

Maryland Health Care Commission

H

I

P

A

A

A Guide to Privacy Readiness Version 1

Released August 2001

Donald E. Wilson, M.D.
Chairman

Ben Steffen
Deputy Director
Data Systems & Analysis

©2001 by Maryland Health Care Commission. This booklet is not to be reproduced in any form without written permission from MHCC.

HOW TO USE THIS GUIDE

The Maryland Health Care Commission developed, *"A Guide to Privacy Readiness"* with the assistance of representatives from the health care industry. The purpose of this document is to promote best practices for privacy among health care providers and organizations in Maryland. Users are encouraged to implement privacy standards in a manner that is reasonable and consistent to the extent of its organizational structure. The Maryland Health Care Commission appreciates contributions made by the EDI/HIPAA Workgroup in the development of *"A Guide to Privacy Readiness."*

Overall Format

"A Guide to Privacy Readiness" is made up of eight sections:

1. **Introduction** (overview of the HIPAA Privacy Regulations)
2. **Maryland Law on the Confidentiality of Medical Records** (highlights the Maryland Privacy Law)
3. **Definitions** (clarifies terms used in the privacy regulations)
4. **Assessment Guide and Work Plan** (see next column)
5. **Business Associate Contract** (illustrative document)
6. **Chain of Trust Partner Agreement** (illustrative document)
7. **Notice of Privacy Practices** (illustrative document)
8. **Computer and Information Usage Agreement** (illustrative document)

©2001 by Maryland Health Care Commission. This booklet is not to be reproduced in any form without written permission from MHCC.



Assessment Guide and Work Plan

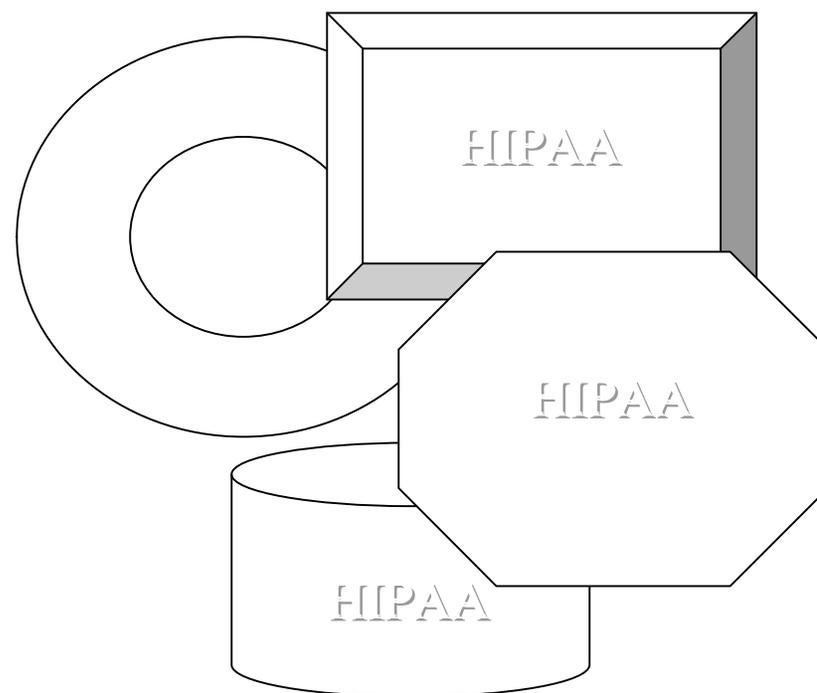
This document is arranged by the following column headings:

- **HIPAA Privacy Standard** (arranged in three categories with corresponding regulatory citation):
 1. Operational standards define appropriate uses and disclosures of medical information (pages 1-5)
 2. Consumer Control standards outline patient privacy right over the use and disclosure of their medical information (pages 6-9)
 3. Administration standards define how the privacy regulations need to be documented, staff training needs and administering complaints (pages 10-20)
 - **Requirements**
 1. Quoted regulatory language
 2. User question to assess readiness
 3. Additional clarification of regulatory language
 - **HIPAA Readiness** (Checklist correlates to question 2 under *Requirements*) Designed to track areas where policies/procedures need development.
 - **Industry Developed Strategies** (suggestions for implementation)
-
- **Self Assessment** (rate your readiness to comply with privacy regulations on page 20)

HIPAA: A GUIDE TO PRIVACY READINESS

Index

- I. Introduction**
- II. Maryland Law on the Confidentiality of Medical Records**
- III. Definitions**
- IV. Assessment Guide and Work Plan**
- V. Business Associate Contract**
(example)
- VI. Chain of Trust Partner Agreement**
(example)
- VII. Notice of Privacy Practices**
(example)
- VIII. Computer and Information Usage Agreement**
(example)



I. INTRODUCTION

Background

On August 21, 1996, then President Bill Clinton signed into law the Health Insurance Portability and Accountability Act of 1996. One part of this law, labeled Administrative Simplification, is intended to reduce the costs and administrative burdens of health care by making possible the standardized, electronic transmission of certain administrative and financial transactions. On December 28, 2000 the U.S. Department of Health and Human Services released the final rule

for Privacy. These regulations cover all medical records and other individually identifiable health information held or disclosed by a covered entity, in any form, whether communicated electronically, on paper, or orally. Covered entities include health plans, health care clearinghouses, and health care providers who transmits any health information in electronic form. Most covered entities have two years to implement the regulations.

HIPAA Privacy Regulations Overview

The HIPAA Privacy Regulations provide patients with significant rights to better understand and control how their health information is used and disclosed. Summarized below are the standards provided by the final rule.

- Providers are required to provide patients with a clearly written explanation of how their medical information will be used, kept and disclosed.
- Providers are required to obtain patient consent before sharing their medical information for treatments, payment, and other health care operations.
- Disclosure of patient information must be limited to the minimum necessary to comply with the request.
- Patients have the right to complain to a covered entity, or to the Secretary of Health and Human Services regarding a violation of the regulations.
- Patients must be able to access, duplicate and amend their medical records. Providers must also make a history of disclosures available upon patient request.
- Detailed authorizations are requested for non-routine disclosures of patient information with exceptions only for treatment, payment, and health care operations.
- Health care providers cannot condition treatment on a patient's consent to disclose health information for non-routine uses.
- Covered entities must provide a means for patients to inquire or make complaints regarding the privacy of their medical records.
- Providers must establish written policies documenting compliance with the privacy standards.
- Policies and procedures must include a process for disclosing protected health information that include steps to assure that business associates maintain the privacy of protected health information.
- A Privacy Official must be designated with the responsibility of ensuring that employees receive sufficient awareness training and instruction on the new privacy protection procedures.
- Violators of these standards are subject to civil liability that includes \$100 per incident, up to \$25,000 per person, per year, per standard.
- Criminal penalties for violations range from \$50,000 and one year in prison to \$250,000 and up to 10 years in prison depending upon the severity of the disclosure.

Application

The Maryland Health Care Commission's Privacy Readiness Assessment Guide and Work Plan is intended to assist most practitioners and small facilities in their privacy assessment, and to provide some industry-developed suggestions for meeting the compliance standards. At the completion of the self-assessment, users will have a functional work plan to assist them in implementing the Privacy Standards. HIPAA is intended to be scalable, users of this guide are encouraged to implement the HIPAA requirements in a manner consistent with their organization's size.

II. Maryland Law on the Confidentiality of Medical Records

Did you know that Maryland already has a privacy law...

- All medical records are considered protected information. This includes both electronic and paper records and also oral communications.
- Patient rights over their medical information include patient-provider medical records confidentiality, permitting patient access to their medical files, and allowing patients to add or alter their medical records according to those procedures established by the provider.
- Health care providers may only disclose medical records upon receipt of patient notification. Health care providers are prohibited from disclosing any patient identifiable information to a person for educational or research purposes, evaluation and management, or accreditation of a facility.
- Any health care provider or other person(s) who knowingly and willfully violate the provisions of Maryland's Medical Records Law are guilty of a misdemeanor. If convicted, the violator is subject to a fine not exceeding \$1,000 for the first offense and \$5,000 for each subsequent conviction.
- Copies of medical records are permitted upon patient request.
- A health care provider may disclose medical records about a patient without authorization when seeking payment for health care services, in emergency situations, to the provider's legal counsel, coordinating benefit payments, or to a unit of State or local government for purposes of investigation. Health care providers must disclose medical records in situations pertaining to criminal investigation, or to an appropriate organ, tissue, or eye recovery agency.
- A facility director may confirm or deny the presence of an individual to a parent, guardian, next of kin, or any individual who has significant interest in the individual's status. State or local government agencies may report the status of an individual in cases of missing persons where a report has been filed.
- Information may be released without consent in circumstances of investigations or treatment in cases of suspected abuse or neglect of a child or adult and, the licensure or certification, or discipline of a health professional.
- Personal notes for mental health therapy that are kept separate from the medical record are not considered part of the medical record. Mental health information subject to disclosure includes information concerning diagnosis, treatment plans, symptoms, prognosis, or progress updates.
- A health care provider or any other person who knowingly and willfully requests or obtains a medical record under false pretenses or through deception, or knowingly and willfully discloses a medical record is subject to a fine not exceeding \$50,000, imprisonment for not more than one year or both. If the offense is committed under false pretenses, a fine not exceeding \$100,000, imprisonment for five years or both. If the offense is committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious intent, penalties include up to a \$250,000 fine, imprisonment for not more than 10 years or both.

III. Definitions

Term	Description
Authorization	<p>An authorization is a written document signed by a patient giving permission to a provider to disclose protected health information for purposes other than treatment, payment and health care operations. An authorization must contain specific description of the information to be disclosed, the name or other specific identification of the person(s) making the request, expiration date, 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.</p> <p>Examples of disclosures for which authorizations are required include: Disclosures to an employer for an employment physical, pre-enrollment and underwriting for insurance, the sharing of protected health information by an insurer with an employer, disclosure of psychotherapy notes for most purposes - including treatment, payment and healthcare operations – requires a specific authorization that is distinct from any authorization for use and disclosure of other protected health information. Psychotherapy notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment, results of clinical tests and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.</p>
Business Associate	<p>A person or entity who performs a function for or assists a <i>covered entity</i> or <i>health care arrangement</i> with a function or activity involving the use or disclosure of <i>individually identifiable health information</i> (IIHI). Examples of functions include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. The provision of the service involves the disclosure of IIHI from the covered entity or arrangement, or from another business associate of the covered entity or arrangement, to the person or entity. A covered entity may be a business associate of another covered entity.</p>
Consent	<p>Consent is a written document that a provider must obtain prior to using or disclosing protected health information for treatment, payment or health care operations. A consent must be written in plain language and refer the individual to the covered entity's Notice of Privacy Practices for a more complete description of such uses and disclosures and state that the individual has the right to review the Notice of Privacy Practices prior to signing the consent. In addition, if the covered entity has reserved the right to change its Notice of Privacy Practices, that must be noted in the consent. The consent must also include language that the individual has the right to request that the provider restrict how protected health information is used or disclosed to carry out treatment, payment or health care operations; that the covered entity is not required to agree to requested restrictions and if a covered entity agrees to a requested restriction, the restriction is binding on the provider; state that the individual has the right to revoke the consent in writing, except to the extent that the provider has already acted upon the consent; and the consent must be signed by the individual and dated. A consent is defective if it lacks any of these requirements.</p>
Covered Entity	<p>A health plan. A health care clearinghouse. A health care provider who transmits any health information in electronic form in connection with a standard transaction.</p>

Term	Description
<i>Covered Functions</i>	Functions of a covered entity, the performance of which makes the entity a health plan, health care provider or health care clearinghouse.
<i>Data Aggregation</i>	The combining of protected health information by a business associate created or received in its capacity as a business associate of another covered entity, to permit the creation of data for analyses that relate to the health care operations of the respective covered entities.
<i>Direct Treatment Relationship</i>	A treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.
<i>Disclosure</i>	Release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.
<i>HHS</i>	The Department of Health and Human Services
<i>Health Care</i>	Care, services or supplies related to the health of an individual including, but not limited to, the following: preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body and sale or dispensing of a drug, device, equipment or other item in accordance with a prescription.
<i>Health Care Clearinghouse</i>	A public or private entity (including billing services, repricing companies, community health management information systems, or community health information systems and “value-added” networks and switches) that processes or facilitates processing of health information received from another entity in nonstandard format into standard data elements or standard transactions or receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.
<i>Health Care Operations</i>	Health care operations include general administrative and business functions necessary for a covered entity to remain a viable business. The final rule clarifies a number of provisions, notably adding two categories of activities: Business planning and development, such as cost management and planning related analyses related to managing and operating the entity and; business management activities and general administrative functions such as fundraising and marketing of certain services to the extent permitted without authorization. The final regulation also adds to health care operations the disclosure of protected health information for due diligence, internal grievance resolution and customer service to provide data and statistical analyses.

Term	Description
Health Care Provider	A provider of medical services including: <i>institutional providers</i> (such as hospitals, skilled nursing facilities, home health agencies, comprehensive outpatient rehabilitation facilities); <i>facilities and practitioners</i> (including clinics and centers, physicians, clinical laboratories, pharmacies, nursing homes, licensed/certified health care practitioners and suppliers of durable medical equipment); and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.
Health Information	Any information, whether oral or recorded in any form or medium that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, healthcare clearinghouse and relates to the past, present or future physical or mental health condition of an individual; the provision of health care or the past, present or future payment for the provision of health care to an individual.
Indirect Treatment Relationship	A relationship between an individual and a health care provider in which the health care provider delivers health care to the individual based on the orders of another health care provider, and the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.
Individual	A person who is the subject of protected health information.
Individually Identifiable Health Information (IIHI)	Information that is a subset of health information, including demographic information collected from an individual that is created or received from a health care provider, health plan, employer or health care clearinghouse and 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 which identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.
Marketing	<p>A communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service. Covered entities may use and disclose protected health information for the following excepted activities without authorization:</p> <ol style="list-style-type: none"> 1. Communications made by a covered entity for the purpose of describing participating providers or health plan network; 2. Communications tailored to the circumstances of a particular individual, made by a health care provider to an individual as part of the treatment of the individual, such as referrals, prescriptions, etc.; 3. Communications tailored to the circumstances of a particular individual and made by a health care provider or health plan to an individual in the course of managing the treatment or for the purpose of directing or recommending alternative therapies, providers or settings of care.

Term	Description
Organized Health Care Arrangement	Includes arrangements in which participants need to share protected health information about their patients. The arrangements involve clinical or operational integration among legally separate covered entities in which it is often necessary to share protected health information for the joint management and operations of the arrangement. Key component of these arrangements is that individuals who obtain services from them have an expectation that these arrangement are integrated and that they jointly manage their operations.
Payment	The activities undertaken by or on behalf of a health plan to obtain premiums or to determine or fulfill responsibility of coverage and for provision of benefits under the health plan or a health care provider or health plan, to obtain reimbursement for the provision of health care. Activities that constitute payment include determinations of coverage, including eligibility, coordination of benefits and a specific individual's cost sharing amount, adjudication or subrogation of health benefit claims; risk adjustment; health care data processing related to billing, claims management, and collection activities; obtaining payment under a contract for reinsurance and utilization review activities including concurrent and retrospective review of services.
Protected Health Information (PHI)	All individually identifiable health information (IIHI) transmitted or maintained by a covered entity, regardless of form. Protected health information excludes IIHI in education records.
Psychotherapy Notes	Notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or group, joint or family counseling session. Psychotherapy notes excludes medication prescription, session start and stop times, modalities and frequency of treatment, results of clinical tests and summaries of diagnosis, functional status, treatment plans, symptoms, prognosis and progress.
Research	A systematic investigation, including research development, testing and evaluation, designed to develop or contribute to general knowledge.
Treatment	Provision, coordination or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient or the referral of a patient from one health care provider to another.
Use	With respect to individually identifiable health information, the sharing, employment, application, utilization, examination or analysis of such information within an entity that maintains such information.

IV. ASSESSMENT GUIDE AND WORK PLAN

HIPAA PRIVACY STANDARD	REQUIREMENT(s)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Uses & Disclosures of PHI (PHI)</p> <p>§164.502(a)</p> <p>Operational</p>	<p><i>Privacy rules require consent for disclosure of PHI for treatment, payment and health care operations, and authorization for all other purposes for which written permission is required.</i></p> <p>? Have you made a distinction between consent and authorization documents and added the appropriate language for use and disclosure of PHI?</p> <p><u>Clarification:</u> Consents are required for providers and optional for health plans. Consent may be a condition for receiving treatment. Authorizations are required for all other disclosures and require detail.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Update existing consents, authorizations to bill, and other forms used for the release of medical records. Add language stating that written consent is required for the use and disclosure of PHI for treatment, payment and health care operations. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Uses & Disclosures for which an authorization is required</p> <p>§164.508</p> <p>Operational</p>	<p><i>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, 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.</i></p> <p>? Does your authorization document contain all the required elements for disclosure of PHI?</p> <p><u>Clarification:</u> Authorizations are required to be more specific than consents regarding disclosure of PHI.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Specify intended use of PHI in authorization forms. Indicate in the document that authorizations go beyond consent for release of information for purposes other than payment, treatment, and health care operations ▪ Where applicable, indicate in the authorization form examples of intended uses PHI and what circumstances an authorization is required, for example disclosure of psychotherapy notes. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Minimum Necessary</p> <p>§164.502(b) §164.514(d)</p> <p>Operational</p>	<p><i>A covered entity must limit use and disclosure of PHI to the minimum necessary to carry out the intended purpose of the request.</i></p> <p>? Do you and/or your staff have a complete understanding of what is considered “minimum necessary” for various disclosures of PHI?</p> <p><u>Clarification:</u> Minimum necessary does not apply to disclosures between providers in the context of treatment.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Update employee policies that disclose PHI, such as for claims payment, limited distribution only to information related to a specific treatment. ▪ Use actual examples from payers to train employees on minimum necessary requirements. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Disclosures to Business Associates</p> <p>§164.502(e)</p> <p>Operational</p>	<p><i>Disclosures of PHI may be made to business associates where a Business Associate Contract is in place.</i></p> <p>? Can you identify the situations where a Business Associate Contract must be in place?</p> <p><u>Clarification:</u> Business Associate Contracts are not necessary between providers treating an individual.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Revise existing trading partner agreements to explain privacy standard requirements when using PHI. ▪ Request trading partners sign a Business Associate Agreement, i.e., medical labs and medical transcribers. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object</p> <p>§164.510</p> <p>Operational</p>	<p><i>PHI may be disclosed by a Covered Entity without the individual's consent or authorization when used for facility directories (for clergy and other visitors), or to update family members and individuals involved in the individual's care.</i></p> <p>? 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?</p> <p><u>Clarification:</u> Individuals must be given the opportunity to prohibit or restrict certain disclosures of PHI.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Update Notice of Privacy Practices documentation to state that facilities may disclose limited PHI <i>but must allow the patient an opportunity to object under limited situations</i>. Examples of <i>certain situations</i> are: listing a patient's name in facility directory, blocking a family member from receiving information on health status, or for disaster relief purposes. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Uses and Disclosures for which consent, an authorization or opportunity to agree or object is not required</p> <p>§164.512(a) – (l) Operational</p>	<p><i>A covered entity may use or disclose protected health information without the written consent or authorization of the individual in the following circumstances:</i></p> <ul style="list-style-type: none"> <i>(a) Uses and disclosures required by law</i> <i>(b) Uses and disclosures for public health activities</i> <i>(c) Disclosures about victims of abuse, neglect or domestic violence</i> <i>(d) Uses and disclosures for health oversight activities</i> <i>(e) Disclosures for judicial and administrative proceedings</i> <i>(f) Disclosures for law enforcement purposes</i> <i>(g) Uses and disclosures about decedents</i> <i>(h) Uses and disclosures for cadaveric organ, eye or tissue donation purposes</i> <i>(i) Uses and disclosures for research purposes</i> <i>(j) Uses and disclosures to avert a serious threat to health or safety</i> <i>(k) Uses and disclosures for specialized government functions</i> <i>(l) Disclosures for workers' compensation</i> <p>? Is the workforce familiar with the special circumstances that would allow for the disclosure of PHI without a consent or authorization?</p> <p>? Are patients notified of uses and disclosures that may be made without their consent or authorization?</p> <p><small>Clarification: The regulations provide methods by which these uses and disclosures may be conducted. These uses and disclosures are limited and are outlined in detail in the regulations. The regulations give considerations to entities acting in good faith to protect the privacy rights of individuals when disclosing PHI for these purposes.</small></p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Develop detailed policies outlining each of these uses and disclosures with elements necessary for compliance. ▪ Include in Notice of Privacy Practices the organizations practices for permitting identified uses and disclosures without consent or authorization in limited circumstances pursuant to HIPAA standards. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p> <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>De-identification of PHI</p> <p>§164.514(a)</p> <p>Operational</p>	<p><i>Individual health information loses its HIPAA protections and may be used or disclosed freely if it cannot be used to identify an individual.</i></p> <p>? Are you aware of the 19 identifiers that de-identify PHI data and free it for disclosure?</p> <p><u>Clarification:</u> To be considered “de-identified,” the health information cannot contain any of the nineteen specific identifiers of the individual and his/her relatives, employers, or household members. However, it is possible that, even if one or more identifiers remain, information can still be treated as de-identified if a qualified statistician determines that the risk of identification is very small.</p> <p>The nineteen identifiers are:</p> <ol style="list-style-type: none"> 1. Name 2. All address information 3. E-mail addresses 4. Dates (except year) 5. Social Security Number 6. Medical record numbers 7. Health plan beneficiary numbers 8. Account numbers 9. Certificate numbers 10. License numbers 11. Vehicle identifiers 12. Facial photographs 13. Telephone numbers 14. Device identifiers 15. URLs 16. IP addresses 17. Biometric identifiers 18. The geographic unit formed by combining all zip codes with the same three initial digits containing more than 20,000 people and the initial three digits of all geographic unit with fewer than 20,000 people is changed to 000. 19. Any other unique identifying number, characteristic, or code and 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 	<input type="checkbox"/> Yes	<input type="checkbox"/> No ➔	<ul style="list-style-type: none"> ▪ Implement a release of information policy that requires senior level authorization on de-identified health information. ▪ Develop a checklist with the eighteen identifiers for de-identifying PHI data to be used for verification when preparing de-identifiable data files. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Uses and Disclosures of PHI for Marketing</p> <p>§164.514(e)</p> <p>Operational</p>	<p><i>Providers may use limited patient information (demographics and dates of service), without authorization, for marketing and fund raising activities.</i></p> <p>? Do you know what patient information may be used for fund raising activities and marketing purposes?</p> <p><u>Clarification:</u> Except for general communications (i.e., newsletters), disclosures for marketing and fund raising must notify individuals on how their name may be removed from receiving future solicitations.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Inform individuals of the right to opt-out of marketing and fund raising communications as part of patient registration by including a statement of choice. ▪ Include the organization's marketing and fund raising policy in the Notice of Privacy Practices. Identify marketing practices pertaining to face-to-face encounters and products with nominal value. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Notice of Privacy Practices for PHI</p> <p>§164.520</p> <p>Operational</p>	<p><i>Covered entities must provide individuals with Notice of Privacy Practices.</i></p> <p>? Are you familiar with the prerequisites of the Notice of Privacy Practices documentation and do you have a process for assuring that this information reaches every individual seen in your office?</p> <p><u>Clarification:</u> The notice must be in "plain language" and include the following: (1) information regarding uses and disclosures of PHI (2) clarification of an individual's privacy rights (3) the covered entity's responsibilities under HIPAA (4) how to file complaints with the covered entity or Secretary of HHS (5) the name, title, and phone number of a contact person for more information and (6) the effective date of the notice.</p> <p>A provider that has a direct treatment relationship with the individual must provide the notice no later than the date of the first service delivery (including services delivered electronically). The notice must be available at the service delivery site for distribution upon request and posted in a prominent location.</p> <p>Providing an electronic notice satisfies the privacy practices notice requirement. Covered entities that are part of organized health care arrangements may use a joint notice. Covered entities must retain copies of the notices issued for six years.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Openly display the Notice of Privacy Practices in patient waiting areas. ▪ Give Notice of Privacy Practices to each patient at time of office visit or as part of admission process. ▪ Update policies to include the defined elements of the Notice of Privacy Practices. ▪ If a web site is used to outline customer services or benefits prominently post the Notice of Privacy Practices and make available electronically through the web site. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Rights to Request Privacy Protection for PHI</p> <p>§164.522(a)</p> <p>Consumer Control</p>	<p><i>A covered entity must allow an individual to request that the covered entity restrict (1) uses and disclosure for treatment, payment and health care operations and (2) disclosures permitted for involvement in the individual's care and notification purposes.</i></p> <p>? Do you fully understand your rights and those of patients who may request restrictions on the use and disclosure of their PHI?</p> <p><u>Clarification:</u> The restriction must be properly documented and retained for six years. However, the covered entity is not required to agree to the restriction. If the covered entity agrees to the restriction, it must abide by it except in emergency situations. A covered entity may terminate its agreement to a restriction if the individual agrees to or request the termination of the restriction, or if the covered entity informs the individual that it is terminating the restriction.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Carefully review uses and disclosure practices with the patient as part of the initial visit. Ask the patient to identify restrictions of PHI. ▪ Include language in the Notice of Privacy Practices that patients have the right to request in writing restrictions on the uses and disclosures of their PHI, and that the covered entity is not required to agree with a requested restriction. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Confidential Communications Requirements</p> <p>§164.522(b)</p> <p>Consumer Control</p>	<p><i>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.</i></p> <p>? 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?</p> <p><u>Clarification:</u> This standard permits individuals to receive communications of PHI from a covered health care provider or a health plan by an alternative means or at an alternative address.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Verify contact information and address as part of scheduling office visits. Include a section for alternative contact information on patient registration form. ▪ Define the boundaries of "reasonable" in the Notice of Privacy Practices document by noting when your office will provide health information to an alternative address or by an alternative means. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Access of Individuals to PHI</p> <p>§164.524</p> <p>Consumer Control</p>	<p><i>The individual has a right to inspect and copy his or her PHI, in whole or in part, for as long as the covered entity maintains the information.</i></p> <p>? Are your medical files managed in a way that allows for patient inspection and/or release of files?</p> <p><u>Clarification:</u> Individuals do not have an automatic right to access (1) psychotherapy notes (2) information on a criminal, civil or administrative action or proceeding or (3) PHI that is maintained by a covered entity that is subject to or exempted from Clinical Laboratory Improvements Amendments (CLIA) to the extent the provision of access would be prohibited by law.</p> <p>The covered entity must act on a request for access within 30 days of receiving the request if the information is maintained and accessible on-site or within 60 days otherwise. The covered entity may grant itself a 30-day extension if certain conditions are met. Under certain circumstances a covered entity may deny a request for access of the PHI. For example, when access would endanger the life or safety of the individual. In the event that request for access is denied, the covered entity must provide the individual an opportunity for review. The covered entity must designate a health care professional who did not participate in the original denial to conduct the review. The review decision must be made in a reasonable period of time and written notice of the review decision must be provided to the individual. Fees may be charged for access to PHI to cover the cost of photocopying, mailing, and summary preparation. The covered entity may provide the individual with a summary of the PHI request if the individual agrees to advance to the summary and to the fees imposed. The covered entity must retain the designated record sets that are subject to access by individuals and the titles of persons or offices responsible for processing requests for six years.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Include language in Notice of Privacy Practices that patients have the right to access their personal health information for the previous six years. ▪ Record patient requests for access to their medical records in patient's file. ▪ As part of initial visit, advise patients of the right to access their medical records and the associated costs of doing so. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Amending PHI</p> <p>§164.526</p> <p>Consumer Control</p>	<p><i>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.</i></p> <p>? Are you aware of your obligations and rights should a patient request amendments be made to their medical record?</p> <p>? If yes, do you have a process in place for doing so?</p> <p><u>Clarification:</u> A covered entity may deny the request for amendment if (1) the PHI was not created by the covered entity (unless the individual claims the originator of the PHI is no longer available to amend the PHI) (2) the PHI is not part of the designated record set (3) the PHI was not available for inspection or (4) the PHI is accurate and complete. The covered entity may require the individual to make the request for amendment in writing and provide the rationale for the request. The covered entity must act within 60 days of the request (with a possible 30-day extension similar to that described for access to PHI). If the request for amendment is granted, the covered entity must notify the individual that amendment was accepted and obtain the individual's identification of and agreement to inform relevant persons. The covered entity must make reasonable efforts to inform relevant persons. The covered entity must make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the individual and the covered entity, including business associates.</p> <p>If the request for amendment is denied, the covered entity must provide the individual with a timely written notice. The notice must explain the reason for denial, the individual's right to submit a written statement of disagreement or to have the request for amendment included with future disclosures, and the individual's right to complain to the covered entity or the Secretary of HHS. The covered entity may prepare a rebuttal statement to the individual's state of disagreement. A copy of the rebuttal statement must be provided to the individual. Future disclosures of the PHI must include the statement of disagreement or request for amendment, the denial notice, and the rebuttal or summary of this information. If a covered entity informs another covered entity of a necessary amendment of PHI, the covered entity must amend the record. The covered entity must retain documentation for six years.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Include patient's right to amend PHI in the Notice of Privacy Practices. Outline process for making such a request. ▪ Implement procedures requiring appropriate provider signatures to approve amendments to patient records or resolving disputes. Retain approval or denial documentation as part of the medical record. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p> <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Accounting of Disclosures of PHI</p> <p>§164.528</p> <p>Consumer Control</p>	<p><i>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, except for the following disclosures.</i></p> <p><i>(1) For payment, treatment, and health care operations (2) to the individual (3) for the facility's directory or to persons involved in the individual's care (4) for national security or intelligence purposes (5) to correctional institutions or law enforcement officials (6) which occurred prior to the HIPAA compliance date.</i></p> <p>? Are you currently documenting medical record disclosures on your patients?</p> <p><u>Clarification:</u> The covered entity must act on the request for an account of disclosure within 60 days with possible 30-day extensions as was described for accessing PHI. The covered entity must provide individuals with the first accounting at no charge. For subsequent requests within the same 12 month period, the covered entity may charge a reasonable, cost-based fee.</p> <p>The covered entity must provide a written account of each specific disclosure that includes the date of the disclosure, the person to whom the information was disclosed, brief description of the disclosed information, or, in lieu of the summary, a copy of the authorization or request for disclosure.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Maintain records of all patient disclosures regarding PHI as part of the medical record. Include in the documentation the date, description, and to whom information was disclosed. ▪ Implement procedures to authenticate patient requests for accounting and disclosure of PHI. ▪ Incorporate the patient's rights to receive a disclosure log of their PHI for <i>six years</i> prior to the date on which the accounting is requested in the Notice of Privacy Practices. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Personnel Designations §164.530(a) Administration	<p><i>Covered entities must designate a Privacy Official who is responsible for the development and implementation of the policies and procedures of the entity and a contact person or office to receive complaints and provide further information about the covered entity's privacy practices.</i></p> <p>? Is there an employee among your office staff designated to carry out the requirements of the HIPAA privacy standards?</p> <p>? Is there an employee among your office staff designated as the contact person for complaints and providing privacy practice information?</p> <p><u>Clarification:</u> One employee is to be designated to be responsible for overseeing the implementation of policies and procedures, including the Notice of Privacy Practices as well as the employee policies manual on HIPAA standards and to ensure HIPAA compliance.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Identify a staff member with knowledge of your organization with authority to investigate complaints to fill the role of Privacy Official. Designate an individual to address privacy complaints. Two different individuals or one in the same can handle these roles. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p> <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
Training §164.530(b) Administration	<p><i>A covered entity must train members of its workforce about the entity's policies and procedures for PHI and document that training has been provided.</i></p> <p>? Do you currently hold training sessions (or staff meetings) to facilitate PHI training?</p> <p>? Do you maintain records of those in attendance at trainings?</p> <p><u>Clarification:</u> Training must be completed:</p> <ul style="list-style-type: none"> ▪ For each member of the covered entity's workforce by no later than the compliance date for the covered entity; and ▪ Thereafter, for each new member of the workforce, within a reasonable period of time following the date of hire; and ▪ Within a reasonable period of time after a material change in the entity's privacy policies and procedure becomes effective. 	<input type="checkbox"/> Yes <input type="checkbox"/> Yes	<input type="checkbox"/> No➔ <input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Identify policies and procedures relating to PHI. Determine appropriate personnel for training. Request workforce sign documentation outlining items covered during training and place copy in employee personnel files. ▪ Conduct PHI training upon hire and refresher training annually. Request workforce sign a statement of completion at the end of refresher training and place in employee personnel files. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p> <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
Safeguards §164.530(c) Administration	<p><i>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.</i></p> <p>? Do you have policies in place to secure and restrict access?</p> <p>? Is your office staff aware of the importance of consistent patient confidentiality practices when handling files, answering the phone, faxing, etc.?</p> <p>? Do you have a security policy to protect electronic medical information?</p> <p><u>Clarification:</u> Assure that employees use logins and passwords to access health information and that computers are safely secured from unauthorized use.</p>	<input type="checkbox"/> Yes <input type="checkbox"/> Yes <input type="checkbox"/> Yes	<input type="checkbox"/> No➔ <input type="checkbox"/> No➔ <input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Determine level of PHI access needed by each member of the workforce to complete his or her job. ▪ Establish access levels to PHI using logins and passwords as determined by job duties. ▪ Include security awareness as part of initial employee training and refresher training programs. ▪ Add manual locks to unsecured cabinets or store PHI in a secure location. ▪ Train workforce to limit conversations regarding PHI to private locations. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p> <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p> <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Complaints to the Covered Entity</p> <p>§164.530(c)</p> <p>Administration</p>	<p><i>A covered entity must provide a process for individuals to make complaints concerning its policies and procedures or its compliance with its policies and procedures or the requirements of the regulation.</i></p> <p>? Does your office currently have a course of action for patient complaints?</p> <p><i>Clarification:</i> The covered entity must document all complaints received and their disposition.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Advise patients during the registration process of the procedure to file a complaint. Include steps to file a complaint in the Notice of Privacy Practices. ▪ Designate a member of the workforce as the contact person for receiving and documenting complaints. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Sanctions</p> <p>§164.530 (e)</p> <p>Administration</p>	<p><i>A covered entity must have and apply appropriate sanctions against its employees who fail to comply with the entity's privacy policies and procedures or the regulations.</i></p> <p>? Do you have a policy in place designed to handle a breach in patient confidentiality?</p> <p>? Are you and your office staff aware of the ramifications of violating an individual's rights under the new law?</p> <p><i>Clarification:</i> Sanctions are not to be applied in certain situations, i.e. disclosures by whistleblowers and workforce member crime victims or as intimidating or retaliatory acts.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Specify in the employee policies manual the organization's policy for dealing with privacy infractions. Review with employees upon hire and at refresher training. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<input type="checkbox"/> Yes	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Refraining from Intimidating or Retaliatory Acts</p> <p>§164.530(g)</p> <p>Administration</p>	<p><i>A covered entity may not intimidate, threaten, coerce, discriminate or retaliate against an individual.</i></p> <p>? Is your office staff encouraged to identify areas of potential non-compliance with the new law?</p> <p><u>Clarification:</u> Action cannot be taken against an individual who exercises any right or process established under the regulation, including: the filing of a complaint, testifying, assisting, or participating in an investigation, compliance review, or hearing. Individuals can choose not to participate in any act or practice made unlawful by the regulation, provided the individual or person has a good faith belief that the practice opposed is unlawful, and that the manner of the opposition is reasonable and does not involve a disclosure of PHI that in itself constitutes violation.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> Offer employee-training programs that clarify the philosophy of management surrounding compliance with the Privacy Regulations. Management must train employees to exercise sound decisions that adhere to existing policies and to feel safe reporting non-compliance matters to the Privacy Official. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Waiver of Rights</p> <p>§164.530(h)</p> <p>Administration</p>	<p><i>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.</i></p> <p>? Do you convey objective behavior and/or opinions to your patients?</p> <p><u>Clarification:</u> Patient must be informed by the organization that they have the right to file complaints and that the filing of a complaint will not interfere with their health care.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> Include language in the Notice of Privacy Practices that patients will not be asked to waive their rights to file a complaint with the Department of Health & Human Services as a condition of treatment. Include contact information for the Office of Civil Rights in the Notice of Privacy Practices. ((866)-OCR-PRIV) <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Policies and Procedures</p> <p>§164.530(i)(1)</p> <p>Administration</p>	<p><i>A covered entity must develop and implement policies and procedures relating to PHI that are designed to comply with the elements of the regulations.</i></p> <p>? Is there an employee among your office staff designated to develop and implement policies and procedures to carry out the requirements of the HIPAA privacy standards?</p> <p><i>Clarification:</i> The policies and procedures must take into account the size of and the type of activities that relate to PHI undertaken by the covered entity.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Develop policies and procedures specific to HIPAA privacy requirements. Maintain in an electronic document or a hard copy for easy access by employees. ▪ Privacy policies and procedures should be developed in a manner that takes into account the <i>size</i> of and <i>type</i> of activities that relate to PHI by the covered entity. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Changes to Policies or Procedures</p> <p>§164.530(i)(2)</p> <p>Administration</p>	<p><i>A covered entity must revise its policies and procedures as necessary and appropriate to comply with changes in the law or regulations, or when it changes a privacy practice that is stated in its notice of privacy practices.</i></p> <p>? Is there an employee among your office staff designated to maintain and update policies and procedures, and to carry out the requirements of the HIPAA privacy standards?</p> <p><i>Clarification:</i> A covered entity must change policies and procedures as necessary to comply with changes in law.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ A role of the Privacy Official is to monitor changes in the law, include as part of their job responsibility the task of updating all relevant documentation, employee training documents, and re-train existing employees. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Changes to Privacy Practices Stated in the Notice of Privacy Practices</p> <p>§164.530(i)(4)</p> <p>Administration</p>	<p><i>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.</i></p> <p>? 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?</p> <p><u>Clarification:</u> The covered entity may change a privacy practice stated in the notice without having reserved the right to do so, provided that the change meets the implementation requirements described in the section and the change is effective only for PHI created or received after the effective date of the notice.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Include language in the Notice of Privacy Practices that the covered entity reserves the right to change a privacy practice and outline activities of the organization regarding implementing changes in the law or operation relative to PHI. ▪ Inform patients of substantial changes in the Notice of Privacy Practices as part of the registration process. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Documentation</p> <p>§164.530(j)</p> <p>Administration</p>	<p><i>A covered entity must maintain its policies and procedures in written or electronic form for six years from the date of creation of the policies and procedures, or from the date when the policies and procedures became effective, whichever ever is later.</i></p> <p>? Are your policies and procedures managed in a way that would allow employees access to them for the last six years?</p> <p><u>Clarification:</u> For any communication required by the regulation to be in writing, the covered entity must maintain a written or electronic copy as documentation.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Store HIPAA policies in binders accessible to employees. Provide employees with a copy of the HIPAA policies annually. Where possible, set up policies and procedures in an electronic format. Index policies and procedures by versions to comply with the six year retention rule. ▪ Include in your Notice of Privacy Practices that you reserve the right to make changes at any time to your policies and procedures. Indicate how changes will be communicated to patients. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Retention Period</p> <p>§164.530(j)(2)</p> <p>Administration</p>	<p><i>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.</i></p> <p>? Do you have date sensitive standards for all documentation in written or electronic form?</p> <p><u>Clarification:</u> A covered entity must retain written and electronic documentation for six years.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> Include a purge date on all written and electronic documentation. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Prior Consents and Authorizations</p> <p>§164.532 (a)</p> <p>Administration</p>	<p><i>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, even though the consent does not strictly comply with the requirements for consent or authorization.</i></p> <p>? Is staff educated on the organization's HIPAA implementation timeline, which provides for a transition period for using existing consents and authorizations?</p> <p><u>Clarification:</u> The covered entity must not make any use or disclosure that is expressly excluded from the consent or authorization or other express legal permission obtained from the individual prior to the implementation date, and must comply with any limitations placed by the individual executing the document. This provision also applies generally to uses and disclosures relating to treatment, payment, and health care operations, and to research projects, with respect to PHI received or created prior to the compliance date and subject to any limitations or exclusions contained in the original permission.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> Train workforce to understand what PHI information can be used or disclosed prior to the HIPAA implementation date as part of their initial training. Clearly outline changes relating to use and disclosure of PHI after the implementation date. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Compliance Dates for Initial Implementation of the Privacy Standards</p> <p>§164.534</p> <p>Administration</p>	<p><i>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.</i></p> <p>? Do you have an action plan for contacting payers to determine their HIPAA readiness prior to the implementation date?</p> <p><i>Clarification:</i> Small health plans (\$5,000,000 or less in revenue) must comply within 36 months of the effective date of the regulations.</p>	<p><input type="checkbox"/></p> <p>Yes</p>	<p><input type="checkbox"/></p> <p>No➔</p>	<ul style="list-style-type: none"> ▪ Contact major payers to obtain their targeted HIPAA compliance date. Some payers expect to implement HIPAA standards well in advance of the required date. Most covered entities are required to comply with the standards within 24 months of the effective date. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>General Rule and Exceptions – State Law</p> <p>§160.203</p> <p>Administration</p>	<p><i>Conflicting state law is preempted.</i></p> <p>? Are you familiar with Maryland State Law regarding confidentiality of medical records?</p> <p><i>Clarification:</i> There are four exceptions to this general rule: (1) the Secretary 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. (2) To ensure appropriate State regulations of insurance and health plans to the extent expressly authorized by statute or regulations (3) For State reporting on health care delivery or cost. (4) For purposes of serving a compelling need related to public health, safety, or welfare or if the Secretary determined that an intrusion into privacy is warranted as determined by the need.</p> <p>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 (6) provides any other greater privacy protection.</p>	<p><input type="checkbox"/></p> <p>Yes</p>	<p><input type="checkbox"/></p> <p>No➔</p>	<ul style="list-style-type: none"> ▪ Familiarize all employees with current State Law. Train employees to recognize where existing state laws supersede these federal regulations when State Law provides greater protections for individuals. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Complaints to the Secretary of HHS</p> <p>§160.306</p> <p>Administration</p>	<p><i>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.</i></p> <p>? Have you included in your Notice of Privacy Practices the right for individuals to file a complaint with the Secretary of HHS?</p> <p><u>Clarification:</u> Complaints to the Secretary must be in writing or electronic and must include the covered entities contact information and the nature of the violation.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> Advise patients during the registration process of the right to file a complaint and the appropriate steps. Include a section in the <i>Notice of Privacy Practices</i> on complaints. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Requirements for Filing Complaints</p> <p>§160.306(b)</p> <p>Administration</p>	<p><i>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 time limit is waived by the Secretary for good cause shown.</i></p> <p>? Have you included in your Notice of Privacy Practices the process by which individuals may file a complaint with the Secretary of HHS?</p> <p><u>Clarification:</u> Patients and family members need to be advised on the time frame in which they are permitted to file a complaint with the Secretary of HHS and that the complaint must be in writing and must name the covered entity in question.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> Advise patients during the registration process of the right to file a complaint and the appropriate steps. Include a section in the <i>Notice of Privacy Practices</i> on complaints. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>

HIPAA PRIVACY STANDARD	REQUIREMENT(S)	HIPAA READINESS		INDUSTRY DEVELOPED STRATEGY TO ASSIST PRACTITIONERS & FACILITIES
<p>Responsibilities of Covered Entities: Provide Records and Compliance Reports</p> <p>§160.310</p> <p>Administration</p>	<p><i>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 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.</i></p> <p>? Does your office have a process in place to respond to requests for information and documentation from the Secretary?</p> <p><u>Clarification:</u> All policies and procedures and all other documentation of compliance with HIPAA Privacy Standards are to be maintained in the event of a request by the Secretary of HHS.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Develop a summary document that outlines HIPAA activities of the organization. ▪ Delegate Privacy Official as contact regarding HIPAA compliance. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<p>Responsibilities of Covered Entities: Cooperate with Complaint Investigations and Compliance Reviews</p> <p>§160.310 (b)(c)</p> <p>Administration</p>	<p><i>Requires a covered entity to cooperate with the Secretary in investigations or compliance review of policies, procedures, or practices of a covered entity.</i></p> <p>? Is workforce trained on their responsibility to cooperate with the Secretary regarding all investigations or compliance reviews?</p> <p>? Is your workforce aware that they must permit access to information and documentation by the Secretary at any time and without notice?</p> <p><u>Clarification:</u> 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.</p>	<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ▪ Inform workforce during orientation of management's willingness to participate in HHS investigations. ▪ Clearly identify for the workforce on all organizational flow charts a Privacy Official and contact person for complaints, and requests for additional information. <p>➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing</p>
<input type="checkbox"/> Yes	<input type="checkbox"/> No➔	<ul style="list-style-type: none"> ➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing ➔ <input type="radio"/> Not applicable <input type="radio"/> Needs developing 		

HIPAA PRIVACY READINESS SELF ASSESSMENT

Overall, I would consider my practice and/or organization to be:

_____ **Mostly compliant** with the HIPAA Privacy Regulation requirements.

_____ **Somewhat compliant** with the HIPAA Privacy Regulation requirements.

_____ **Not at all compliant** with the HIPAA Privacy Regulation requirements.

Maryland Health Care Commission

V. Business Associate Contract

Practitioner and Facility Development Tips

Business Associates are expected to adhere to the same standards as the covered entity as to protected health information. Business Associates include people or entities performing a function for or assisting a covered entity involving the use or disclosure of protected health information. Business Associate Contracts are not required for practitioners or facilities in treatment of a patient. ***This document provides practitioners and facilities with best practice guidelines for developing an organization specific Business Associate Contract.***

Under HIPAA, the Department of Health and Human Services has no direct jurisdiction over Business Associates. Covered entities are expected to ensure continued privacy protections of health information by entering into Business Associate Contracts. As part of the Business Associate Contract, covered entities are required to investigate when complaints are received or other information containing substantial and credible evidence of violations by a Business Associate. ***A covered entity that becomes aware of a material breach by a Business Associate is required to take reasonable steps to correct the breach or terminate the contract with the Business Associate.***

Best Practices - Development Guidelines:

- *Solicit legal counsel to develop and review Business Associate Contract language.*
- *Business Associate agrees not to use or further disclose the information provided or made available by Covered Entities for any purpose other than as expressly permitted or required by the contract.*
- *Covered entities may use or disclose information in limited situations. These uses and disclosures must be within the scope of the Business Associate's services provided to the covered entity such as: claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and repricing; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.*
- *Business Associate is permitted to use or disclose information if necessary for management and administration or to carry out legal responsibilities provided: The Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially, and agrees that the information provided by the covered entity will not be further used or disclosed other than as permitted or required by the contract or as required by law. Business Associate is permitted to provide data aggregation services relating to the health care operations of the covered entity.*
- *Appropriate Safeguards: Business Associate will establish and maintain reasonable safeguards to prevent any use or disclosure of the information, other than as specified in the contract.*

Maryland Health Care Commission

- *Subcontractors and Agents:* Business Associate agrees that anytime information is provided or made available to any subcontractors or agents, Business Associate must enter into a subcontract that contains the same terms, conditions and restrictions on the use and disclosure of information as contained in the contract.
- *Right of Access to Information:* Business Associate agrees to make available and provide a right of access to information by the individual for whom the information was created and disclosed.
- *Provide Accounting:* Business Associate agrees to make information available as required to provide an accounting of disclosures.
- *Access to Books and Records:* Business Associate agrees to make its internal practices, books, and records relating to the use or disclosure of information received from, or created or received by Business Associate on behalf of the covered entity, available to the Secretary of HHS for purposes of determining compliance with the privacy regulations.
- *Return or Destruction of Information:* At termination of the contract, Business Associate agrees to return or destroy all information received from, or created by the covered entity.
- *Reporting Procedures:* Business Associate must report to the Covered Entity any use or disclosure of information not provided for by its contract or of which it becomes aware.
- *Amendment Procedure:* Business Associate must make available protected health information for amendment and incorporate any amendments to PHI according to the regulations
- *Sanction Procedures:* Business Associate must develop and implement a system of sanctions for any employee, subcontractor or agent who violates the privacy regulations.
- *Property Rights:* The information shall be and remain the property of the covered entity. The Business Associate agrees that it acquires no title or rights to the information, including any de-identified information, as a result of the contract.
- *Termination of Contract:* Business Associate agrees that the covered entity has the right to immediately terminate the contract if the covered entity determines that Business Associate has violated the privacy regulations.

Maryland Health Care Commission

Sample Business Associate Contract Form:

This form is provided without any warranty, expressed or implied, as to its legal effect and completeness. Use of this form is entirely at your own risk.

THIS CONTRACT:

Is entered into on this _____ day of _____, 2001, between Provider/Plan/Clearinghouse and Vendor/Person(s).

WITNESSETH:

WHEREAS, COVERED ENTITY will make available and/or transfer to BUSINESS ASSOCIATE certain information, in conjunction with goods or services that are being provided by BUSINESS ASSOCIATE to COVERED ENTITY, that is confidential and must be afforded special treatment and protection. WHEREAS, BUSINESS ASSOCIATE will have access to and/or receive from COVERED ENTITY certain information that can be used or disclosed only in accordance with this Contract and the HHS Privacy Regulations.

COVERED ENTITY and BUSINESS ASSOCIATE:

Agree as follows: Limits On Use And Disclosure Established By Terms Of Contract. BUSINESS ASSOCIATE hereby agrees that it shall be prohibited from using or disclosing the information provided or made available by the covered entity for any purpose other than as expressly permitted or required by the contract.

The term of this Contract shall commence as of _____ (the Effective Date), and shall expire when all of the information provided by COVERED ENTITY to BUSINESS ASSOCIATE is destroyed or returned to the covered entity.

THE PARTIES:

Hereby agree that BUSINESS ASSOCIATE shall be permitted to use and/or disclose information provided or made available from the covered entity for the following stated purposes: *Include a general statement describing the stated purposes that BUSINESS ASSOCIATE may use or disclose the Information.* These uses and disclosures must be within the scope of the BUSINESS ASSOCIATE'S representation of the covered entity.

Additional purposes for which the BUSINESS ASSOCIATE may use or disclose information:

1. BUSINESS ASSOCIATE is permitted to use information if necessary for the proper management and administration of BUSINESS ASSOCIATE or to carry out legal responsibilities of BUSINESS ASSOCIATE.
2. BUSINESS ASSOCIATE is permitted to disclose information received from COVERED ENTITY for the proper management and administration of BUSINESS ASSOCIATE or to carry out legal responsibilities of BUSINESS ASSOCIATE, provided the disclosure is required by law; or the 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 purposes for which it was disclosed to the person, the person will use appropriate safeguards to prevent use or disclosure of the information, and the person immediately notifies the BUSINESS ASSOCIATE of any instance of which it is aware in which the confidentiality of the information has been breached.

Maryland Health Care Commission

3. BUSINESS ASSOCIATE is also permitted to use or disclose information to provide data aggregation services, as that term is defined by 45 C.F.R. 164.501, relating to the healthcare operations of the covered entity.
4. BUSINESS ASSOCIATE will establish and maintain appropriate safeguards to prevent any use or disclosure of the information, other than as provided for by the contract.

REPORTS OF IMPROPER USE OR DISCLOSURE:

BUSINESS ASSOCIATE hereby agrees that it shall immediately report to the Covered Entity any discovery use or disclosure of information not provided for or allowed by the contract.

SUBCONTRACTORS AND AGENTS:

BUSINESS ASSOCIATE hereby agrees that anytime information is provided or made available to any subcontractors or agents, BUSINESS ASSOCIATE must enter into a subcontract with the subcontractor or agent that contains the same terms, conditions, and restrictions on the use and disclosure of information as contained in the contract. Businesses Associate must obtain the Covered Entity's approval prior to entering into such agreements

RIGHT OF ACCESS TO INFORMATION:

BUSINESS ASSOCIATE hereby agrees to make available and provide a right of access to information by the Individual in accordance with 45 F.R.R. 164.524, including substitution of the words Covered Entity with Business Associate where appropriate.

AMENDMENT AND INCORPORATION OF AMENDMENTS:

BUSINESS ASSOCIATE agrees to make Information available for amendment and to incorporate any amendments to information in accordance with 45 C.F.R. 164.526, including substitution of the words covered entity with BUSINESS ASSOCIATE where appropriate.

PROVIDE ACCOUNTING:

BUSINESS ASSOCIATE agrees to make information available as required to provide an accounting of disclosures in accordance with 45 C.F.R. 164.528, including substitution of the words covered entity with BUSINESS ASSOCIATE where appropriate.

ACCESS TO BOOKS AND RECORDS:

BUSINESS ASSOCIATE hereby agrees to make its internal practices, books, and records relating to the use or disclosure of information received from, or created or received by BUSINESS ASSOCIATE on behalf of the covered entity, available to the Secretary or the Secretary's designee for purposes of determining compliance with the privacy regulations.

RETURN OR DESTRUCTION OF INFORMATION:

At termination of the contract, BUSINESS ASSOCIATE hereby agrees to return or destroy all information received from, or created or received by BUSINESS ASSOCIATE on behalf of the covered entity. BUSINESS ASSOCIATE agrees not to retain any copies of the information after termination of the contract. If return or destruction of the information is not feasible, BUSINESS ASSOCIATE agrees to extend the protections of the contract for as long as necessary to protect the information and to limit any further use or disclosure. If BUSINESS ASSOCIATE elects to destroy the information, it shall certify to the covered entity that the information has been destroyed.

Maryland Health Care Commission

MITIGATION PROCEDURES:

BUSINESS ASSOCIATE agrees to have procedures in place for mitigating, to the maximum extent practicable, any deleterious effect from the use or disclosure of information in a manner contrary to the contract or the privacy regulations.

SANCTION PROCEDURES:

BUSINESS ASSOCIATE agrees and understands that it must develop and implement a system of sanctions for any employee, subcontractor or agent who violates this agreement or the privacy regulations.

PROPERTY RIGHTS:

The information shall be and remain the property of the covered entity. BUSINESS ASSOCIATE agrees that it acquires no title or rights to the information, including any de-identified information, as a result of the contract.

CONTRACT TERMINATION:

BUSINESS ASSOCIATE agrees that the covered entity has the right to immediately terminate the contract and seek relief under the Disputes Article if the covered entity determines that BUSINESS ASSOCIATE has violated a material term of the contract.

GROUND FOR BREACH:

Any non-compliance by BUSINESS ASSOCIATE with the contract or the privacy regulations will automatically be considered to be a grounds for breach, if BUSINESS ASSOCIATE knew and failed to immediately take reasonable steps to cure the non-compliance.

DISPUTES:

Any controversy or claim arising out of or relating to the contract will be finally settled by compulsory arbitration in accordance with the Commercial Arbitration Rules of the American Arbitration Association, except for injunctive relief as described below.

INJUNCTIVE RELIEF:

Notwithstanding any rights or remedies provided for in the contract, the covered entity retains all rights to seek injunctive relief to prevent or stop the unauthorized use or disclosure of information by BUSINESS ASSOCIATE or any agent, contractor or third party that received information from BUSINESS ASSOCIATE.

MISCELLANEOUS:

The contract shall be binding on the parties and their successors, but neither party may assign this agreement without the prior written consent of the other, which consent shall not be unreasonably withheld.

NOTICES:

Whenever under the contract one party is required to give notice to the other, such notice shall be deemed given if mailed by first class United States mail, postage prepaid:

Company Name: _____ Address: _____

Contact Person: _____ Title: _____

Maryland Health Care Commission

COVERED ENTITY:

[Name/Address] either party may at any time change its address for notification purposes by mailing a notice stating the change and setting forth the new address.

BUSINESS ASSOCIATE:

[Name/Address] either party may at any time change its address for notification purposes by mailing a notice stating the change and setting forth the new address.

GOOD FAITH:

The parties agree to exercise good faith in the performance of the contract.

ATTORNEY'S FEES:

Except as otherwise specified in the contract, if any legal action or other proceeding is brought for the enforcement of the contract, or because of an alleged dispute, breach, default, misrepresentation, or injunctive action, in connection with any of the provisions of the contract, each party shall bear their own legal expenses and the other cost incurred in that action or proceeding.

ENTIRE AGREEMENT:

The contract consists of this document, and constitutes the entire agreement between the parties. There are no understandings or agreements relating to this agreement which are not fully expressed in the contract and no change, waiver or discharge of obligations arising under the contract shall be valid unless in writing and executed by the party against whom such change, waiver or discharge is sought to be enforced.

IN WITNESS WHEREOF:

BUSINESS ASSOCIATE and COVERED ENTITY have caused this Contract to be signed and delivered by their duly authorized representatives, as of the date set forth above.

BUSINESS ASSOCIATE COVERED ENTITY

By: _____

By: _____

Print Name: _____

Print Name: _____

Title: _____

Title: _____

Maryland Health Care Commission

VI. Chain of Trust Partner Agreement

Practitioner and Facility Development Tips

Chain of Trust Partner Agreements is part of a comprehensive information security program consisting of written policies and procedures. These policies and procedures cover operating standards, training, technical and procedural controls, risk assessment, auditing and monitoring, and assigned responsibility for management of the information security program. ***This document provides practitioners and facilities with best practice guidelines for developing an organization specific Chain of Trust Partner Agreement.***

Best Practices - Development Guidelines:

- *Solicit legal counsel to develop and review contract language for Chain of Trust Partner Agreements.*
- *Identify all parties to be included in a Chain of Trust Partner Agreements.*
- *Look to utilize and modify existing confidentiality agreements currently in place with third party electronic trading partners.*
- *Identify data rights responsibilities and accountability of trading partners.*
- *Identify the consequences of failure by either party to abide by the Chain of Trust Partner Agreement.*
- *Establish a monitoring process and policy to ensure that compliance is met.*
- *Determine procedure if trading partner refuses to sign a Chain of Trust Partner Agreement.*

Maryland Health Care Commission

Sample Chain of Trust Partner Agreement:

This form is provided without any warranty, expressed or implied, as to its legal effect and completeness. Use of this form is entirely at your own risk.

This Chain of Trust Agreement is made the _____ day of _____, 2001, at _____, by and between HEALTH CARE ORGANIZATION (the "ORGANIZATION") and BUSINESS PARTNER (the "RECIPIENT"). WHEREAS, ORGANIZATION maintains and operates at _____ WHEREAS, RECIPIENT performs _____ work which requires it to have access to information regarding ORGANIZATION'S confidential and protected health information ("INFORMATION"); WHEREAS, ORGANIZATION desires to protect the confidentiality and integrity of the INFORMATION and to prevent inappropriate disclosure of the information; NOW THEREFORE, the parties agree as follows:

CONFIDENTIALITY:

RECIPIENT agrees that they will not use the INFORMATION in any way detrimental to ORGANIZATION, and that RECIPIENT will keep such INFORMATION confidential. It is understood and agreed by RECIPIENT that they will notify all applicable business partners and employees of the confidential nature of the INFORMATION and shall direct such parties to treat INFORMATION with due diligence and care. Neither party shall disclose protected health information or other information that is considered, proprietary, sensitive, or confidential unless there is a need to know basis. Both parties agree that they will limit distribution of confidential information to only parties with a legitimate need in performance of the services as herein provided under this agreement. Disclosure of confidential information is prohibited indefinitely, even after termination of employment or business relationship, unless specifically waived in writing by the authorized party. This section shall survive the termination, expiration, or cancellation of this agreement.

TERM:

This Agreement shall be effective _____, 2001, and shall continue _____. This agreement shall automatically renew itself for an additional twelve-month period unless otherwise terminated by either party. In the event that this Agreement is automatically renewed, RECIPIENT agrees to be bound by the Terms and Conditions currently in effect. The confidentiality provisions of this agreement shall survive indefinitely, even beyond the termination of this agreement.

DISCLOSURES REQUIRED BY LAW:

In the event that RECIPIENT is required by law to disclose INFORMATION, RECIPIENT agrees to provide ORGANIZATION with notice in a timely manner, so that ORGANIZATION may seek protective order as appropriate.

STATE AND FEDERAL STATUTE COMPLIANCE:

RECIPIENT warrants and represents that it is in compliance, or will become compliant with all relevant federal/state statutes, rules, regulations and applicable interpretive rulings in a timely manner. Further, both parties agree to remain in compliance with all relevant federal/state statutes, rules, and regulations during the entire term of this agreement. RECIPIENT agrees to maintain adequate safeguards to ensure that information exchanged between ORGANIZATION and RECIPIENT is protected and used solely for the purposes agreed upon within this agreement. Failure to comply with this provision can result in immediate and automatic termination of the previously agreed upon business relationship, without penalty or cost to either party.

Maryland Health Care Commission

POLICY AND PROCEDURE REVIEW:

RECIPIENT shall make available on demand to ORGANIZATION a copy of all policies and procedures relevant to safeguarding information.

REPORT OF IMPROPER DISCLOSURE OR SYSTEMS COMPROMISE:

ORGANIZATION and RECIPIENT agree to immediately notify all parties within their "Chain of Trust" of any improper or unauthorized access and disclosure of the information, any misuse of the information, including but not limited to systems' compromises. ORGANIZATION and RECIPIENT will take all necessary steps to prevent and limit any further improper or unauthorized disclosure and misuse of information. RECIPIENT shall also maintain an incident log of all improper or unauthorized disclosures. At the request of ORGANIZATION, RECIPIENT will make available to ORGANIZATION a copy of incident log.

RETURN OF MATERIALS:

Unless otherwise specifically required by statute or rule, RECIPIENT shall promptly return to ORGANIZATION all material containing or reflecting any ORGANIZATION proprietary information whether prepared by ORGANIZATION or as a result of providing services for which the RECIPIENT has been specifically authorized by ORGANIZATION. In addition, the RECIPIENT shall exercise due diligence to destroying the INFORMATION in a manner that will render non-identifiable all documents, memoranda, notes or other writings prepared by RECIPIENT, or its representatives, which are based on the INFORMATION.

SUB-CONTRACTORS:

If RECIPIENT discloses the INFORMATION to any subcontractor, independent contractor, or agent, it shall require such party to execute a Chain of Trust Agreement that upholds the same standards contained within this agreement.

ADDITIONAL ACCESS TO INFORMATION:

If RECIPIENT significantly alters the information provided by ORGANIZATION, ORGANIZATION shall have the right to access the altered information upon written request to RECIPIENT. Such access shall be provided to ORGANIZATION within a reasonable period after receipt of the request and shall be during the normal business hours of RECIPIENT. RECIPIENT shall incorporate changes or amendments to the INFORMATION if requested by the ORGANIZATION.

INJUNCTIVE RELIEF:

RECIPIENT acknowledges that the remedy at law for any breach by it or the terms of this agreement shall be inadequate and that the damages resulting from such breach are not readily susceptible to being measured in monetary terms. Accordingly, in the event of a breach or threatened breach by RECIPIENT of the terms of this agreement, ORGANIZATION shall be entitled to immediate injunctive relief and may obtain a temporary order restraining any threatened or further breach. Nothing herein shall be construed as prohibiting ORGANIZATION from pursuing any other remedies available to ORGANIZATION for such breach or threatened breach, including recovery of damages from RECIPIENT. RECIPIENT further represents that it understands and agrees that the provisions of this agreement shall be strictly enforced and construed against it.

THIRD PARTY BENEFICIARIES:

Both parties understand and agree that other parties (individuals or entities) who are the subject of the INFORMATION provided to RECIPIENT are intended to be third party beneficiaries of this Agreement.

Maryland Health Care Commission

SEVERABILITY:

In the event that any provision of this agreement violates any applicable statute, ordinance or rule of law in any jurisdiction that governs this agreement, such provision shall be ineffective to the extent of such violation without invalidating any other provision of this Agreement.

CONSTRUCTION OF AGREEMENT:

The language in all parts of this agreement shall in all cases be simply construed according to its fair meaning and not strictly for or against the RECIPIENT or ORGANIZATION. The headings preceding each paragraph are for convenience only and shall not in any way be construed to effect the meaning of the paragraphs themselves.

HOLD HARMLESS:

RECIPIENT agrees to indemnify, defend, and hold harmless ORGANIZATION, its directors, officers, agents, shareholders, and employees against all claims, demands, or causes of action that may arise from RECIPIENT'S employees, agents, or independent contractors improper disclosure of the information and from any intentional or negligent acts or omissions.

ENTIRE AGREEMENT; AMENDMENTS:

This Agreement contains the entire agreement between the parties with respect to the matters covered by this Agreement and supersedes all prior negotiations, agreements and employment contracts between the parties, whether oral or in writing. This agreement may not be amended, altered or modified except by written agreement signed by all parties of this agreement. No provision of this agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision shall not be construed as a waiver of any other term or provision.

AUTHORITY:

The persons signing below have the right and authority to execute this agreement for their respective entities and no further approvals are necessary to create a binding agreement.

GOVERNING LAW:

This agreement shall be governed by the privacy regulations and applicable State laws. In witness whereof, the parties have executed this Chain of Trust Agreement the day and year first written above.

Maryland Health Care Commission

VII. Notice of Privacy Practices

Practitioner and Facility Development Tips

An individual has a right under most circumstances to adequate notice of the uses and disclosures of protected health information that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protect health information. The Notice of Privacy Practices outlines how medical information about a patient may be used and disclosed and their access to this information. ***This document provides practitioners and facilities with best practice guidelines for developing an organization specific Notice of Privacy Practices.***

Best Practices - Development Guidelines:

- *Include the following statement in the header: 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.*
- *Include a description, including at least one example, of the types of uses and disclosures that the covered entity is permitted using protected health information for treatment, payment, and health care operations.*
- *Include a description of each of the other purposes for which the covered entity is permitted or required to disclose protected health information without the individual's written consent or authorization.*
- *Clearly indicate if the covered entity intends to contact the individual to provide appointment reminders or information about treatment alternatives.*
- *Outline all fund raising activities used by the organization.*
- *Include a statement of the individual's right with respect to protected health information and a description of how the individual may exercise their rights that includes:*
 - *The right to request restrictions on certain uses and disclosures of protected health information. Indicate that the organization is not required to agree to a requested restriction;*
 - *The right to receive confidential communication of protected health information by an alternative method;*
 - *The right to inspect and copy protected health information;*
 - *The right to receive an accounting of disclosures of protected health information;*
 - *The right of an individual to receive a paper copy of a notice originally received electronically upon request.*
- *Include a statement that the covered entity is required by law to maintain the privacy of protected information.*
- *Include a statement that the covered entity is bound by the terms of the notice currently in effect.*

Maryland Health Care Commission

- *Indicate organization intentions relating to making future changes in the Notice of Privacy Practices.*
- *Outline distribution procedures for the Notice of Privacy Practices.*
- *Include a statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by C.F.R. 164.508(b)(5).*

Maryland Health Care Commission

Sample Notice of Privacy Practices:

This form is provided without any warranty, expressed or implied, as to its legal effect and completeness. Use of this form is entirely at your own risk.

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.

UNDERSTANDING YOUR HEALTH RECORD/INFORMATION:

Each time you visit a hospital, physician, or other healthcare provider, a record of your visit is made. Typically, this record contains your symptoms, examination and test results, diagnoses, treatment, and a plan for future care or treatment. This information, often referred to as your health or medical record, serves as a basis for planning your care and treatment and serves as a means of communication among the many health professionals who contribute to your care. Understanding what is in your record and how your health information is used helps you to ensure its accuracy, better understand who, what, when, where, and why others may access your health information, and make more informed decisions when authorizing disclosure to others.

YOUR HEALTH INFORMATION RIGHTS:

Unless otherwise required by law your health record is the physical property of the healthcare practitioner or facility that compiled it, the information belongs to you. You have the right to request a restriction on certain uses and disclosures of your information, and request amendments to your health record. This includes the right to obtain a paper copy of the notice of information practices upon request, inspect, and obtain a copy of your health record. Obtain an accounting of disclosures of your health information, request communications of your health information by alternative means or at alternative locations, revoke your authorization to use or disclose health information except to the extent that action has already been taken.

OUR RESPONSIBILITIES:

This organization is required to maintain the privacy of your health information. In addition, provide you with a notice as to our legal duties and privacy practices with respect to information we collect and maintain about you. This organization must abide by the terms of this notice, notify you if we are unable to agree to a requested restriction, accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations. We reserve the right to change our practices and to make the new provisions effective for all protected health information we maintain. Should our information practices change, we will mail a revised notice to the address you've supplied us. If we maintain a Web site that provides information about our customer services or benefits we will post our new notice on that Web site. We will not use or disclose your health information without your authorization, except as described in this notice.

FOR MORE INFORMATION OR TO REPORT A PROBLEM:

If you have questions and would like additional information, you may contact _____ at _____. If you believe your privacy rights have been violated, you can file a complaint with the Secretary of Health and Human Services. There will be no retaliation for filing a complaint.

EXAMPLES OF DISCLOSURES FOR TREATMENT, PAYMENT, AND HEALTH OPERATIONS

We will use your health information for treatment. For example: Information obtained by a healthcare practitioner will be recorded in your record and used to determine the course of treatment

Maryland Health Care Commission

that should work best for you. By way of example, your physician will document in your record their expectations of the members of your healthcare team. Members of your healthcare team will then record the actions they took and their observations (example varies by practitioner type). We will also provide your other practitioners with copies of various reports that should assist them in treating you.

We will use your health information for payment. For example: A bill may be sent to you or a third-party payer. The information on or accompanying the bill may include information that identifies you, as well as your diagnosis, procedures, and supplies used.

We will use your health information for regular health operations. For example: Members of the medical staff, the risk or quality improvement manager, or members of the quality improvement team may use information in your health record to assess the care and outcomes in your case and others like it. This information will then be used in an effort to continually improve the quality and effectiveness of the healthcare and service we provide.

Business Associates: There may be some services provided in our organization through contracts with Business Associates. Examples include physician services in the emergency department and radiology, certain laboratory tests, and a copy service we use when making copies of your health record. When these services are contracted, we may disclose some or all of your health information to our Business Associate so that they can perform the job we've asked them to do. To protect your health information, however, we require the Business Associate to appropriately safeguard your information.

Directory (inpatient settings): Unless you notify us that you object, we will use your name, location in the facility, general condition, and religious affiliation for directory purposes. This information may be provided to members of the clergy and, except for religious affiliation, to other people who ask for you by name.

Notification: We may use or disclose information to notify or assist in notifying a family member, personal representative, or another person responsible for your care, your location, and general condition.

Communication with family: Health professionals, using their best judgment, may disclose to a family member, other relatives, close personal friends or any other person you identify, health information relevant to that person's involvement in your care or payment related to your care.

Research (inpatient): We may disclose information to researchers when an institutional review board that has reviewed the research proposal, and established protocols to ensure the privacy of your health information has approved their research.

Funeral directors: We may disclose health information to funeral directors consistent with applicable law to carry out their duties.

Organ procurement organizations: Consistent with applicable law, we may disclose health information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs for the purpose of tissue donation and transplant.

Marketing: We may contact you to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

Maryland Health Care Commission

Fund raising: We may contact you as part of a fund-raising effort.

Food and Drug Administration (FDA): As required by law, we may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.

Workers compensation: We may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to workers compensation or other similar programs established by law.

Public health: As required by law, we may disclose your health information to public health or legal authorities charged with tracking birth and deaths, as well as with preventing or controlling disease, injury, or disability.

Correctional institution: Should you be an inmate of a correctional institution, we may disclose to the institution or agents thereof health information necessary for your health and the health and safety of other individuals. An inmate does not have the right to the Notice of Privacy Practices.

Law enforcement: We may disclose health information for law enforcement purposes as required by law or in response to a valid subpoena. Federal law makes provision for your health information to be released to an appropriate health oversight agency, public health authority or attorney, provided that a work force member or business associate believes in good faith that we have engaged in unlawful conduct or have otherwise violated professional or clinical standards and are potentially endangering one or more patients, workers or the public.

Notice of Privacy Practices availability: This notice will be prominently posted in the office where registration occurs. Patients will be provided a hard copy and the notice will be maintained on our Web site (if applicable Web site exists) for downloading.

EFFECTIVE DATE: _____

Maryland Health Care Commission

VIII. Computer and Information Usage Agreement

Practitioner and Facility Development Tips

All persons who are authorized to view data both through enterprise information systems and through individual department local area networks and databases **must read and comply with a Covered Entity's security and confidentiality policy**. Under HIPAA, the use of a computer network shared by many users must incorporate policies and procedures to protect health care information. **This document provides practitioners and facilities with best practice guidelines for developing an organization specific computer and information usage agreements:**

- *Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job.*
- *Respect the ownership of proprietary software. Do not make unauthorized copies of such software for your own use, even when the software is not physically protected against copying.*
- *Inspect the capability of the systems, and limit your own use so as not to interfere unreasonably with the activity of other users.*
- *Respect the procedures established to manage the use of the system.*
- *Prevent unauthorized use of any information in files maintained, stored, or processed by Covered Entity.*
- *Do not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through work assignments.*
- *Do not operate any non-licensed software on any computer provided by the covered entity.*
- *Do not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with covered entity policy.*
- *Do not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.*
- *Do not remove any record (or copy) or report from the office where it is kept except in the performance of my duties.*
- *Report any violation of this agreement.*
- *Understand that the information accessed through all covered entity's information systems contains sensitive and confidential patient/member care, business, financial and hospital employee information that should only be disclosed to those authorized to receive it.*

Maryland Health Care Commission

- *Do not release your authentication code or device to anyone else, or allow anyone else to access or alter information under my identity.*
- *Do not utilize anyone else's authentication code or device in order to access any covered entity's system.*
- *Respect the confidentiality of any reports printed from any information system containing patient/member information and handle, store, and dispose of these reports appropriately.*
- *Do not divulge any information that identifies a patient/member.*
- *Understand that all access to the system will be monitored.*
- *Understand that my obligations under this agreement will continue after termination of my employment. I understand that my privileges hereunder are subject to periodic review, revision, and if appropriate, renewal.*

Maryland Health Care Commission

Sample Computer and Information Usage Agreement:

This form is provided without any warranty, expressed or implied, as to its legal effect and completeness. Use of this form is entirely at your own risk.

ORGANIZATION considers maintaining the security and confidentiality of protected health information (PHI) a matter of its highest priority. All those granted access to this information must agree to the standards set forth in this Computer and Information Usage Agreement. All those who cannot agree to these terms will be denied access to PHI entrusted by our patients to this organization. Each person accessing ORGANIZATION data and resources holds a position of trust relative to this information and must recognize the responsibilities entrusted in preserving the security and confidentiality of this information. The following conditions apply to all those having access to protected health information.

I will:

- Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job.
- Respect the ownership of proprietary software. For example, do not make unauthorized copies of such software for your own use, even when the software is not physically protected against copying.
- Respect the finite capability of the systems, and limit use so as not to interfere unreasonably with the activity of other users.
- Respect the procedures established to manage the use of the system.
- Prevent unauthorized use of any information in files maintained, stored, or processed by ORGANIZATION
- Not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through my work assignment.
- Not operate any non-licensed software on any computer provided by ORGANIZATION
- Not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with ORGANIZATION policy.
- Not knowingly include or cause to be included in any record or report, a false, inaccurate, or misleading entry.
- Not remove PHI from the office where it is kept except in the performance of my duties.
- Understand that the information accessed through all ORGANIZATION information systems contains sensitive and confidential patient/member care, business, financial and hospital employee information, which should only be disclosed to those, authorized to receive it.
- Not release my authentication code or device to anyone else, or allow anyone else to access or alter information under my identity.
- Not utilize anyone else's authentication code or device in order to access any ORGANIZATION system.
- Respect the confidentiality of any reports printed from any information system containing patient/member information and handle, store and dispose of these reports appropriately.
- Not divulge any information that identifies PHI.
- Understand that all access to the system will be monitored.

I understand that my access to PHI maintained by ORGANIZATION is a privilege and not a right afforded to me. By signing this agreement, I agree to protect the security of this information and maintain all PHI in a manner consistent with the requirements outlined under the privacy regulations and applicable State laws.

Signature/Date

Title