose(s) for which it is being sought, to whom the information will be released, how the client(s) may withdraw permission for its release, and the length of time that the release will be in effect.

(b) Clinical social workers know and observe both legal and professional standards for maintaining the privacy of records, and mandatory reporting obligations. Mandatory reporting obligations may include, but are not limited to: the reporting of abuse or neglect of children or of vulnerable adults; the duty to take steps to protect or warn a third party who may be endangered by the client(s); and, the duty to report the misconduct or impairment of another professional. Additional limits to confidentiality may occur because of parental access to the records of a minor; the access of legal guardians to the records of some adults; access by the courts to mandated reports; and access by third party payers to information for the purpose of treatment authorization or audit. When confidential information is released to a third party, the clinical social worker will ensure that the information divulged is limited to the minimum amount required to accomplish the purpose for which the release is being made.

(c) Clinical social workers treating couples, families, and groups seek agreement among the parties involved regarding each individual's right to confidentiality, and the mutual obligation to protect the confidentiality of information shared by other parties to the treatment. Clients involved in this type of treatment should, however, be informed that the clinical social worker cannot guarantee that all participants will honor their agreement to maintain confidentiality.

(d) When confidential information is used for purposes of professional education, research, or publication, the primary responsibility of the clinical social worker is the protection of the client(s) from possible harm, embarrassment, or exploitation. When extensive material is used for any of these purposes, the clinical social worker makes every effort to obtain the informed consent of the client(s) for such use, and will not proceed if the client(s) denies this consent. Whether or not a consent it obtained, true identity of the client. Any such presentation will be limited to the amount necessary for the professional purpose, and will be shared only with responsible individuals.

(e) The development of new technologies for the storage and transmission of data poses a greater danger to the privacy of individuals. Clinical social workers take special precautions to protect the confidentiality of material stored or transmitted through computers, electronic mail, facsimile machines, telephones, telephone answering machines, and all other electronic or computer technology. When using these technologies, disclosure of identifying information regarding the client(s) should be avoided whenever possible.

From the Clinical Social Work Association Code of Ethics, pp. 7–9, 1997.

Appendix 3: Enforcement of HIPAA Violations (From the Office of Civil Rights Enforcement Statistics for HIPAA Violations, December, 2013)

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html

Enforcement Highlights

(As of December 31, 2013)

The HIPAA Privacy Rule is a set of federal standards to protect the privacy of patients' medical records and other health information maintained by covered entities: health plans, which include many governmental health programs, such as the Veterans Health Administration, Medicare and Medicaid; most doctors, hospitals and many other health care providers; and health care clearinghouses. These standards provide patients with access to their medical records and with significant control over how their personal health information is used and disclosed. Compliance with the standards was required as of April 14, 2003 for most entities covered by HIPAA. On that date, OCR began accepting complaints involving the privacy of personal health information in the health care system.

The HIPAA Security Rule establishes national standards for the security of electronic protected health information. The final rule adopting HIPAA standards for security was published in the Federal Register on February 20, 2003. This final rule specifies a series of administrative, technical, and physical security procedures for covered entities to use to assure the confidentiality of electronic protected health information. The standards are delineated into either required or addressable implementation specifications. Compliance with the standards was required as of April 20, 2005, for most entities covered by HIPAA. The authority to administer and enforce the Security Rule was transferred to OCR on July 27, 2009.

Enforcement Results as of the Date of This Summary

- HHS / OCR has investigated and resolved over 22,026 cases by requiring changes in privacy practices and other corrective actions by the covered entities. Corrective actions obtained by HHS from these entities have resulted in change that is systemic and that affects all the individuals they serve. HHS has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates noncompliance by the covered entity. OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.

- In another 9,899 cases, our investigations found no violation had occurred.

- In the rest of our completed cases (52,629) HHS determined that the complaint did not present an eligible case for enforcement. These include cases in which:

    - OCR lacks jurisdiction under HIPAA – such as a complaint alleging a violation prior to the compliance date or alleging a violation by an entity not covered by HIPAA;

    - the complaint is untimely, or withdrawn or not pursued by the filer;

    - the activity described does not violate the Rules – such as when the covered entity has disclosed protected health information in circumstances in which the Rules permits such a disclosure.

- In summary, since the compliance date in April 2003, HHS has received over 90,001 HIPAA complaints. We have resolved ninety-four percent of complaints received (over 84,554): through investigation and enforcement (over 22,026); through investigation and finding no violation (9,899); and through closure of cases that were not eligible for enforcement (52,629).

From the compliance date to the present, the compliance issues investigated most are, compiled cumulatively, in order of frequency:

1. Impermissible uses and disclosures of protected health information;
2. Lack of safeguards of protected health information;
3. Lack of patient access to their protected health information;
4. Uses or disclosures of more than the minimum necessary protected health information; and
5. Lack of administrative safeguards of electronic protected health information.

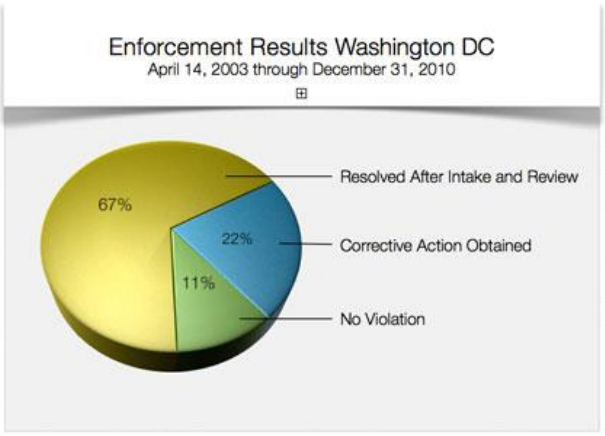
The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:

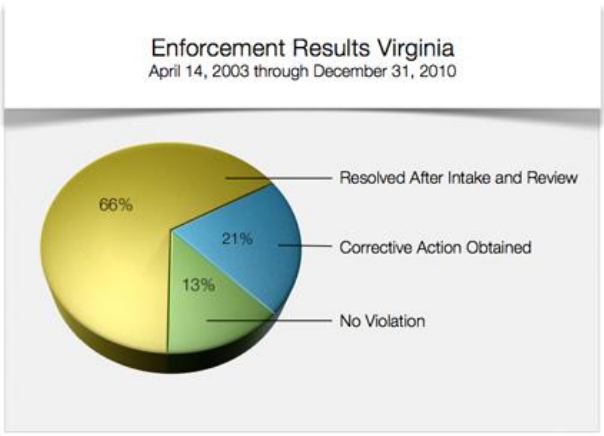
1. Private Practices;
2. General Hospitals;
3. Outpatient Facilities;
4. Health Plans (group health plans and health insurance issuers); and,
5. Pharmacies.

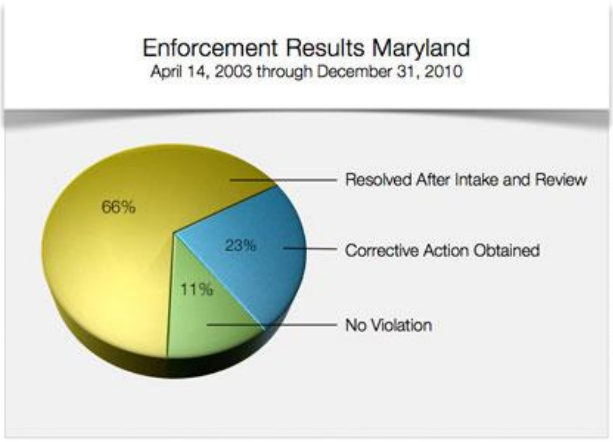
Security Rule Enforcement Results as of the Date of This Summary

- With regard to the subset of complaints specifically pertaining to the Security Rule, since OCR began reporting its Security Rule enforcement results in October 2009, HHS has received approximately 777 complaints alleging a violation of the Security Rule. During this period, we closed 584 complaints after investigation and appropriate corrective action. As of December 31, 2013, OCR had 258 open complaints and compliance reviews.

Enforcement Results by GWSCSW States/Jurisdictions (12/31/10)







Appendix 4

U.S. Department of Health and Human Services Office for Civil Rights [found on disc]

Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 and 164)

Regulation Text (December 28, 2000) as amended:

Part 160 (May 31, 2002)

Parts 160, 164 (August 14, 2002)

[This page intentionally left blank.]

Appendix 5: Matrix for GAP Analysis

HIPAA Privacy Requirement: GAP Analysis and Timeline	YES	NO	Section Reference
1. Have you designated, in writing, a Privacy Official to carry out the requirements of the HIPAA privacy standards?			
2. Have you designated, in writing, an individual as the contact person for complaints and for providing privacy information?			
3. Do you have a process that assures Notices of Privacy Practices is available to each appropriate individual?			
4. Have you developed a process that acknowledges receipt of the Notice of Privacy Practices (NPP) document in writing?			
5. Have you included language in your Notice of Privacy Practices stating the right to change a privacy practice? If so, do you have a policy for how to distribute changes in privacy practice?			
6. Do your existing consent and authorization to release information forms reference the NPP and are you aware of the types of information you can release without consent and authorization forms?			
7. Do you have a method for carefully reviewing the Use and Disclosure of Protected Health Information (PHI) in the first meeting with clients? Are you familiar with the rights of clients to restrict the use of PHI? Finally do you understand that you are not necessarily required to agree with the restriction?			
8. Does your Authorization document contain all the required elements for Disclosure of PHI? This includes: • A specific description of the information to be disclosed • The name or other specific identification of the person(s) making the request • Expiration date (note Research) • A statement of the Individual's right to revoke • Statement that information Used or Disclosed may be subject to re-disclosure • Signature and date • If signed by a representative, a description of the authority.			
9. Does your NPP clearly state that you may disclose limited PHI but must allow individual to object under limited circumstances?			
10. Are you familiar with the special circumstances that would allow for the Disclosure of PHI without Authorization and do you have policies that outline these restrictions?			
11. Are clients notified of uses and disclosures that may be made routinely or without Authorization?			

HIPAA Privacy Requirement: GAP Analysis and Timeline	YES	NO	Section Reference
12. HIPAA allows release of limited PHI without authorization for fundraising. Do you have a policy and disclosure information that addresses this issue?			
13. Do you have an opt-out procedure allowing clients to withdraw their information form fund raising activities?			
14. Do you currently maintain a record of disclosure of PHI in the case record?			
15. Have you identified your Business Associates and determined where a contract must be in place?			
16. Do you maintain records for at least six years?			
17. Do you have language in your NPP that clients have the right to access their PHI along with policies about accessing that information?			
18. Are you aware of your rights and obligations when individuals requests an amendment to their case record?			
19. Do you have a process in place for clients to amend their record?			
20. Can you accommodate clients who request to receive PHI at an alternative location or by alternative means?			
21. Do you understand the HIPAA concept of “Minimum Necessary” for PHI disclosures?			
22. Are you aware of the concept of “de-identification” and the 19 identifiers, the absence of which frees PHI for disclosure?			
23. Do you understand what a Limited Data Set is and when Disclosure is permissible?			
24. Do you keep records of HIPAA training sessions?			
25. Do you keep attendance records of those training sessions?			
26. Do you have policies that deal with breaches in confidentiality?			
27. Are you aware of the consequences of violating breaches in confidentiality?			
28. Do you have a procedure for handling complaints regarding your policies and procedures.			
29. Do you have language in your NPP that says clients will not be asked to waive their rights to file a complaint as a condition of treatment?			
30. Have you included language in your NPP notifying clients of their right to file a complaint with the Department of Health and Human Services?			
31. Have you included language in your NPP about the procedure for filing a complaint and the timeline for doing so?			

HIPAA Privacy Requirement: GAP Analysis and Timeline	YES	NO	Section Reference
32. Are you aware that a Covered Entity may not intimidate, threaten, coerce, discriminate or retaliate against a client for filing a complaint?			
33. Do you have policies that restrict access to PHI?			
34. Are you (and your staff) aware of the importance of the consistent handling of PHI in all aspects (such as telephone, faxing, file handling, public conversations etc.) of practice?			
35. Do you have a security policy in place to protect electronic PHI?			
36. Is there someone designated to develop and implement Policies and Procedures to carry out the requirements of the HIPAA privacy standards?			
37. Is there someone designated to maintain and update Policies and Procedures and to carry out the requirements of the HIPAA Privacy standards as they change?			
38. Are your policies and procedures managed in a way that would allow employees access to them for the last six years?			
39. Do you have date sensitive standards for all documentation in written or electronic form?			
40. Is staff educated on the organization's HIPAA implementation timeline, which provides for a transition period for using existing consents and Authorizations?			
41. Do you have an action plan for contacting payers to determine their HIPAA readiness prior to the implementation date?			
42. Are you familiar with the laws of your State regarding medical records and other health information?			
43. Does your organization have a process in place to respond to requests for information and documentation from the Secretary of HHS?			
44. Are employees trained on their responsibility to cooperate with the Secretary of HHS regarding all			

1. **Have you designated a Privacy Official to carry out the requirements of the HIPAA privacy standards?**

   Covered Entities must designate a Privacy Official who is responsible for the development and implementation of the Policies and Procedures of the Covered Entity and a contact person or office to receive complaints and provide further information about the Covered Entity's privacy practices.

2. **Is there an employee among your staff designated as the contact person for complaints and providing privacy practice information?**

   Covered Entities must designate a Privacy Official who is responsible for the development and implementation of the Policies and Procedures of the Covered Entity and a contact person or office to receive complaints and provide further information about the Covered Entity's privacy practices.

3. **Are you familiar with the requirements regarding Notices of Privacy Practices and do you have a process for assuring that this information is available to every appropriate Individual?**

   Openly display privacy notice in waiting areas. Have copies available. Create or update current policies to include privacy policy. Post on website if you have one. Covered Entities must provide Individuals with Notice of Privacy Practices at the time of first delivery of service after the compliance date. A Covered Entity must document compliance with the notice requirements by retaining a copy of each version of notices issued and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment and reasons why it was not obtained.

4. **If you are a Direct Treatment Provider have you developed an acknowledgement of receipt of the Notice of Privacy Practices document and process?**

   Acknowledgement must be in writing. If you cannot get written acknowledgement, document why you cannot.

   Except in an emergency Treatment situation, a Direct Treatment Provider must make a good faith effort to obtain a written acknowledgment of receipt of the notice provided and, if not obtained, document its good faith efforts to obtain such acknowledgment and the reasons why the acknowledgment was not obtained.

5. **Are you familiar with the section of the HIPAA privacy regulations regarding your rights to change privacy practices and the notification required to do so?**

   Include language stating the right to change privacy practice. Have a policy for how to distribute changes in privacy practice, i.e., how will you get it out to people. If a Covered Entity has not reserved its right to change a privacy practice described in the Notice, the Covered Entity is bound by the privacy practices stated in the Notice with respect to PHI created or received while the Notice is in effect.

6. **Are you aware of the Uses and Disclosures of PHI allowed by the regulations to carry out Treatment, Payment or Health Care Operations (TPO)?**

   Update existing forms and add language referencing the NPP. Update P&P to include requirements for obtaining authorizations. Privacy regulations allow Uses and Disclosure of PHI for TPO, but require written authorization for almost all other Uses or Disclosures not required by law.

7. **Do you fully understand your rights and those of patients who may request restrictions on the Use and Disclosure of their PHI?**

   Carefully review uses and disclosure of PHI in first meeting with client. Ask patient to identify restrictions on PHI. Include language in NPP that patients have the right to request in writing restrictions on the uses and disclosure of PHI and that Covered Entity is not required to agree with the restriction. Evaluate you system to determine if the requested restriction is possible given your information systems. If not, address this inability in the notice.

   A Covered Entity must allow an Individual to request that the Covered Entity restrict the use and disclosure of PHI:

   - *Uses or Disclosure for TPO, and*
   - *Disclosures permitted for involvement in the Individual's care and notification purposes.*
   - *The Covered Entity is not required to agree to the restriction.*

8. **Does your Authorization document contain all the required elements for Disclosure of PHI?**

   Specify the intended use of PHI in an authorization form. Indicate in the document that authorizations are for release of information that is not TPO. In general, but with specific exceptions, written Authorization is required for any Use or Disclosure of PHI not for TPO. Core elements of an Authorization are:

   - *A specific description of the information to be disclosed*
   - *The name or other specific identification of the person(s) making the request*
   - *Expiration date (note Research)*
   - *A statement of the Individual's right to revoke*
   - *Statement that information Used or Disclosed may be subject to re-disclosure*
   - *Signature and date*
   - *If signed by a representative, a description of the authority.*

9. **Is your Notice of Privacy Practices documentation written to clearly illustrate the limited situations where an Individual has the right to agree or object to the disclosure of information, and is this information displayed in a visible location?**

   Update NPP to state that facilities may disclose limited PHI but must allow individual to object under limited circumstances. Make sure your system can block the information client doesn't want released. PHI may be disclosed by a Covered Entity without the Individual's Authorization when used for facility directories (for clergy and other visitors), or to update family members and others involved in the Individual's care, provided the Individual is given an opportunity in advance to object.

10. Is your Workforce familiar with the special circumstances that would allow for the Disclosure of PHI without Authorization?

Develop detailed policies outlining each of these uses and disclosures with elements necessary for compliance. Include in NPP organizations duty to use and disclosure other than TPO without authorization in limited circumstances pursuant to HIPAA standards. A Covered Entity may (must) use or disclose PHI without written Authorization of the Individual in the certain limited circumstances, such as those required by law or public health activities.

11. Are patients notified of uses and disclosures that may be made routinely or without Authorization?

Develop detailed policies outlining each of these uses and disclosures with elements necessary for compliance. Include in the NPP the organization's duty to use and disclose for other than TPO without authorization in limited circumstances. A Covered Entity may (must) use or disclose PHI without written Authorization of the Individual in the certain limited circumstances, such as those required by law or public health activities.

12. Do you know what PHI may be used for Fund-raising activities?

Inform individuals of their right to opt out of this by including a statement of choice. Include policy. Covered Entities may use limited PHI (demographics and dates of service), without Authorization, for Fund-raising activities. Covered Entities may use or disclose to a Business Associate or to an institutionally related foundation, PHI for the purpose of raising funds.

13. Do you have an opt-out procedure that allows patients to withdraw their information from Fund-raising activities?

Inform individuals the right to opt out of fundraising activities. Covered Entities may use limited PHI (demographics and dates of service), without Authorization, for Fund-raising activities. Covered Entities may use or disclose to a Business Associate or to an institutionally related foundation, PHI for the purpose of raising funds.

14. Are you currently documenting medical record disclosures on your patients?

Maintain records of disclosures of PHI outside of TPO. Include dates of release, description of info released and to whom it was released. Incorporate individual's right to receive record of disclosure of PHI in NPP for six years beginning April 14, 2003. An Individual has the right to receive an accounting of the Disclosures of their PHI made by the Covered Entity in the six years prior to the request with exceptions for TPO and certain other circumstances.

15. Can you identify the situations where a Business Associate Contract must be in place?

Identify BA and contact them to determine HIPAA awareness. Revise or create contracts to include HIPAA requirements for PHI. Have Business Associates sign contracts. Disclosures of PHI may be made to Business Associates where a Business Associate Contract is in place.

16. **Are your medical files and/or management system data retained for at least 6 years?**

    The individual has a right to inspect and copy his or her protected health information (PHI), in whole or in part, for as long as the Covered Entity maintains the information. Include language in NPP that clients have right to access PHI. Record requests to access information in the file. Develop P&P for handling requests for access including review process if access is denied. Develop P&P for access to electronic information.

17. **Are your medical files and/or patient information systems managed in a way that allows for patient inspection and/or release of files?**

    Include language in NPP that clients have the right to access their PHI. Record requests must be documented in the individual's file. The individual has a right to inspect and copy his or her protected health information (PHI), in whole or in part, for as long as the Covered Entity maintains the information.

18. **Are you aware of your obligations and rights should an individual request amendments be made to PHI in the Designated Record Set?**

    An Individual has the right to have a Covered Entity amend his or her PHI in a Designated Record Set for as long as the Covered Entity maintains the information.

19. **If yes, do you have a process in place for doing so?**

    An Individual has the right to have a Covered Entity amend his or her PHI in a Designated Record Set for as long as the Covered Entity maintains the information. Include the individual's right to amend PHI in NPP and indicate process for making this change. Implement procedures to approve or deny amendments to Designated Record Sets or to resolve disputes and document approval or denial in the record.

20. **Do you have a mechanism in place to accommodate those Individuals that may request to receive communications of PHI by an alternative means or at an alternative address?**

    A Provider must permit Individuals to request, and must accommodate reasonable requests by Individuals to receive communications of PHI by the Provider by alternative means or at alternative locations. Verify contact information. Include in P&P when you are willing to provide health information to an alternative address or by alternative means.

21. Do you and/or your staff have a complete understanding of what is considered "Minimum Necessary" for various Disclosures of PHI?

A Covered Entity must limit Use or Disclosure of PHI to the Minimum Necessary to carry out the intended purpose of the request. Establish level of access each individual in workforce has to PHI to complete job. Establish access levels to PHI using passwords and logins as determined by job duties. Update policies governing use and disclosure of PHI, such as for claims payment limiting info to that required for a specific billing event. Use examples to train employees on Minimum Necessary requirements. Make sure manuals have P&P for dealing with infractions. Develop procedures implementing the Minimum Necessary requirement eg ensure that reports that are sent outside agency have only the MN information to comply with the nature of the request.

22. Are you aware of the 19 identifiers that de-identify PHI data and frees the data for disclosure?

a. *Individual health information loses its HIPAA protections and may be used or disclosed freely if it cannot be used to identify an individual. Implement a policy that requires senior level authorization for release of de-identified PHI. Develop a checklist of the 19 identifiers for de-identifying PHI. Review existing reports to see if any of the 19 identifiers are present. Evaluate recipients need for the information. If identifiers are present determine need and create BA relationship. Find out if software vendors provide de-identifiers as a feature.*

   Other requirements relating to uses and disclosures of protected health information.

   Standard: de-identification of protected 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 is not individually identifiable health information.

   Implementation specifications: requirements for de-identification of protected health information. A Covered Entity may determine that health information is not individually identifiable health information only if:

   1. *A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:*

   2. *Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and*

   3. *Documents the methods and results of the analysis that justify such determination; or*

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

- *Names;*
- *All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:*
    - *The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and*
    - *The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.*
- *All elements of dates (except year) for dates directly related to an 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 age, except that such ages and elements may be aggregated into a single category of age 90 or older;*
- *Telephone numbers;*
- *Fax numbers;*
- *Electronic mail addresses;*
- *Social security numbers;*
- *Medical record numbers;*
- *Health plan beneficiary numbers;*
- *Account numbers;*
- *Certificate/license numbers;*
- *Vehicle identifiers and serial numbers, including license plate numbers;*
- *Device identifiers and serial numbers;*
- *Web Universal Resource Locators (URLs);*
- *Internet Protocol (IP) address numbers;*
- *Biometric identifiers, including finger and voice prints;*
- *Full face photographic images and any comparable images; and*
- *Any other unique identifying number, characteristic, or code except as permitted by paragraph (c) of this section; and*

c. The Covered Entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

23. Do you and your staff understand what constitutes a Limited Data Set and when Disclosure is permissible?

A Covered Entity may use or disclose a Limited Data Set if the Covered Entity enters into a Data Use Agreement with the Limited Data Set recipient. A Covered Entity may use or disclose a limited data set only of the CE obtains satisfactory assurance in the form of a Data Use Agreement. It must include the requirement that the recipient use or disclose the PHI for limited purposes. This remains PHI and protected by privacy regulations and MN restrictions but it does not need to be tracked for accounting to the individual.

24. Do you currently hold training sessions (or staff meetings) to facilitate PHI training?

A Covered Entity must train members of its Workforce about the Covered Entity's Policies and Procedures for PHI and document that training has been provided. Provide training to personnel about PHI. Identify P&P that deal with PHI and cover those policies. Document training employees have taken. Conduct PHI training upon hiring and provide annual updates. Have employees sign documentation of completion of update training.

25. Do you maintain records of those in attendance at training sessions?

A Covered Entity must train members of its Workforce about the Covered Entity's Policies and Procedures for PHI and document that training has been provided.

26. Do you have a policy in place designed to handle a breach in confidentiality?

A Covered Entity must have and apply appropriate sanctions against its employees who fail to comply with the Covered Entity's privacy Policies and Procedures or the regulations. Specify in employee manual penalties for privacy infractions. Review at hiring and refresher trainings.

27. Are you and your office staff aware of the ramifications of violating an Individual's rights under the new Standards?

A Covered Entity must have and apply appropriate sanctions against its employees who fail to comply with the Covered Entity's privacy Policies and Procedures or the regulations. Specify policy and review at hiring and retraining.

28. Does your organization currently have a course of action for complaints?

A Covered Entity must provide a process for individuals to make complaints concerning its Policies and Procedures regarding its compliance with the requirements of the regulation. Include steps in NPP to file complaints. Be sure to document complaints and their nature.

29. Do you convey objective behavior and/or opinions regarding complaints?

A Covered Entity may not require an individual to waive his or her right to file a complaint with the DHHS as a condition of Treatment, Payment, and enrollment in a Health Plan, or eligibility for benefits.

Include language in Policies and Procedures and in the NPP that clients will not be asked to waive rights to receive treatment.

30. Have you included in your Notice of Privacy Practices the right for Individuals to file a complaint with the Secretary of HHS?

Any person who believes that a Covered Entity is not complying with the applicable requirements of HIPAA may file a complaint with the Secretary of HHS. Include a section in NPP on complaints.

31. Have you included in your Notice of Privacy Practices the process by which individuals may file a complaint with the Secretary of HHS?

A complaint must be filed within 180 days of when the complainant knew or should have known that the act or omission complained of occurred unless the HHS Secretary for good cause shown waives the time limit. Be sure to include time frame for filing a complaint, the fact that it must be in writing and include the entity's name.

32. Is your staff encouraged to report areas of potential non-compliance with the new Standards?

A Covered Entity may not intimidate, threaten, coerce, discriminate or retaliate against an Individual.

Include in training, management's philosophy of adhering to policies on privacy. Train your staff to make sound decisions, to follow procedures and report to privacy officer any problems. You cannot take action against anyone who files complaint (employee) or is participating in an investigation. Individuals can choose not to participate in any action they believe is illegal as long as it is reasonable and does not involve a disclosure of PHI that is unlawful.

33. Do you have policies in place to secure and restrict access to PHI consistent with HIPAA requirements?

A Covered Entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and reasonably safeguard PHI from any intentional or unintentional Use or Disclosure, or violation of the requirements of the regulation. Have staff sign confidentiality agreements. Include security awareness as part of initial training and update. Lock file cabinets containing PHI. Train staff to limit conversations containing PHI to private locations.

34. Is your staff aware of the importance of consistent confidentiality practices when handling files, answering the phone, faxing, etc.?

A Covered Entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and reasonably safeguard PHI from any intentional or unintentional Use or Disclosure, or violation of the requirements of the regulation. Use logins and passwords, secure computers, and assure that non-electronic PHI is secured.

35. Do you have a security policy to protect electronic medical information?

A Covered Entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and reasonably safeguard PHI from any intentional or unintentional Use or Disclosure, or violation of the requirements of the regulation. Again, use logins and passwords, make sure computers are secured from unauthorized use, and assure that access to non-electronic PHI is secured.

36. Is there an employee among your staff designated to develop and implement Policies and Procedures to carry out the requirements of the HIPAA privacy standards?

A Covered Entity must develop and implement Policies and Procedures relating to PHI that are designed to comply with the elements of the regulations. Standards are scalable to assure that Policies and Procedures are relevant to the organization and the amount of PHI contained therein.

37. Is there an employee among your staff designated to maintain and update Policies and Procedures and to carry out the requirements of the HIPAA Privacy and Security Standards?

A Covered Entity must revise its Policies and Procedures as necessary and appropriate to comply with changes in the law or regulations, when it changes a privacy practice that is stated in its Notice of Privacy Practices, or when a security practice changes.

38. Are your policies and procedures managed in a way that would allow employees access to them for the last six years?

A Covered Entity must maintain its Policies and Procedures in written or electronic form for six years from the date of its creation or the date when it last was in effect, whichever is later. Make copies available to employees and update annually. Make electronic copy available when possible and index in such a way that employees can tell which is current.

39. Do you have date sensitive standards for all documentation in written or electronic form?

A Covered Entity must retain documentation required by regulation for six years from the date of its creation or the date when it last was in effect, whichever is later. Consider "purge data date" on all electronic documentation at six years unless state law requires you to keep it longer.

40. Is your staff educated on the organization's HIPAA implementation timeline, which provides for a transition period for using existing consents and Authorizations?

A Covered Entity may continue to use or disclose an individual's PHI with the individual's consent or Authorization prior to the compliance date of the regulation. Train employees to understand this.

41. Do you have an action plan for contacting payers to determine their HIPAA readiness prior to the implementation date?

Health Care Providers, Clearinghouses, and most Health Plans must comply with the regulations no later than 24 months after the effective date of the final rule as published in the Federal Register. While sole practitioners who are not Covered Entities are not required to comply with HIPAA rules, prudent clinicians will educate themselves and be in compliance.

42. Are you familiar with the laws of your State regarding medical records and other health information?

Conflicting State Law is preempted, with certain restrictions. In particular, State Laws that are More Stringent than the regulations may take precedence. There are four exceptions to this general rule:

- *The Secretary of HHS determines that the State Law, regulation, or rule is necessary to prevent fraud and abuse related to the provision of or payment for health care;*
- *To ensure appropriate State regulations of insurance and Health Plans to the extent expressly authorized by statute or regulations;*
- *For State reporting on Health Care delivery or cost; and*
- *For purposes of serving a compelling need related to public health, safety, or welfare or if the Secretary of HHS determined that an intrusion into privacy is warranted as determined by the need.*

The broadest of these exceptions is the exception for State Laws that are "More Stringent" than the regulation. A State Law is More Stringent when it (1) prohibits or restricts a Use or Disclosure that the regulation would permit; (2) grants greater rights of access or amendment to an Individual's own PHI; (3) provides for a greater amount of information to be disclosed to an Individual upon request; (4) requires more narrowly focused or limited consents or Authorization; (5) requires more detailed record keeping; or (6) provides any other greater privacy protection.

Be aware of state laws. Consult with an attorney to determine which laws are more stringent.

43. Does your organization have a process in place to respond to requests for information and documentation from the Secretary of HHS?

Covered Entities are required to keep records of HIPAA compliance and submit compliance reports in such time and manner and containing such information as the Secretary of HHS may determine to be necessary to enable the Secretary to ascertain whether the Covered Entity has complied or is complying with the applicable requirements of the regulations. Develop summary document that outlines HIPAA activities of the organization. Maintain all documentation in the event of a request from HHS.

44. Are employees trained on their responsibility to cooperate with the Secretary of HHS regarding all investigations or compliance reviews?

It is the responsibility of a Covered Entity (CE) to cooperate with the Secretary of HHS in investigations or compliance review of policies, procedures, or practices of a CE. A CE must permit access by the Secretary of HHS during normal business hours to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the General Administrative Requirements of the HIPAA privacy rule (Part 160 of the regulation) and the standards, requirements, and implementation specifications of Privacy of Individually Identifiable Information provisions of the regulations (Part 164, Subpart E of the regulation). If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, a Covered Entity must permit access by the Secretary at any time and without notice. Organizations need to be prepared to provide accurate and updated documentation of all HIPAA privacy related policies, requests, use, and disclosures, etc. in the event that a patient files a complaint with the Secretary of HHS. Inform employees of their need to cooperate with HHS.

Appendix 6
Matrix for Risk Assessment – HIPAA Privacy and Security Rules

REQUIREMENTS FOR IMPLEMENTATION	
Chain of trust partner agreement	
Contingency plan (all listed implementation features must be implemented).	• Applications and data criticality analysis. Data backup plan. • Disaster recovery plan. Emergency mode operation plan. Testing and revision.
Formal mechanisms for processing records:	
Information access control (all listed implementation features must be implemented)	Access authorization. Access establishment. Access modification.
Internal audit	
Personnel security (all listed implementation features must be implemented)	• Assure supervision of maintenance personnel by authorized, knowledgeable person. • Maintenance of record of access authorizations. • Operating, and in some cases, maintenance personnel have proper access authorization. Personnel clearance procedure. • Personnel security policy/procedure. System users, including maintenance personnel, trained in security.
Security configuration mgmt. (all listed implementation features must be implemented)	• Documentation. • Hardware/software installation & maintenance review and testing for security features. • Inventory. Security Testing. Virus checking.
Security incident procedures (all listed implementation features must be implemented)	Report procedures. Response procedures.
Security management process (all listed implementation features must be implemented)	• Risk analysis. • Risk management. Sanction policy. • Security policy.

REQUIREMENTS FOR IMPLEMENTATION	
Termination procedures (all listed implementation features must be implemented)	• Combination locks changed. Removal from access lists. • Removal of user account(s). • Turn in keys, token or cards that allow access.
Training (all listed implementation features must be implemented)	• Awareness training for all personnel (including mgmt). • Periodic security reminders. • User education concerning virus protection. User education in importance of monitoring log in success/failure, and how to report discrepancies. • User education in password management.
PHYSICAL SAFEGUARDS TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY	
Assigned security responsibility	
Media controls (all listed implementation features must be implemented)	• Access control. • Accountability (tracking mechanism). Data backup. • Data storage. Disposal.
Physical access controls (limited access) (all listed implementation features must be implemented)	• Disaster recovery. Emergency mode operation. • Equipment control (into and out of site). Facility security plan. • Procedures for verifying access authorizations prior to physical access. Maintenance records. • Need-to-know procedures for personnel access. • Sign-in for visitors and escort, if appropriate. • Testing and revision.
Policy/guideline on work station use	
Secure work station location	
Security awareness training	

REQUIREMENTS FOR IMPLEMENTATION	
TECHNICAL SECURITY SERVICES TO GUARD DATA INTEGRITY, CONFIDENTIALITY, AND AVAILABILITY	
Access control (The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access. The use of Encryption is optional)	• Context-based access. Encryption. • Procedure for emergency access. Role-based access. • User-based access.
Audit controls	
Authorization control (At least one of the listed implementation features must be implemented)	Role-based access. User-based access.
Data Authentication	
Entity authentication (The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented)	• Automatic logoff. Biometric. • Password. PIN. • Unique user identification. • Telephone callback. Token.
TECHNICAL SECURITY MECHANISMS TO GUARD AGAINST UNAUTHORIZED ACCESS TO DATA THAT IS TRANSMITTED OVER A COMMUNICATIONS NETWORK	
1. Communications/network controls (The following implementation features must be implemented: 2. Integrity controls, Message authentication. 3. If communications or networking is employed, one of the following implementation features must be implemented. In addition, if using a network, the following four implementation features must be implemented:	• Access controls. Alarm. • Audit trail. Encryption. • Entity authentication. Event reporting. • Integrity controls. Message authentication. • Access controls, Encryption. Alarm. • Audit trail. • Entity authentication Event reporting.

[This page intentionally left blank.]

Appendix 7

HIPAA Ten Years Later: A New Initiative for Expanding Enforcement

United States Attorneys Bulletin, July, 2007

Paul J. McNulty Deputy Attorney General
Department of Justice William W. Mercer
Acting Associate Attorney General

I. Executive summary

As we commemorate ten remarkably successful years of the Department of Justice's (Department) implementation of the Health Care Fraud and Abuse Control program included in the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, the Department is launching a renewed commitment to its critical health care anti-fraud effort. Over the course of the past fifteen months, the leadership of the Department has been focused on aggressively pursuing new sources of funding for our health care fraud and pharmaceutical fraud enforcement efforts. This memorandum will outline the results of those efforts and chart the course for the reinvigoration and expansion of our work in this important area of law enforcement.

We will provide funding for thirteen civil litigators for U.S. Attorneys' offices, seven civil litigators for the Civil Division, and up to three civil litigators for the Office of Consumer Litigation. The addition of these new civil litigators will help our districts and divisions address and resolve pending False Claims Act (FCA) and other civil health care and pharmaceutical fraud cases. We are also setting aside separate additional funding for civil health care fraud litigation support expenses for all U.S. Attorneys' offices and the Civil Division.

On the criminal front, we will provide additional funding for criminal health care fraud litigation support expenses for all U.S. Attorneys' offices. We will also provide funding for the Criminal Division and U.S. Attorneys' offices involved in the three Strike Force districts: South Florida, Los Angeles, and Houston. The Strike Forces will target areas of the country experiencing high levels of health care fraud, including durable medical equipment suppliers engaged in fraud and home health care providers engaged in fraud. The Office of Consumer Litigation will also receive two additional criminal prosecutors to work on pending Food and Drug Administration cases and other pharmaceutical fraud matters.

We will provide funding for the Civil Rights Division to continue its monitoring and enforcement work involving publicly run nursing homes and hospitals. We will also continue our support for the Elder Justice and Nursing Home Initiative by funding nurse consultants to support our failure-of-care cases and funding ongoing research projects that are making important contributions to the field of elder abuse. Finally, the Federal Bureau of Investigation (FBI) will receive new funding and resources for their health care fraud investigations.

By giving the districts and our components an immediate infusion of new funding and resources, we will build on our past accomplishments and continue to grow our efforts to protect the financial integrity of our publicly funded health care programs and continue to ensure the safety of the medical products and services we receive.

II. Ten years of accomplishments

The HIPAA established the Health Care Fraud and Abuse Control Program (HCFAC), a comprehensive program to combat fraud and abuse in health care. The Program was designed to be jointly administered by the Attorney General and the Secretary of the Department of Health and Human Services (HHS) to ensure the agencies coordinate their efforts in fighting fraud. HIPAA annually appropriates monies from the Medicare Trust Fund to an expenditure account, called the HCFAC account, for use in HHS and Department anti-fraud efforts. Before the funds are disbursed, the Attorney General and the HHS Secretary must jointly certify that the funds are being distributed and used in a manner consistent with the intent and purposes of HIPAA. What was revolutionary about HIPAA from an enforcement perspective was that it established mandatory funding streams for the Department and the FBI to support dedicated prosecutors, litigators, and investigators pursuing health care fraud cases. HIPAA provided the appropriated funds which would grow each year until 2003. This meant that, until 2003, the Department could count on increasing resources to pursue health care fraud and pharmaceutical fraud cases and keeping expanding its enforcement efforts.

The growth the Department experienced in health care fraud work since 1997 is remarkable. Over the last ten years since the HCFAC program was created, the Department has significantly increased the number of civil and criminal matters it is pursuing. In FY 2006, the Department convicted 547 defendants of health care fraud offenses, the highest number to date. This represents about a 50% increase in convictions since the start of the HCFAC program in 1997.

On the civil side, last year the Department filed or intervened in 217 new civil health care fraud cases, which represents an increase of about 155% since the program started in 1997. Last year was also a record year for civil recoveries. The U.S. Attorneys' offices and the Civil Division obtained judgments and settlements totaling over $3.2 billion in fraud recoveries. Of that amount, $2.2 billion came from health care fraud cases. In the past seven years, attorneys from the Civil Division and the U.S. Attorneys' offices recovered over $5 billion in pharmaceutical matters, including over $1.2 billion in fiscal year 2006 alone. This included

$704 million obtained from the Swiss biotechnical corporation, Serono, S.A., in a series of cases involving off-label marketing and kickbacks. The Department also obtained $435 million to resolve similar off-label claims with Schering-Plough. Health Care continues to be the chief area of the Department's qui tam litigation under the FCA, accounting for more than 53% of the 5,643 qui tam cases filed since 1986 overall. In the past three years, healthcare recoveries have averaged 74% of the total FCA recoveries the Department sees each year.

III. The importance of our health care fraud work

Health care fraud remains one of the Department's broadest and most comprehensive areas of law enforcement, involving each of its ninety-four U.S. Attorneys' offices, the Criminal Division Fraud Section, the Civil Division, the Civil Rights Division, and the FBI. Our efforts are essential to preserving the financial integrity of our nation's health care system and deterring fraud schemes that put the health of our citizens in jeopardy. This work requires close cooperation with our partners at the Department of Health and Human Services Office of Inspector General (OIG) and the Centers for Medicare and Medicaid Services.

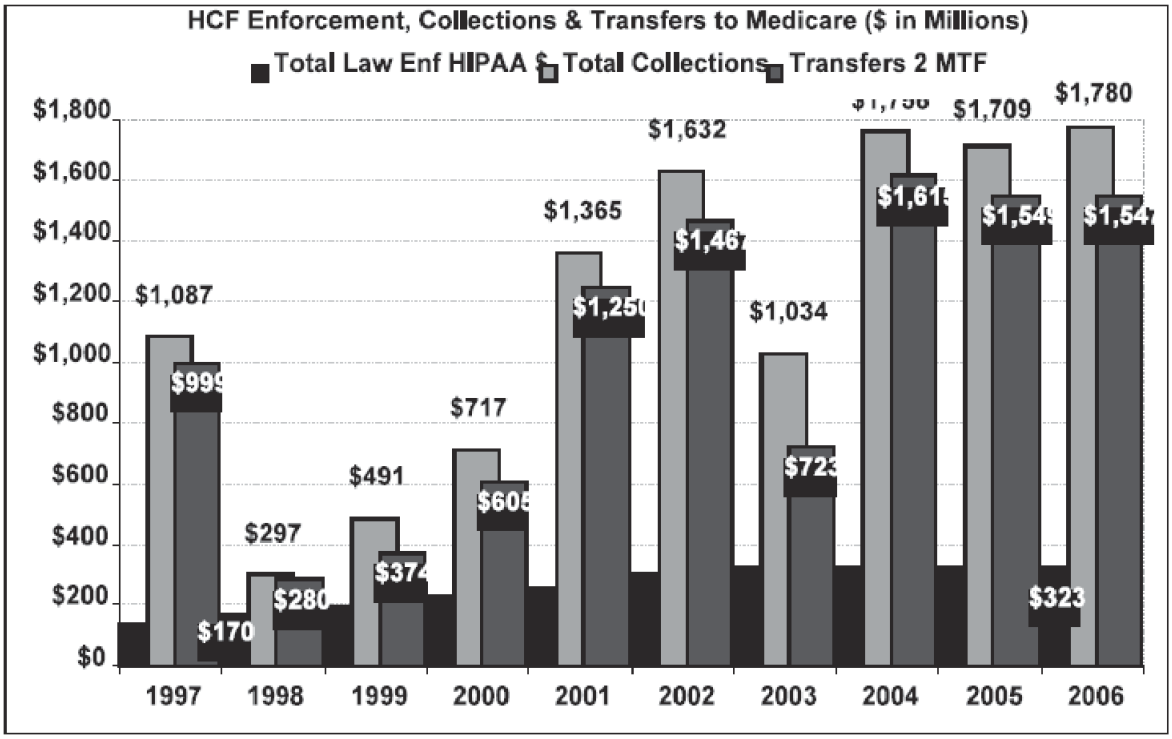
The kinds of cases the Department has pursued over the last year alone reflect the breadth of law enforcement work the Department routinely undertakes. We are prosecuting individuals operating sham durable medical equipment companies that are literally stealing money from the Medicare program—money that could otherwise be spent on providing health care for our elders. We are keeping pharmaceutical companies accountable by ensuring that they follow the law in the way they market and distribute their drugs and refrain from paying kickbacks to doctors in exchange for writing prescriptions. We are keeping hospitals accountable by ensuring that they do not fraudulently submit inflated bills to the Medicare program through upcoding or by requesting outlier payments (special payments intended to defray the expense of the most costly cases) for all their patients. We are investigating nursing homes where residents are dying from malnutrition and infected bedsores, and we are prosecuting the nursing home owners who fail to provide adequate care for the residents.

In every case, our paramount concern is patient harm. Many of the fraud schemes we see are being perpetrated by people who have no regard for the health of the beneficiaries and are willing to put lives at risk in order to line their pockets. We saw this with the doctor who was diluting chemotherapy drugs being administered to cancer patients. We saw this with the infusion therapy scams where HIV-positive patients were being given diluted medication or no medication at all. These unscrupulous people mar what is otherwise an honorable and needed service—caring for the elderly and sick.

Finally, health care fraud is still perceived as a low risk/high reward crime. Playing the odds, the worst that most people defrauding the system believe can happen to them is they get their provider number taken away or they have to pay back the money they stole as an "overpayment." The bottom line is criminals will continue to test the system and try to find vulnerabilities to exploit unless there is a real threat of criminal prosecution.

[This page intentionally left blank.]

Appendix 8



[This page intentionally left blank.]

Appendix 9

Examples of HIPAA Enforcement 2010-12

These case examples of HIPAA Enforcement were retrieved from the Department f Health and Human Services website on October 5, 2009 at http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html.

They represent the kind of problems for private practitioners and mental health centers that can result in a warning or sanction from the Office of Civil Rights.

Entity Rescinds Improper Billing for Medical Record Copies

Covered Entity: Private Practice Issue: Access

A patient alleged that a Covered Entity failed to provide him access to his medical records. After OCR notified the entity of the allegation, the entity released the complainant's medical records but also billed him $100.00 for a "records review fee" as well as an administrative fee. The Privacy Rule permits the imposition of a reasonable cost-based fee that includes only the cost of copying and postage and preparing an explanation or summary if agreed to by the individual. To resolve this matter, the Covered Entity refunded the $100.00 "records review fee."

Private Practice Implements Safeguards

Covered Entity: Private Practice
Issue: Safeguards; Impermissible Uses and Disclosures

A staff member of a medical practice discussed HIV testing procedures with a patient in the waiting room, thereby disclosing PHI to several other individuals. Also, computer screens displaying patient information were easily visible to patients. Among other corrective actions to resolve the specific issues in the case, OCR required the provider to develop and implement policies and procedures regarding appropriate administrative and physical safeguards related to the communication of PHI. The practice trained all staff on the newly developed policies and procedures. In addition, OCR required the practice to reposition its computer monitors to prevent patients from viewing information on the screens, and the practice installed computer monitor privacy screens to prevent impermissible disclosures.

Private Practice Revises Process to Provide Access to Records

Covered Entity: Private Practices
Issue: Access

A private practice failed to honor an individual's request for a complete copy of her minor son's medical record. OCR's investigation determined that the private practice had relied on state regulations that permit a Covered Entity to provide a summary of the record. OCR provided technical assistance to the Covered Entity, explaining that the Privacy Rule permits a Covered Entity to provide a summary of patient records rather than the full record only if the requesting individual agrees in advance to such a summary or explanation. Among other corrective actions to resolve the specific issues in the case, OCR required the Covered Entity to revise its policy. In addition, the Covered Entity forwarded the complainant a complete copy of the medical record.

Private Practice Revises Process to Provide Access to Records

Covered Entity: Private Practices
Issue: Access

At the direction of an insurance company that had requested an independent medical exam of an individual, a private medical practice denied the individual a copy of the medical records. OCR determined that the private practice denied the individual access to records to which she was entitled by the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, OCR required that the private practice revise its policies and procedures regarding access requests to reflect the individual's right of access regardless of payment source.

Privacy Practice Revises Access Policy

Covered Entity: Private Practice
Issue: Access

A private practice denied an individual access to his records on the basis that a portion of the individual's record was created by a physician not associated with the practice. While the amendment provisions of the Privacy Rule permit a Covered Entity to deny an individual's request for an amendment when the Covered Entity did not create that the portion of the record subject to the request for amendment, no similar provision limits individuals' rights to access their protected health information. Among other steps to resolve the specific issue in this case, OCR required the private practice to revise its access policy and procedures to affirm that, consistent with the Privacy Rule standards, patients have access to their record regardless of whether another entity created information contained within it.

Mental Health Center Corrects Process for Providing Notice of Privacy Practices

Covered Entity: Outpatient Facility
Issue: Notice

A mental health center did not provide a notice of privacy practices (notice) to a father or his minor daughter, a patient at the center. In response to OCR's investigation, the mental health center acknowledged that it had not provided the complainant and his daughter with a notice prior to her mental health evaluation. To resolve this matter, the mental health center revised its intake assessment policy and procedures to specify that the notice will be provided and the clinician will attempt to obtain a signed acknowledgement of receipt of the notice prior to the intake assessment. The acknowledgement form is now included in the intake package of forms. The center also provided OCR with written assurance that all policy changes were brought to the attention of the staff involved in the daughter's care and then disseminated to all staff affected by the policy change.

Private Practice Revises Access Procedure

Covered Entity: Private Practice
Issue: Access

A complainant alleged that a private practice physician denied her access to her medical records, because the complainant had an outstanding balance for services the physician had provided. During OCR's investigation, the physician confirmed that the complainant was not given access to her medical record because of the outstanding balance. OCR provided technical assistance to the physician, explaining that, in general, the Privacy Rule requires that a Covered Entity provide an individual access to their medical record within 30 days of a request, regardless of whether or not the individual has a balance due. Once the physician learned that he could not withhold access until payment was made, the physician provided the complainant a copy of her medical record.

Private Practice Ceases Conditioning of Compliance with the Privacy Rule

Covered Entity: Private Practice
Issue: Conditioning Compliance with the Privacy Rule

A physician practice requested that patients sign an agreement entitled "Consent and Mutual Agreement to Maintain Privacy." The agreement prohibited the patient from directly or indirectly publishing or airing commentary about the physician, his expertise, and/ or treatment in exchange for the physician's compliance with the Privacy Rule. A patient's rights under the Privacy Rule are not contingent on the patient's agreement with a Covered Entity. A Covered Entity's obligation to comply with all requirements of the Privacy Rule cannot be conditioned on the patient's silence. OCR required the Covered Entity to cease using the patient agreement that conditioned the entity's compliance with the Privacy Rule. Additionally, OCR required the Covered Entity to revise its Notice of Privacy Practices.

[This page intentionally left blank.]

Appendix 10
Jurisdiction/State Privacy Laws (2012)

[These laws were collected by the Georgetown University Privacy Project and are summarized here. For more information, go to (http://ihcrp.georgetown.edu/privacy/pdfs/statereport1.pdf and http://ihcrp.georgetown.edu/privacy/pdfs/statereport2.pdf)~LWG]

District of Columbia [D.C. Code Ann. § 3-1205.14(a)(16)]

1. **Patient Access**—The District of Columbia does not have a general statute that grants patients access to their health information or medical records. The jurisdiction does statutorily grant access to mental health records.

2. **Patient Bill of Rights**— The D.C. Bill of Rights provides that individual privacy regarding health records must be protected by laws prohibiting disclosure that may result in a violation of individual privacy. [D.C. Code Ann., Art. I, Bill of Rights §4.]

3. **Sanctions**—A health professional who willfully breaches a statutory, regulatory, or ethical requirement of confidentiality with respect to a person who is a patient or client of the health professional, unless ordered by a court, may be subject to disciplinary action by the pertinent licensing board. [D.C. Code Ann. § 3-1205.14(a)(16).]

4. **Mental Health Records**—The District of Columbia recognizes a physician and mental health care professional-patient privilege which allows a patient, in a legal proceeding, to refuse to disclose and to prevent others from disclosing confidential information that the professional acquired in his professional capacity that was necessary to enable him to act in that capacity. [D.C. Code Ann. §§7-1201.01 (defining mental health professional as including psychiatrists, psychologists, social workers, and others); 14-307.]

5. **Right to Sue**—HMOs and their employees who wrongfully disclose confidential health care information while acting in good faith and without negligence may not be liable for civil damages. [D.C. Code Ann. §31-3426(c).]

6. **Penalties for Privacy Violations**—(HMO) If the commissioner of insurance after following appropriate procedures, determines that an HMO has substantially failed to comply with these provisions, he may suspend or revoke the HMO's certificate of authority or impose an administrative penalty ranging up to $1,000 a day for each cause of suspension or revocation. (Individual) Any District of Columbia resident injured by a violation may institute a civil action to recover actual damages, the costs of the action, and reasonable attorney's fees. Actual damages shall not include dignitary damages, including pain and suffering. [D.C. Code Ann. § 31-3419.]

7. **Copying Fees**—no regulation

8. **Privilege**—The District of Columbia recognizes a physician and mental health care professional-patient privilege which allows a patient, in a legal proceeding, to refuse to disclose and to prevent others from disclosing confidential information that the professional acquired in his professional capacity that was necessary to enable him to act in that capacity. [D.C. Code Ann. §§7-1201.01 (defining mental health professional as including psychiatrists, psychologists, social workers, and others); 14-307.]

9. **Privacy and HMOs**—Exceptions to the general rule allow disclosures without the person's consent to carry out the purposes of the statutory provisions governing HMOs; when needed for the conduct of the HMO's business (including to state licensing and certifying agencies); pursuant to statute or court order for the production of evidence or the discovery thereof; and, to the extent pertinent, in the event of a claim or litigation between an enrollee/applicant and the HMO. [A] $10,000 - $50,000 administrative penalty may be imposed if the HMO fails to correct the violation within a reasonable time of receiving written notice.

10. **Breach Notification**—none beyond HIPAA rules PHI- A person's first name or first initial and last name, or phone number, or address, in combination with one of the following: (1) Social Security number; (2) driver's license number or District of Columbia Identification Card number (3) credit card number or debit card number; or any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.

Maryland

1. **Patient Access**—Maryland statutorily grants patients the right of access to their medical records maintained by health care providers, health care institutions, insurance entities, health maintenance organizations and other specified entities. [Md. Code Ann., Health-Gen. § 4-301, et. seq.] The records of mental health patients are subject to additional protections beyond the general requirements for medical records contained in the Confidentiality of Medical Records Act. The attending provider may refuse to disclose to the patient any portion of the medical record if the provider, with "input from a primary provider of mental health services," believes that disclosure would be injurious to the health of a patient. [Md. Code Ann., Health-Gen. §§ 4-303(a); 4-304.]

2. **Patient Bill of Rights**—see #1 and #4

3. **Sanctions**—A physician may be disciplined, including revocation or suspension of license, for failing to provide details of a patient's medical record to the patient in accordance with the CMRA [Md. Code Ann., Health Occ. § 14-404.] Similarly, a podiatrist may be disciplined for failing to provide the details of the medical records of a patient to a licensed health care practitioner or institution or an authorized insurance carrier on proper request. [Md. Code Ann., Health Occ. § 16-312.]

4. **Mental Health Records**—The CMRA applies to medical records maintained by health care providers, a term which is defined as including physicians, physician assistants, osteopaths, audiologists, speech pathologists, licensed nutritionists, dietitians, pharmacies, physical therapists, occupational therapists, acupuncturists, optometrists, chiropractors, registered or licensed nurses, dentists, podiatrists, psychologists, electrologists, licensed or certified social workers and professional therapists, counselors and their agents, employees, officers and directors. [Md. Code Ann., Health-Gen. §§ 4-304; 4-301(h) (defining "health care provider" as those licensed or authorized to provide services under Md. Code Health Occupations Article) and Md. Code Ann., Health Occ. § 1-101, et. seq.] The definition of "health care provider" also includes health care facilities, hospitals (including related institutions), medical laboratories, outpatient clinics and HMOs. [Md. Code Ann., Health-Gen. § 4-301(h).] Mental health records may also be disclosed without the authorization of the patient in certain other circumstances including: to the director of a juvenile or adult correctional facility if the recipient has been involuntarily committed and disclosure is necessary for the proper care and treatment of the recipient; as provided in Md. Code Ann., Cts & Jud. Pro. § 5-609 by a health care facility to a law enforcement agency under certain circumstances; by a health care facility to a parent, guardian, next of kin or other specified individuals to confirm or deny the recipient's presence in the facility; and to allow for service of process or court order on a facility. Mental health records may be disclosed to family members or close friends of the patient without consent unless the patient requests confidentiality. [Md. Code Ann., Health-Gen. § 4-305(b)(7).]

5. **Right to Sue**—Patients have the right to sue and to recover actual damages from health care providers who knowingly violate the Confidentiality of Medical Records Act. [Md. Code Ann., Health-Gen. § 4-309(f).] A provider who knowingly refuses to provide a patient access to his own medical records within a reasonable time (no more than 21 days after the request) may be liable for actual damages. [Md. Code Ann., Health-Gen. § 4-309(a).]

6. **Breach Notification**—Notification is not required if after a good-faith, reasonable and prompt investigation the entity determines that the personal information of the individual was not and will not be misused as a result of the breach. If after the investigation is concluded, the entity determines that notification is not required, the entity shall maintain records that reflect its determination for three years after the determination is made.

7. **Penalties for Privacy Violations**—A provider who knowingly and willfully violates the Confidentiality of Medical Records Act is guilty of misdemeanor and, on conviction, subject to a fine not exceeding $1,000 for the first offense, and $5,000 for subsequent convictions. [Md. Code Ann., Health-Gen. § 4-309(d).]

8. **Copying Fees**—A provider may require the patient to pay a copying fee of 50¢ per page prior to furnishing the requested material. [Md. Code Ann., Health Gen. § 4-304(c) and (d).] In addition, providers may impose a fee not to exceed $15 in clerical costs for medical record retrieval and preparation, as well as the actual cost for postage and handling of the medical record. [Md. Code Ann., Health Gen. § 4-304(c).] These fees are applicable to a medical bill if requested by the patient. [Md. Code Ann., Health Gen. § 4-304 (amended by 2001 Md. Laws Ch. 265).]

9. **Privilege**—no specific regulation

10. **Private Action**—Consumers may bring actions under Title 13 of the Maryland Code, the Unfair and Deceptive Trade Practices Act.

11. **PHI**—include tax ID number as PHI along with 19 other areas not to be disclosed without permission or for TPO purposes.

12. **Attorney General Notification**—The Attorney General must be notified prior to notification of individuals.

Virginia

1. **Patient Access**—Virginia statutorily requires health care providers to furnish patients a copy of their medical records. [Va. Code Ann. § 32.1-127.1:03.] This requirement applies to any "provider," a term that includes physicians, hospitals, dentists, pharmacists, registered or licensed practical nurses, optometrists, podiatrists, chiropractors, physical therapists, physical therapy assistants, clinical psychologists, clinical social workers, professional counselors, licensed dental hygienists and health maintenance organizations. [Va. Code Ann. §§ 32.1-127.1:03(B) (defining "provider"); 8.01-58.1 (defining "health care provider").] It encompasses medical records, which include any written, printed or electronically recorded material maintained by a provider in the course of providing health services to a patient concerning the patient and the services provided. The term "record" also includes the substance of any communication made by a patient to a provider in confidence during or in connection with the provision of health services to a patient. [Va. Code Ann. §§ 32.1-127.1:03(B) (defining "record").]

2. **Patient Bill of Rights**—see #1

3. **Sanctions**—no specific monetary or ethical sanctions

4. **Mental Health Records**—A person who is admitted to a hospital or other facility operated, funded, or licensed by the Department of Mental Health, Mental Retardation and Substance Abuse Services has the right of access to his medical and mental records, consistent with his condition and sound therapeutic treatment. [Va. Code Ann. § 37.1-84.1(A)(8); see also "Patient Access – State Government," above.] A patient who is the subject of information received by a third party payor may request and is entitled to receive from the payor a statement as to the substance of the information, unless the professional or treatment facility, or both, advise the payor that providing such information to the patient will adversely affect the patient's health. Under such circumstances, the third party payor must provide the information to the attorney designated by the patient. [Va. Code Ann. § 37.1-230.]

5. **Right to Sue**—A person whose rights under this statute are violated has the right to file a civil action seeking equitable relief within two years from the date the alleged violation is or should have been discovered. [Va. Code Ann. § 38.2-617.] The court may award costs and reasonable attorney's fees to the prevailing party. [Id.]

6. **Penalties for Privacy Violations**—no specific penalties

7. **Copying Fees**—An insurance company, HMO or other insurance entity must permit the individual to inspect and copy his personal information in person or obtain a copy of it by mail, whichever the individual prefers, within 30 business days of receiving a written request and proper identification from an individual. [Va. Code Ann. § 38.2-608(A).] If the personal information is in coded form, an accurate translation in plain language must be provided in writing. [Va. Code Ann. § 38.2-608(A)(2).] The insurance entity can impose a reasonable fee to cover copying costs. [Va. Code Ann. § 38.2-608(D).]

8. **Privilege**—Virginia recognizes a number of health care provider-patient privileges, which allow a person, in a legal proceeding, to refuse to disclose and to prevent any other person from disclosing confidential communications with the health care provider made for the purpose of diagnosis or treatment of a physical or mental condition. [Va. Code Ann. §§ 8.01-399 (physician and other "licensed practitioner of the healing arts"- patient); 8.01-400.2 (licensed professional counselor, clinical social worker or psychologist-client).] Medical records maintained by health care providers are the property of the provider, or the employer if the health care provider is employed by another health care provider. [Va. Code Ann. § 54.1-2403.3.] Patient records may not be transferred with the sale of a professional practice until an attempt is first made to notify patients of the pending transfer, by mail, at the patient's last known address, and by publishing prior notice in a newspaper of general circulation within the provider's practice area. The notice must inform patients that at their written request, within a reasonable time, records or copies can be sent to another like-regulated provider of the patient's choice or destroyed. [Va. Code Ann. § 54.1-2405.]

9. **Private Action**—Though generally enforced by the Attorney General, nothing in the data breach notification statute will preclude recovery of economic damages.

10. **Breach Notification**—Medical Information Breach Notification Statute: For an authority, board, bureau, commission, district or agency of the state or of any political subdivision of the state, or agencies in the state supported wholly or principally by public funds, the state's Medical Information Breach Notification statute may apply. The statute applies to Medical information. "Medical information" means the first name or first initial and last name with any of the following elements: (1) any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (2) an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records. Notification required if the entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth.

11. **PHI**—see #10

12. **Attorney General Notification**—Personal Information Breach Notification Statute: The Office of the Attorney General must be notified following discovery of a breach of personal information. Medical Information Breach Notification Statute: The Office of the Attorney General and the Commissioner of Health must be notified following discovery of a breach of medical information. The entity must notify both the subject of the medical information and any affected resident of the Commonwealth, if those are not the same person.

Appendix 11
Consumer Health Information Bill of Rights

news
233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601
phone »(312) 233-1100
fax »(312) 233-1090
web »www.ahima.org

FOR IMMEDIATE RELEASE

For more information, please contact:
Bridget Stratton
Public Relations
312-233-1097
bridget.stratton@ahima.org

New guidelines, consumer tips from California help professionals, patients guard against medical identity theft

AHIMA part of coalition to develop new resources

Chicago – Nov. 20, 2013 – New guidelines on preventing and remedying medical identity theft released by the Office of the Attorney General in California offer best practice recommendations for the healthcare industry and tips for consumers. The American Health Information Management Association (AHIMA) contributed to the development of the guidelines, "Medical Identity Theft: Recommendation for the Age of Electronic Medical Records."

Key recommendations for healthcare providers include:

- Implementing an identity theft response program with clear written policies and procedures for investigating a flagged record
- Offering patients who believe they may be victims of medical identity theft a free copy of the relevant portions of their medical records to review for signs of fraud

"Medical identity theft has been called the privacy crime that can kill," said California Attorney General Kamala D. Harris. "As the Affordable Care Act encourages the move to electronic medical records, the healthcare industry has an opportunity to improve public health and combat medical identity theft with forward-looking policies and the strategic use of technology."

The report for the industry focuses on the effect of identity theft on the accuracy of medical records.

"Health information management (HIM) professionals play a key role in safeguarding health information, and helping address issues when questions of identity theft occur," said AHIMA CEO Lynne Thomas Gordon, RHIA, MBA, CAE, FACHE, FAHIMA. "AHIMA is proud to have contributed to this important guide to engage the entire industry and to help consumers learn what they should watch for and how to deal with concerns about the protection and accuracy of their health information."

A piece for consumers, "First Aid for Medical Identity Theft," describes the signs of medical identity theft and provides tips on how to respond. These signs can include notice of a data breach from a healthcare provider, an unknown item on an Explanation of Benefits statement from an insurer, a call from a debt collector about an unfamiliar medical bill and questions on identity or health conditions at a doctor's office or hospital.

"AHIMA is dedicated to offering consumers guidance about how to keep track of their health information," said Thomas Gordon. "At our website, MyPHR.com, we offer links to these

innovative, important tips and tools from California, as well as other resources for consumers and other stakeholders. We're also focused on making sure our members and the HIM community knows best practices are available."

###

About AHIMA
Celebrating its 85th anniversary this year, the American Health Information Management Association (AHIMA) represents more than 71,000 educated health information management professionals in the United States and around the world. AHIMA is committed to promoting and advocating for high quality research, best practices and effective standards in health information and to actively contributing to the development and advancement of health information professionals worldwide. AHIMA's enduring goal is quality healthcare through quality information. **www.ahima.org**

http://www.ahima.org/~/media/AHIMA/Files/PR/n131112%20california%20med%20id.ashx