

**HIPAA ADMINISTRATIVE
SIMPLIFICATION COMPLIANCE GUIDE**

AUGUST 2001

**PREPARED FOR
AMERICAN COLLEGE OF GASTROENTEROLOGY
AMERICAN SOCIETY FOR GASTROINTESTINAL
ENDOSCOPY**

BY PATTON BOGGS LLP

DEVELOPED BY:

PATTON BOGGS LLP
2550 M STREET, NW
WASHINGTON, D.C. 20006

CONTACTS:

MARTHA KENDRICK

202-457-6520

BILL GRADISON

202-457-6184

KATHLEEN LESTER

202-457-6562

A MESSAGE FROM THE ACG PRESIDENT

Not a week goes by but that I receive another invitation to an expensive meeting that will provide me guidance about compliance for the new HIPAA regulations on patient privacy, electronic transactions, and code sets. My problem is the time to do so and the expense in attending such conferences.

It is my hope that this monograph will provide you sufficient information to permit development of your initial office plans for compliance with the regulations while preserving your resources. As you are aware, the American College of Gastroenterology has always had a goal in being of assistance to our members in their practice management activities.

This monograph was developed jointly with the American Society for Gastrointestinal Endoscopy (ASGE). Both organizations will place the guide on their Web site and jointly take responsibility for its maintenance and for keeping it abreast of changes in HIPAA regulations as only a portion of the regulations have been released at this time. When new regulations are developed or the existing rules are modified, you can find the updates by reviewing the guidelines on our Web site or through the ASGE Web site.

I am pleased to provide this guide to you. It demonstrates our continuing commitment to serving our members in their practice needs. I am also pleased that we could do so in conjunction with the ASGE.

Rowen K. Zetterman, MD, FACG
President, ACG

FOREWORD

This Guide provides a general synopsis of what you will need to consider to ensure appropriate compliance with the HIPAA Administrative Simplification regulations. The Department of Health and Human Services (HHS) promulgated these regulations pursuant to authority granted it by Congress in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Administrative Simplification provisions. This statute called for several regulations, including:

- ◆ Standards for Transaction and Code Sets;
- ◆ Standards for Privacy of Individually Identifiable Health Information;
- ◆ Security Standards;
- ◆ Electronic Signature Standards;
- ◆ National Provider Identifiers;
- ◆ National Health Plan Identifiers;
- ◆ National Employer Identifiers; and
- ◆ National Individual Identifiers.

At this time, only the regulations for electronic transactions and code sets and the privacy regulation are final. HHS has proposed the security, electronic signature, national employer identifier, and national health plan identifiers regulations. Because of the controversy surrounding a national individual identifier, it appears unlikely that the Bush Administration will disagree with the Clinton Administration decision not to promulgate this regulation.

Purpose. Through HIPAA, Congress sought to encourage the health care industry to adopt electronic transactions and more efficient systems of information management that would lead to significant savings. In addition, Congress viewed electronic information systems as necessary to gain the medical benefits associated with easy and quick access to patient information. For example, doctors can send information electronically to one another to assist with consultations or gain second opinions of colleagues in different areas of the country. Most of the HIPAA regulations address these issues. They help create a standard language for electronic transactions and assist in alleviating the burden on providers to work with the different codes adopted by different organizations. But Congress understood that electronic information systems could create the potential for great harm if information were used inappropriately or could not be verified as accurate. Thus, Congress also saw the need to create a standard guaranteeing all Americans a minimum level of privacy. In addition, Congress called on HHS to develop security regulations to ensure that the health care industry could be certain of the authenticity of the information being transmitted, as well as the identity of the professionals or entities transmitting and/or receiving the information.

Other laws. These regulations should not be your only concern when seeking to comply with HIPAA. In addition, other non-HIPAA statutes and regulations may impact overall compliance. For example, to the extent Congress or the Federal Trade Commission adopts electronic signature standards, it is possible that entities will want, or be required, to comply with these rules as well. In the area of privacy, there are also the Gramm-Leach-Bliley (GLB) regulations

that States may adopt and apply to certain insurance plans. Providers interacting with entities that come within the definition of “financial institutions” and the scope of GLB should consider the requirements these regulations place on such entities. States are also scurrying to adopt their own version of privacy regulations. If a State in which a provider operates has adopted a privacy law, the provider will need to evaluate the impact of the State law on its compliance plan. In addition, providers seeking to expand their businesses to the Internet will need to look at Federal and State efforts, as well as industry standards, to address issues such as privacy and security.

The HIPAA regulations focus on the transfer of information between specific parties. Therefore, this Guide is organized to provide you with an understanding of how the regulations affect the relationships that are most important to your practice. These relationships include: the provider-patient, provider-provider, provider-health plan, provider-health care clearinghouse, and provider-business associate relationships. The Guide also provides a brief summary of important administrative requirements of the privacy regulation. Additionally, the privacy regulation contains provisions that may alter your compliance requirements. These provisions are explained in the “Special Concerns” section.

Disclaimer. This Guide provides you with general compliance guidance. It cannot replace a specific compliance plan that takes into account the special needs and relationships unique to each practice. Therefore, we encourage you to use this Guide as a starting point for developing your compliance strategy.

TABLE OF CONTENTS

TAB		PAGE
A	EXECUTIVE SUMMARY	6
B	GENERAL INFORMATION	7
	ARE YOU A COVERED ENTITY?	7
	ARE YOU A BUSINESS ASSOCIATE?	7
	HOW TO COMPLY WITH THE HIPAA REGULATIONS	8
	FIRST STEPS FOR COMPLIANCE	8
	MODIFICATIONS TO THE PRIVACY REGULATION	11
	QUESTIONS TO ANSWER IN YOUR POLICIES AND PROCEDURES	12
C	COMPLIANCE CHECKLIST	13
D	THE PROVIDER-PATIENT RELATIONSHIP	16
	DOCUMENTATION	16
	CONSENTS	16
	AUTHORIZATIONS	18
	NOTICES	21
	PROCEDURES	25
	ACCESS RIGHTS	25
	AMENDMENT RIGHTS	26
	ACCOUNTING OF DISCLOSURES	28
	RIGHT TO REQUEST A RESTRICTION	29
	RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS	29
E	THE PROVIDER-PROVIDER RELATIONSHIP	30
	DISCLOSURES FOR TREATMENT PURPOSES	30
	DISCLOSURES FOR HEALTH CARE OPERATIONS	31
F	THE PROVIDER-HEALTH PLAN RELATIONSHIP	32
	DISCLOSURES TO HEALTH PLANS	32
	PAYMENTS	32
	HEALTH CARE OPERATIONS	32
	MINIMUM NECESSARY	33
	BUSINESS ASSOCIATE CONTRACTS AND HEALTH PLANS	33
G	THE PROVIDER-CLEARINGHOUSE RELATIONSHIP	34
H	THE PROVIDER-BUSINESS ASSOCIATE RELATIONSHIP	35
	IDENTIFYING BUSINESS ASSOCIATES	35
	THE BUSINESS ASSOCIATE CONTRACT	35
	OTHER RESPONSIBILITIES OF BUSINESS ASSOCIATES	36

TAB		PAGE
I	ADMINISTRATIVE REQUIREMENTS	37
J	SPECIAL PRIVACY CONCERNS	38
	DE-IDENTIFICATION	38
	PERSONAL REPRESENTATIVES	38
	AFFILIATED ENTITIES	38
	ORGANIZED HEALTH CARE ARRANGEMENTS (OHCAs)	38
	HYBRID ENTITIES	39
K	THE INTERNET	40
L	CONCLUSION	41
M	APPENDIX OF FORMS	42
N	APPENDIX OF DEFINITIONS	46
O	ENDNOTES	49

EXECUTIVE SUMMARY

Only certain entities must comply with the HIPAA regulations. Covered entities and business associates of covered entities are required to comply.

- 1) Are you a covered entity? The regulation applies only to certain health care providers, all health plans, and all health care clearinghouses. (See “General Information” for a description of covered health care providers).
 - a) If you are a covered entity, do you understand how information that identifies specific individuals is collected, maintained, and distributed?
 - b) If you are a covered entity, have you complied with the use and disclosure requirements of the regulation by the required compliance date (April 14, 2003)?
 - c) Have you obtained the appropriate documentation from your patients (consents and authorizations)?
 - d) Have you provided your patients with the appropriate documentation (notices)?
 - e) Do you have the required contracts with your business associates?
 - f) If you are a covered entity, have you complied with the individual rights provisions of the regulation (*e.g.*, the right to access and amend their information in certain circumstances)?
 - g) If you are a covered entity, have you complied with the administrative requirements of the regulation?
- 2) Are you a business associate of a covered entity?
 - a) If you are a business associate, have you signed a business associate contract with the covered entities with which you work?
 - b) If you are a business associate, are you using and disclosing information consent with your business associate contract?

In the pages that follow, this Guide provides you with more detail about these requirements. It contains narrative descriptions of the specific regulatory requirements, as well as model forms, important questions, and a final “Checklist” to assist you with your compliance efforts. Because the regulations impact your relationships with others, the Guide provides you with specific information about how the regulations will impact your relationships with patients, other providers, health plans, clearinghouses, and agents who use information on your behalf or in other ways that assist you.

GENERAL INFORMATION

This section describes how you can begin complying with the regulation.

I. Does the regulation apply to you?

A. Are You a Covered Entity?

The HIPAA regulations do not apply to all people or entities within the health care industry. Only providers engaged in electronic HIPAA transactions, health plans, and health care clearinghouses are subject to the regulation. Electronic HIPAA transactions are:

- ◆ Health Care Claims or Equivalent Encounter Information;
- ◆ Health Care Payments and Remittance Advice
- ◆ Coordination of Benefits
- ◆ Health Care Claim Status;
- ◆ Enrollment and Disenrollment in a Health Plan;
- ◆ Eligibility for a Health Plan;
- ◆ Health Plan Premium Payments;
- ◆ Referral Certification and Authorization;
- ◆ First Report of Injury; and
- ◆ Health Claims Attachments.¹

If you do not engage in one of these transactions² electronically, you do not have to comply with these regulations.

B. Are you a Business Associate?

As a general rule, business associates are entities that act on behalf of a covered entity or perform one of the services specified in the regulation for a covered entity. Covered entities may also be business associates. As a business associate, you should understand the requirements placed upon covered entities.

Business associates of covered entities will need to consider compliance strategies in light of the contracts they execute with covered entities. Before they obtain individually identifiable health information from a covered entity, a business associate will need to enter into a business associate contract with the covered entity that meets the requirements of the regulation. Both business associates and covered entities (which may also be business associates in some cases) will need to consider how these documents should be drafted. See “The Provider-Business Associate Relationship”.

Determining whether you are a covered provider or business associate is a fact specific question. Unless you want to implement the regulation regardless of the Federal mandate, you should discuss with counsel whether you come within the scope of the regulation.

II. How to Comply with the HIPAA Regulations

If a covered provider, you will need to develop a compliance strategy and program. Although the specifics of compliance programs may vary, any successful compliance program should contain the following steps:

- ◆ Conduct a preliminary survey of current practices;
- ◆ Develop and distribute written standards of conduct/policies and procedures that demonstrate compliance;
- ◆ Designate a privacy official and/or committee and ensure that they have the appropriate authority to oversee and monitor compliance and enforce the policies and procedures internally;
- ◆ Develop and implement training programs for all affected employees;
- ◆ Ensure that all employees hired are committed to complying with the law;
- ◆ Establish a complaint process and mechanisms to investigate complaints from employees and contractors as well as customers; and
- ◆ Establish a system to monitor compliance, conduct audits, and respond appropriately to misconduct.

III. First Steps for Compliance

When beginning to develop a compliance strategy, you should:

- ◆ Conduct a preliminary survey;
- ◆ Develop and implement policies and procedures;
- ◆ Designate and empower a privacy official or privacy committee;
- ◆ Train your employees;
- ◆ Implement a complaint process; and
- ◆ Set a realistic time frame for developing your program to ensure compliance by the required date.

A. *Preliminary Survey*

The first step in complying with any law is to understand how it impacts current operations. For the HIPAA regulations, this first step is extremely important. It means you must understand what information is being used and/or disclosed, how information is used and/or disclosed, to whom the information is being used and/or disclosed, and why the information is being used and/or disclosed. It also means understanding your existing practices and procedures for information collection, maintenance, use, and disclosure. The following questions are an example of how to conduct this type of survey:

- ◆ What information does your organization use and/or disclose?
- ◆ Who inside and outside of the organization handles this information?

- ◆ What current processes, policies, or practices exist for protecting this information? And, are they written or merely understood?
- ◆ How are electronic transactions conducted, if at all?
- ◆ What code sets are used if electronic transactions are conducted?
- ◆ What agreements, if any, are there with other entities to which information is disclosed?

This list is not exhaustive, but should provide you with an idea of the type of investigation necessary. Knowing your existing practices and policies will help to avoid duplicating efforts and enable you to build a program tailored to your needs rather than adopt an entirely new and more costly program.

B. Policies and Procedures.

The privacy regulation requires covered entities to implement policies and procedures “that are designed to comply with the standards, implementation specifications, or other requirements” of the regulation.³ See “Questions You Should Answer in Your Policies and Procedures” for an explanation of what your policies and procedures should include. It is likely that the security regulation will contain a similar requirement. Because the transaction, code sets, and identifiers regulations are more technical than policy oriented in nature, your policies and procedures will need to refer to them only generally.

Your policies and procedures also contain how you will implement the minimum necessary standard. The regulation requires that you use and/or disclose only the minimum amount of information necessary for the purpose of the use or disclosure.⁴ Your minimum necessary policies must:

- ◆ Identify those persons or classes of persons in the workforce who need access to PHI to carry out their duties;
- ◆ Identify (for each person/class) the categories of PHI to which access is needed and any conditions appropriate for such access;
- ◆ For routine and recurring disclosures, describe the amount of PHI reasonably necessary to achieve the purpose of the disclosure;
- ◆ For non-routine and non-recurring disclosures, describe the criteria designed to limit the PHI disclosed to the minimum amount necessary, the process for reviewing special requests for disclosures using this criteria, and when you are permitted to rely on a request as the minimum amount necessary (*e.g.*, requests may by public officials);
- ◆ For routine and recurring requests of PHI, describe the amount of PHI reasonably necessary to achieve the purpose of the request; and
- ◆ For non-routine and non-recurring requests, describing the process for reviewing the request on an individual basis.

In most cases, you will not be required to decide each case on an individual basis, but may rely upon your minimum necessary policies and procedures.

The privacy regulation does not dictate the specifics, but states that they “must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information [PHI] undertaken by the covered entity.”⁵ As a general matter, all individually identifiable health information in any form (oral, paper, or electronic) is PHI.⁶ Thus, your policies and procedures can be tailored to your needs.

C. Privacy Official/Committee

The privacy regulation requires covered providers to designate a privacy official.⁷ This person will need to oversee the development and implementation of the policies and procedures. This person or a designated office must receive complaints and provide further information about the notice provided to patients. The privacy official does not have to be an individual who deals only with privacy. In a small office, the privacy official may be a nurse or office manager. In a larger practice or hospital setting, the privacy official may have not other responsibilities.

D. Employees

The privacy regulation requires covered providers to train members of its workforce on their privacy policies and procedures “as necessary and appropriate for the members of the workforce to carry out their functions.”⁸ For example, the person who processes claims will need to understand and use the code sets (or what is required by the clearinghouse that translates the claims into the standard code) and identifiers. A nurse who assists a doctor with examining and evaluating patients and has access to all PHI when serving in this capacity will need to understand your policies and procedures in a more complete fashion than an office assistant who only answers the phone. A building janitor employed by the landlord and who never has access to PHI will not need to be trained. If the policies and procedures change, you will need to ensure your employees understand their most recent iteration.

You will also need to monitor your employees to ensure compliance. If they do not comply with your privacy policies and procedures (unless they are acting as a whistleblower or are a victim of a crime,⁹ attempting to exercise their individual privacy rights, or filing or assisting with a complaint¹⁰), the privacy regulation requires covered providers to apply appropriate sanctions against them and document any actions taken.¹¹

E. Complaint Process

As with most of the administrative requirements, the complaint process applies at this juncture only to the privacy regulation and may apply to the security regulation once it is finalized. You must designate an individual or office to receive and oversee the complaint process.¹² You must develop “a process for individuals to make complaints concerning the covered entity’s policies and procedures . . . or its compliance with such policies and procedures.”¹³ The regulations do not require a specific process, but do mandate that all complaints and how they are resolved (if at all) be documented.¹⁴

F. Time Frame

Congress mandated that all covered providers comply with the regulation within two years of the date of the final regulation. At this time, the compliance date for the transaction and code sets regulations is October 16, 2002; for the privacy regulation, the compliance date is April 14, 2003. You should understand that all health care clearinghouses and health plans (except for statutorily defined small health plans) must also be in compliance by these dates as well.

The privacy regulation contains transition provisions¹⁵ that permit covered providers (and other covered entities) to continue to rely upon consents and authorizations obtained before the compliance date, even if these documents do not meet the requirements of the regulation. The documents must be about the consent or authorization to use or disclose information, but otherwise, the transitional provisions are extremely generous. Therefore, it is advisable that you consult with counsel to determine if documents you already have (or may wish to use during the transition period) come within these transitional provisions. If they do, you will need to be concerned only with obtaining consents and authorizations for future patients.

IV. Modifications to the Privacy Regulation

On Friday, July 6, 2001, HHS issued the first set of guidance regarding the privacy regulation.¹⁶ This Guide incorporates this guidance, which addressed several important areas, including consents, the minimum necessary standard, and oral communications. However, it also stated that HHS plans to propose specific changes to the privacy regulation. The guidance also specifically stated that HHS will propose changes to:

- ◆ Permit a pharmacist to fill prescriptions that a doctor phones-in when the pharmacist does not have a patient's consent;
- ◆ Permit direct treatment providers receiving a first-time patient referral to use protected health information (PHI) to schedule appointments, surgery, or other procedures before obtaining a patient's consent;
- ◆ Increase covered entities' confidence that they may engage in all types of communication necessary to provide appropriate patient care, including oral communications with family members, treatment discussions with staff involved in coordinating patient care, and using patient names to locate individuals in waiting areas;
- ◆ Increase covered entities' confidence that certain common practices, such as sign-in sheets, X-ray light boards, and bedside medical charts, are not prohibited by the minimum necessary standard; and
- ◆ Ensure that parents have "appropriate access" to protected health information about their children.

Other than the potential changes in the consent requirements, the modifications are likely to alter how providers implement the regulation. Even so, you will need to stay alert to changes as HHS publishes them.

QUESTIONS TO ANSWER IN YOUR POLICIES AND PROCEDURES

- ◆ How you will obtain consents from patients;
- ◆ How you will use and/or disclose the information you obtain via a consent;
- ◆ How you will obtain authorizations from patients;
- ◆ How you will use and/or disclose the information you obtain via an authorization;
- ◆ The revocation process for consents and authorizations;
- ◆ Your general minimum necessary policies;
- ◆ How you will evaluate requests for restrictions on uses and disclosures of PHI and, if you agree to such a restriction, how you will implement the agreement;
- ◆ How and when you will de-identify information, maintain it as de-identified, or re-identify it, if you choose to do so;
- ◆ How you will work with business associates;
- ◆ How you will implement the personal representative requirements;
- ◆ How you will evaluate and implement requests for confidential communications of PHI;
- ◆ How you will deal with disclosures by whistleblowers and workforce member crime victims;
- ◆ If you are a hybrid entity (or part of one), how and when you will disclose PHI to other components of the hybrid entity;
- ◆ If you act as an affiliated entity, how you will ensure that your affiliates comply with the regulation;
- ◆ How you exchange PHI with business associates;
- ◆ If you are a covered entity with multiple covered functions, how you will ensure that you comply with the provisions applicable to each function when appropriate;
- ◆ How you will resolve conflicts between consents and authorizations in accordance with the regulation;
- ◆ How and when you will use and/or disclose PHI pursuant to one of the regulatory exceptions;
- ◆ How and when you will use and/or disclose PHI for marketing and/or fundraising purposes pursuant to the exceptions in the regulation;
- ◆ How you will verify the identity and authority of a person/entity to whom you make a disclosure;
- ◆ How and when you will deliver to patients, change, notify patients of changes, and maintain the required notice of your privacy policies and practices;
- ◆ How you will comply with the right of individuals to access their PHI in designated record sets, including the process for denying such requests;
- ◆ How you will comply with the right of individuals to amend their PHI in designated record sets, including the process for denying such requests;
- ◆ How you will provide individuals with an accounting of the disclosures of their PHI;
- ◆ Who in the organization is the privacy official who implements these policies and procedures, receives complaints, and provides further information about the notice;
- ◆ How you will train employees to ensure they comply with these policies and procedures and sanction them if they do not;
- ◆ Your administrative, technical, and physical safeguards to protect the privacy of PHI: this section will need to be updated with the Security Standard requirements once those regulations are final;
- ◆ How you will handle complaints from individuals;
- ◆ How you will mitigate, to the extent practicable, the harmful effect(s) known to you that occur because of an inappropriate use or disclosure of PHI;
- ◆ Your practices regarding refraining from intimidating or retaliatory acts against individuals attempting to exercise their rights under this regulation or making a complaint against you;
- ◆ Your commitment not to require individuals to waive their rights under this regulation as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits;
- ◆ The process for changing your policies and procedures; and
- ◆ The documentation you maintain and how it is maintained.

COMPLIANCE CHECKLIST

Complying with the HIPAA regulations requires a thorough understanding of your practices and your business relationships. Therefore, it is impossible to provide a complete checklist that encompasses all of the possible ways to comply or potential issues you may face while trying to comply. Even so, you may find the following questions helpful as you are developing a program to meet your specific needs. One note of caution is in order: as more of the HIPAA regulations become final, it will be important to update this list and Guide. For example, this list does not contain questions addressing the security regulation. Although this regulation has been proposed, it is likely that the Final Rule will look significantly different than those proposed.

The HIPAA Checklist

- Are you a covered entity (are you engaged in any electronic HIPAA transaction)?
- Have you identified your business associates?
- Have you identified when you act as a business associate, if ever?
- Have you incorporated (or hired someone to assist you to incorporate) the standard transaction code sets into your electronic HIPAA transactions?
- Have you obtained a provider identifier (once available)?
- Do you have the appropriate identifiers for the employers and health plans with which you deal (once available)?
- Have you identified how, to whom, and from whom individually identifiable health information flows in your practice?
- Have you determined if one of the special organizational provisions (such as OHCA's, hybrid entities, or affiliated entities) applies to your practice and whether you will take advantage of such a relationship?
- Have you evaluated when you can use or disclose de-identified information so that the requirements of the privacy regulation do not apply?
- Have you entered into the appropriate agreements with your business associates?
- Have you determined when another covered entity may require you to enter into a business associate agreement?
- Have you developed the necessary documents to provide to patients: consents, authorizations, and notices?
- Have you determined if any of your existing consents or authorizations come within the transitional provisions and, therefore, are grandfathered into the privacy regulation?
- Have you determined how you will obtain consents and authorizations from your patients to use or disclose their information?
- Have you determined how you will provide notices?
- Are you familiar with the exceptions that permit the use and/or disclosure of protected health information (PHI) without a consent or authorization?
- Have you established your practices for providing individuals with their rights to: access and amend their information in designated record sets (of you and your business associates); obtain an accounting of disclosures of their information; request restrictions on uses and disclosures of their information; and receive confidential communications of their information?

- Have you developed your policies and procedures for using and/or disclosing the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure?
- Have you designated a privacy official?
- Have you trained your workforce about your privacy practices?
- Have you implemented the appropriate administrative, technical, and physical safeguards to protect PHI?
- Have you established a complaint process for individuals to register their complaints with you?
- Have you established a system that ensures that individuals who register complaints (including members of your workforce) are not retaliated against?
- Have you developed a disciplinary process for sanctioning members of your workforce who violate your privacy policies?
- Have you developed and implemented policies and procedures designed to comply with the privacy regulation?
- Have you developed and implemented a system to maintain the required documentation for six years?
- Have you brought your website into compliance as well?
- Have you reviewed other Federal, State, and local laws, as well as professional standards, to ensure you comply with all relevant privacy and security laws?

THE PROVIDER-PATIENT RELATIONSHIP

The most important relationship affected by the HIPAA regulations is that between providers and patients. It is highly unlikely that the transaction, code sets, or identifiers regulations will directly impact this relationship. Until the security regulation is final, it is unclear the extent to which that regulation may impact the relationship. However, the final privacy regulation does discuss this relationship in great detail. For some providers, the regulation only codifies what is already their standard practice and, perhaps, adds a few new twists on these practices. For others, the regulation will require a new approach to patients. Any provider would be well served to determine his/her current privacy practices for patients before adopting a specific program. There is no one-size-fits-all solution. Most providers will be able to reduce the costs associated with the regulation by integrating their current practices that already meet the Federal regulation. Be wary of anyone claiming you must revamp your entire practice.

The privacy regulation requirements can be divided into two parts – (1) documentation you must produce (consents, authorizations, and notices) and (2) procedures you must develop (individual rights).

I. Documentation

A. Consents

With some exceptions, the privacy regulation requires you to obtain a consent from each patient before disclosing PHI for the purposes of treatment,¹⁷ payment,¹⁸ and/or health care operations.¹⁹ You need to obtain consents if you wish to use or disclose PHI for one, any, or all of these purposes.²⁰ A consent obtained by one provider cannot be relied upon by another covered entity unless it is a joint consent between providers in an organized health care arrangement (OHCA) or the other covered entity is a business associate.²¹ See “Special Concerns” for an explanation of OHCA’s.

You do not need to obtain a consent:

- ◆ If you have an indirect treatment relationship²² with the individual (*e.g.*, a medical laboratory) or
- ◆ If you obtain the PHI during the course of treating an inmate.²³

You do not have to obtain prior consent:

- ◆ In emergency treatment situations (provided that you attempt to obtain consent as soon as reasonable practicable after the delivery of treatment);
- ◆ If you are required by law to treat the individual and you are unable to obtain consent; or
- ◆ If you attempt to obtain consent, but are unable to because of a substantial communications barrier and you determine, in the exercise of professional judgment, that consent can be inferred from the circumstances.

You must document why you were unable to obtain the consent in these cases.²⁴

Most providers who already obtain consents from patients for treatment or to transfer information to health plans for payments will not need to change drastically their current practices. First, consents must contain the information specified in the regulation; otherwise, they are considered defective.²⁵ Below is an example of a proper consent form.

Consent

You agree to permit your protected health information to be used and disclosed for purposes of treatment, payment, and health care operations. For more details about these uses and disclosures, please see our Privacy Notice.

We reserve the right to change our privacy policies described in the Privacy Notice. You may call us to receive an updated Notice.

You have the right to request that we restrict how your protected health information is used or disclosed to carry out treatment, payment, or health care operations. We are not required to agree with this request, but if we do, we are bound by it.

You have the right to revoke your consent in writing. A revocation, however, will not apply to the extent we have taken action in reliance upon the use or disclosure of your information.

Signature

Date

You should obtain the consent during your first visit with an individual. A new consent does not need to be obtained at each visit. The consent may be part of the paperwork that individuals sign when they first come to an office. Alternatively, the consent can be electronic, so long as an appropriate signature is attached. Consenting to uses and disclosures of PHI for purposes of treatment, payment, and/or health care operations may be conditioned on the provision of treatment.²⁶ It may not be combined in a single document with the notice,²⁷ but may be combined with other types of legal permission, including an informed consent for treatment or a research authorization, so long as the consent is visually and organizationally separate from the other permission and is separately signed and dated.²⁸ Consents are revocable, but remain effective to the extent a covered provider has relied upon it.²⁹ Consents should be maintained for at least six years from the date the documents were last in effect.³⁰

B. Authorizations

With some exceptions, the privacy regulation requires you to obtain an authorization from each patient before you may use or disclose PHI for all purposes other than treatment, payment, or health care operations.³¹ Authorizations are also required for the use and disclosure of psychotherapy notes.³²

Authorization documents will need to be more detailed than consents. Some elements, however, remain consistent regardless of the purpose. To the extent you routinely use or disclose PHI for a purpose other than treatment, payment, or health care operations, you may be able to develop a standard authorization form that can be signed by your patients. In less common circumstances, you may need to develop special documents. Of course, if you do *not* wish to use or disclose PHI for purposes other than those of treatment, payment, or health care operations, you will *not* need to develop authorization documents at all.

The regulation outlines the requirements for authorizations, which fall into two categories: authorizations requested by a covered entity for its own uses and disclosures³³ and authorizations requested by a covered entity for disclosures by others.³⁴ Both types of authorizations must contain the core elements and meet the core requirements, which include, among other things, a description of the information to be used or disclosed, to whom the covered entity may disclose the information, who is authorized to request a use or disclosure and an expiration date.³⁵ In addition, each type of authorization must contain additional elements outlined in detail in the regulation.³⁶

All authorizations must include the following provisions:

- ◆ A description of the information to be used or disclosed;
- ◆ The name or other specific identification of the person(s) or class of persons authorized to make the requested use or disclosure;
- ◆ The name or other specific identification of person(s) or class of persons to whom you may make the requested use or disclosure;
- ◆ An expiration date or expiration event that relates to the individual or purpose of the use or disclosure;
- ◆ A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by the Federal privacy regulation; and
- ◆ The signature of the individual and date (and, if a personal representative is signing, the authority to act for the individual).³⁷

Authorizations that are requested by you for your own uses and disclosures must contain additional elements.³⁸ Authorizations you request for disclosures by others must contain special provisions as well.³⁹ You should consult with counsel to determine when these additional provisions are necessary.

Below is a sample authorization containing the core elements.

<h2 style="color: blue;">Authorization</h2>	
You agree to the use and/or disclosure of the following information:	
<hr/> <hr/> <hr/>	
A request for the use or disclosure of this information may be made by:	
<hr/> <hr/> <hr/>	
This information may be used or disclosed to:	
<hr/> <hr/> <hr/>	
This authorization expires on: _____	
Information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by the Federal privacy regulation.	
_____ Signature	_____ Date
[You may need to add other provisions if you are seeking an authorization to use or disclose the information yourself or if you are obtaining the authorization on behalf of another covered entity]	

You should obtain an authorization before you need to use or disclose the PHI for a particular purpose. Because authorizations expire, it is important to ensure that the authority is current. Like consents, they may be obtained electronically, so long as an appropriate signature is attached. Authorizations for purposes other than treatment, payment, and/or health care operations may not be conditioned on the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits, unless an exception applies.⁴⁰ Of importance to providers is the exception that permits an authorization to be conditioned on the provision of health care that is solely for the purpose of creating it for disclosure to a third party.⁴¹

As a general rule, authorizations may not be combined with any other document. There are three exceptions to this rule. First, two authorizations may be combined so long as one of the

authorizations is not for psychotherapy notes (unless both of the documents are for disclosures of psychotherapy notes) or one of the authorizations has not been conditioned as permitted by the regulation.⁴² Second, an authorization for research that includes treatment may be combined with a consent.⁴³ Finally, an authorization for a use or disclosure of psychotherapy notes may be combined with another such authorization.⁴⁴

Authorizations are revocable and must contain an expiration date or event. They should be maintained at least six years under the regulation,⁴⁵ but it would be advisable to retain them as long as they are valid (*i.e.*, have not been revoked or have not expired) plus an additional six years after they have become inactive.

1. Conflicts between Consents and Authorizations

It is possible that an individual will execute a consent and an authorization that are inconsistent with one another. For example, an individual may consent to the use and disclosure of his/her PHI for purposes of treatment, payment, and health care operations, but then authorize the use of his/her PHI for the health care operations conducted only by a specific provider. The regulation requires the covered provider to comply with the more restrictive of the two documents.⁴⁶ Alternatively, you may seek to obtain a new consent or authorization that is consistent with the patient's wishes.⁴⁷ Because of the unique nature of these occurrences, it is advisable that providers develop a process to deal with such situations on a case-by-case basis.

2. Regulatory Exceptions to Consents and Authorizations

Neither consents nor authorizations are required in certain specified instances. Thus, so long as the special requirements of the provisions of the regulation are met, covered providers may use or disclose PHI without a consent or authorization in the following circumstances:

- ◆ Uses and disclosures for facility directories, provided that an individual has the opportunity to object and does not;⁴⁸
- ◆ Uses and disclosures for involvement in the individual's care and for notification purposes, provided that an individual has the opportunity to object and does not;⁴⁹
- ◆ Uses and disclosures required by law;⁵⁰
- ◆ Uses and disclosures for public health activities;⁵¹
- ◆ Uses and disclosures about victims of abuse, neglect, or domestic violence;⁵²
- ◆ Uses and disclosures for health oversight activities;⁵³
- ◆ Uses and disclosures for judicial and administrative proceedings;⁵⁴
- ◆ Uses and disclosures for law enforcement purposes;⁵⁵

- ◆ Uses and disclosures about decedents;⁵⁶
- ◆ Uses and disclosures for cadaveric organ, eye, or tissue donation purposes;⁵⁷
- ◆ Uses and disclosures for research purposes, so long as an Institutional Review Board (IRB) has approved the use and/or disclosure of the PHI;⁵⁸
- ◆ Uses and disclosures to avert serious threat to health or safety;⁵⁹
- ◆ Uses and disclosures for specialized government functions: military and veterans activities, national security and intelligence activities, protective services for the President and others, medical suitability determinations for the Department of State, correctional institutions and other law enforcement custodial situations, and covered entities that are government programs providing public benefits;⁶⁰ and
- ◆ Disclosures for workers' compensation.⁶¹

Each of these regulatory exceptions mandates that certain requirements are met for the exception to apply. For example, to use or disclose PHI for research purposes without an authorization, you (or the person conducting the research) must obtain IRB approval for the use or disclosure, as described in the regulation. Therefore, when seeking to develop a compliance plan, it is important to understand when these regulatory exceptions may be applied and note what you must do to meet the additional requirements.

There are also some small exceptions for uses and disclosures of PHI for purposes of marketing, fundraising, and underwriting. For covered providers, it is important to realize that, without first obtaining an authorization, you may make a “marketing” communication to an individual during a face-to-face encounter, that concerns products or services of nominal value, or that concerns the health-related products or services of the covered entity or a third party that meets requirements outlined in the regulation.⁶² This exception means that providers can discuss the pros and cons of different prescription drugs and treatments or send newsletters or similar communications to patients. If you are engaged in marketing activities, you should consult with counsel to consider these provisions based on the particular facts relevant to your practice.

C. Notices

You must also provide your patients with notice of your privacy practices, including the uses and disclosures of PHI that may be made by you, the individual's rights with regard to his/her PHI, and your legal duties with respect to PHI.⁶³ Notices must be provided in a specific manner. Health care providers with direct treatment relationships (*i.e.*, providers who communicate with patients directly and not through other providers) must initially deliver the notice no later than the first service delivery after April 14, 2003.⁶⁴ You must post the notice in a “clear and conspicuous prominent location where it is reasonable to expect individuals seeking service . . . to be able to read the notice.”⁶⁵ The notice must also be available at the delivery site for individuals to request and take with them.⁶⁶ When you revise the notice, you must make it available to patients on request on or after the effective date of the change.⁶⁷

Notices may also be delivered electronically. Covered providers with websites must prominently post the notice on the site and make it available electronically through the site.⁶⁸ Providers may also email notices to patients, if the individual agrees to electronic notice and has not revoked the agreement. A paper copy must be available if electronic notice fails.⁶⁹

Covered providers that participate in an OHCA may provide joint notices to their patients, so long as the special requirements for joint notices are met.⁷⁰ See “Special Concerns” for an explanation of OHCA’s.

Notices are highly fact specific. They must contain the following elements:

- ◆ A 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.”
- ◆ A description of the uses and disclosures you are permitted to make for treatment, payment, and health care operations;⁷¹
- ◆ A description of the uses and disclosures you are permitted or required to make for other purposes without the individual’s consent or authorization;⁷²
- ◆ A statement that you will make other uses and disclosures only with the individual’s authorization and that this authorization may be revoked;
- ◆ A statement that you may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual, if you intend to engage in such activities;
- ◆ A statement that you may contact the individual to raise funds for the covered entity, if you intend to engage in such activities;
- ◆ A statement of the individual’s rights with respect to his/her PHI and how the individual may exercise them;
- ◆ A statement that you are required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI;
- ◆ A statement that you are required to abide by the terms of the notice most currently in effect;
- ◆ A statement that you reserve the right to change the terms of its notice and to make the new notice provisions effective for all PHI that it maintains and describe how it will provide individuals with a revised notice;
- ◆ A statement that individuals may complain to you or the Secretary of HHS if they believe their privacy rights have been violated, a brief description of how the individual may file a complaint with you, and a statement that the individual will not be retaliated against for filing a complaint;
- ◆ The name or title and telephone number of a person or office to contact; and
- ◆ The date on which the notice is first in effect.⁷³

Notices may contain additional optional provisions, such as elections to use and disclose PHI in a more limited manner than required by the regulation. As with consents and authorizations, notices must be retained for six years.⁷⁴ A sample notice is provided on the following page.

Notice: Effective _____

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.

We may use and disclose your protected health information for purposes of treatment, payment, and health care operations, as permitted by Federal law. **[provide a description of these uses and disclosures].**

We may use and disclose your protected health information for purposes other than for treatment, payment, or health care operations without your consent or authorization, as permitted or required by the Federal law. **[provide a description of these uses and disclosures].**

We will make other uses and disclosures only with your authorization; this authorization may be revoked.

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 **[necessary only if you (the provider) intend to engage in such activities]**

We may contact you to raise funds for our organization **[necessary only if you (the provider) intend to engage in such activities]**

You have the right to **access and amend** your protected health information that is used to make decisions about individuals. You have the right to receive an **accounting** of disclosures of your protected health information. You have the right to **request a restriction** on certain uses and disclosures of your protected health information. We are not required to grant your request. You have the right to receive **confidential communications** of your protected health information. You have the right to **obtain a paper copy of this notice** upon request. You may exercise these rights as follows:

We are required by law to maintain the privacy of protected health information and to provide you with notice of our legal duties and privacy practices with respect to protected health information.

We are required to abide by the terms of the most current notice in effect.

We reserve the right to change the terms of our notice and to make the new notice provisions effective for all protected health information that we maintain. We will provide you with a revised notice by _____ **[necessary only if you (the provider) intend to change a privacy practice that is listed in the notice]**

If you believe your privacy rights have been violated, you may complain to us or the Secretary of HHS. You may file a complaint in the following way: _____

We will not retaliate against you for filing a complaint.

For more information about this notice, contact: _____

[You may wish to include additional provisions]

II. Procedures

In addition to the required documentation, the privacy regulation mandates certain practices. These practices arise from the individual rights created by the regulation. These rights include (A) the right to access PHI in designated record sets; (B) the right to amend PHI in designated record sets; (C) the right to obtain an accounting of disclosures of PHI; (D) the right to request a restriction on the uses and disclosures of PHI; and (E) the right to request the confidential communication of PHI.

Designated Record Sets. An important distinction is drawn in the individual rights section. The access and amendment rights apply only to information in designated record sets. A term of art, designated record sets are defined as a group of records maintained by a covered entity that are used, in whole or in part, to make decisions about individuals. This includes, but is not limited to, medical, billing, enrollment, payment, claims adjudication, and case or medical management system records.⁷⁵ Thus, if you hold information that is not in a designated record set (meaning it is not used to make decisions about individuals – any individual, not just the individual who is the subject of the information), you do not have to provide the access or amendment rights.

A. Access Rights.

You must give individuals the opportunity to inspect and copy their PHI for as long as the information is maintained in designated record sets.⁷⁶ This right does not apply to psychotherapy notes, information compiled in reasonable anticipation of certain legal proceedings and actions, and certain information subject to the Clinical Laboratory Improvement Amendments of 1988.⁷⁷

You may deny access without an opportunity to review if:

- ◆ The information is specifically excepted from the right (as listed above);
- ◆ You are a correctional institution or acting under the direction of such institution and access would harm the individual, other inmates, or the personnel at the institution;
- ◆ The information is part of ongoing research and access would jeopardize the research, so long as certain conditions are met;
- ◆ The information is subject to the Privacy Act of 1974 and denial meets the requirements of that Act; or
- ◆ You obtained the information from someone other than the individual under a promise of confidentiality and access would likely reveal the source of the information.⁷⁸

You may also deny access on other grounds, so long as you provide an opportunity for another licensed health care provider of your choice to review the decision. These grounds are:

- ◆ You determine that, in your professional judgment, access is reasonably likely to endanger the life or physical safety of the individual or another person;

- ◆ The PHI refers to another individual (who is not another health care provider) and, in your professional judgment, access is reasonably likely to cause substantial harm to the individual or another person; or
- ◆ The request is made by the individual's personal representative and you determine, in your professional judgment, that access by the personal representative is likely to cause substantial harm to the individual or another person.⁷⁹

If you deny access on a non-reviewable ground, nothing more is required. If, however, denial is based on a reviewable ground, you must select another licensed health care professional to review the denial and abide by the result.⁸⁰ If the denial is upheld, you, to the extent possible, must provide access to other PHI after excluding the information that creates the valid ground(s) for denial.⁸¹ You must also provide a timely, written denial in plain language that describes the basis for the denial, the right to review and how to exercise this right (if applicable), the complaint procedures (including how to contact the Office for Civil Rights at HHS and the name and contact information of your privacy officer).⁸² When applicable, you should note who maintains the information if you do not maintain it, but know where it is maintained.⁸³

If you agree to provide access, it must be done in a timely manner. As a general rule, you must provide access no later than 30 days after the receipt of the request.⁸⁴ The access provided must meet the following requirements:

- ◆ If identical information is maintained in distinct designated record sets or at more than one location, only one copy of the information must be produced;⁸⁵
- ◆ Access must be provided in the form or format requested by the individual, if readily producible in such form;⁸⁶
- ◆ Access may be provided in summary or by explanation so long as the individual agrees to the summary or explanation and the fees prior to the provision of information;⁸⁷
- ◆ Access must be provided by arranging a convenient location and time with the individual;⁸⁸
- ◆ You may impose a reasonable, cost-based fee to cover the cost of copying, postage, and preparing an explanation or summary of the PHI (if the summary or explanation is agreed to by the individual).⁸⁹

You must also maintain for six years documentation of the designated record sets accessible and the titles of the persons or offices responsible for receiving and processing access requests.⁹⁰

The key to ensuring compliance with these provisions is to establish the appropriate procedures and make sure that employees understand them.

B. Amendment Rights

You must give individuals the opportunity to amend PHI or a record about the individual in a designated record set.⁹¹ This right exists for as long as the PHI is maintained in the designated

record set.⁹² You may require that the request be in writing.⁹³ You must act upon the request within 60 days of receipt.⁹⁴

You may deny a request for an amendment if you determine:

- ◆ The information was not created by you, unless there is a reasonable basis to believe that the originator of the information is no longer available to amend it (*i.e.*, another provider, now retired, has forwarded records that a patient wishes to have amended);
- ◆ The information is not part of the designated record set;
- ◆ The information would not be available under the access provisions; or
- ◆ The information is accurate and complete.⁹⁵

If you deny the request, in whole or in part, you must provide the individual with a timely, written denial that, in plain language:

- ◆ Describes the basis for the denial, describes the individual's right to submit a written statement disagreeing with the denial and how to exercise this right;
- ◆ Describes that if there is no statement of disagreement that the individual may request the provider submit the request for amendment along with the record with any future disclosure; and
- ◆ Describes how the individual may pursue the complaint process with the provider or the Secretary of HHS.⁹⁶

If the individual files a written statement of disagreement, you may, but are not required to, prepare a written rebuttal.⁹⁷ The documents (the request, written statement of disagreement, and rebuttal – any of which have been submitted) must be linked to the PHI in the record that has been identified as being the subject of such a request.⁹⁸ The statement of disagreement (or a summary of it by the provider) or the request for amendment (or summary of it) if no statement of disagreement has been filed, must be included with future disclosures of the PHI.⁹⁹

If you grant a request to amend PHI, you must amend the record, at a minimum, by identifying the PHI that is the subject of the request and append or otherwise link the corrected information to it.¹⁰⁰ Also, you must notify the individual and make reasonable efforts to notify others identified by the individual and persons (including your business associates) that you know to have the PHI and that may have relied or foreseeably may rely upon it to the detriment of the individual.¹⁰¹ If you receive a notice of amendment, you must amend the PHI you hold.¹⁰²

You must document the title of the persons or the offices responsible for carrying out this process and retain this documentation for six years.¹⁰³

As with the access requirements, the key to ensuring compliance with these provisions is to establish the appropriate procedures and make sure that employees understand them.

C. Accounting of Disclosures

You must also develop procedures to provide patients with an account of disclosures of their PHI upon request.¹⁰⁴ The accounting must include most disclosures of the PHI made by the provider during the six years prior to the date of the request (unless the individual requests a shorter period of time).¹⁰⁵ The accounting does not have to include disclosures:

- ◆ To carry out treatment, payment, or health care operations;
- ◆ To the individual who is the subject of the PHI;
- ◆ For a facility directory;
- ◆ To persons involved in an individual's cares;
- ◆ For purposes of notification;
- ◆ For national security or intelligence purposes;
- ◆ To correctional institutions or law enforcement officials; or
- ◆ That occurred prior to April 14, 2003.¹⁰⁶

If a health oversight agency or law enforcement official requests, you must also refrain from including disclosures to these individuals for a time specified by the agent or official.¹⁰⁷ You must document the request and the name of the agent or official making the request.¹⁰⁸

An accounting of disclosures must be written and include the following:

- ◆ Disclosures of PHI that occurred during the six years (unless the individual requests a shorter period of time) prior to the request, including disclosures to or by business associates; and
- ◆ Each disclosure notation must include the date of the disclosure, the name of the entity or person to whom the disclosure was made (and address, if known), a brief description of the PHI disclosed, and a brief statement of the purpose of the disclosure (or a copy of an individual's authorization or written request under which the disclosure was made).¹⁰⁹

If the disclosure is part of a set of disclosures made to the same entity or person, the accounting may include the required information for the first disclosure, the frequency of these disclosures, and the date of the last disclosure during the accounting period.¹¹⁰

You must act upon the individual's request within 60 days of receipt.¹¹¹ The first accounting during a 12 month period must be free of charge; however, you may charge a reasonable, cost-based fee for subsequent accounting during this time period.¹¹² You must maintain documentation of the

information required to be included in the accounting, any written accounting provided to an individual, and the title of the person or the offices responsible for receiving and processing accounting requests for six years.¹¹³

D. Right to Request a Restriction

Although you must provide individuals with the right to request a restriction on the uses and disclosures of PHI for treatment, payment, health care operations and on the uses and disclosures for involvement in an individual's care or for notification purposes, you are not required to grant such a request.¹¹⁴ The regulation does not require documentation or implementing denial processes for these requests.

If you do agree to a restriction, you must abide by the restriction.¹¹⁵ If the information is required for emergency treatment, you may use or disclose the information. However, if you agreed to the restriction, you must request that the provider to whom the disclosure is made not further use or disclose the information.¹¹⁶ Restrictions also do not apply to uses or disclosures for facility directories, disclosures to the individual who is the subject of the PHI, or to uses or disclosures for which a consent or authorization is not required (see above for list of these uses and disclosures).¹¹⁷ If you wish to terminate the agreement, you must follow the procedures outlined in the regulation.¹¹⁸ If you agree to a restriction, you must maintain documentation of the agreement for six years.¹¹⁹

E. Right to Request Confidential Communications

You must provide patients with the opportunity to request the confidential communication of their PHI.¹²⁰ If you receive such a request, you must communicate PHI by an alternative means or to alternative locations, if reasonable.¹²¹ You may require the request be in writing. Granting such a request may be conditioned on the specification of an alternative address or other method of contact or, when appropriate, upon receiving information as to how payment will be handled.¹²² You cannot require an explanation from the individual as to the reason for the request.¹²³

THE PROVIDER-PROVIDER RELATIONSHIP

To the extent that you engage in electronic HIPAA transactions with other providers, the relationship may be altered by the transaction, code sets, or identifiers regulations. You may wish to adopt the new code sets (which tend to be those already used by the community, such as the ICD-9 codes) for efficiency reasons. Until the security regulation is final, it is unclear the extent to which that regulation may impact the relationship. The security regulation, however, is likely to require that certain verification and authentication is followed, as well as general security measures are adopted. The final privacy regulation does discuss this relationship, but to a lesser degree than the provider-patient relationship.

I. Disclosures for Treatment Purposes

The most common communication of information between providers tends to be for purposes of treatment. Treatment may include referral to specialists (*i.e.*, direct treatment relationships) or consultations in which a second provider never sees the patient (*i.e.*, indirect treatment relationships).

The consent provides you with the authority to disclose PHI to other providers for treatment.¹²⁴ These providers, if in a direct treatment relationship, must obtain their own consent. You may not obtain a consent on behalf of another provider or covered entity, unless the consent is a joint consent for an OHCA.¹²⁵ Alternatively, you may obtain an authorization on their behalf from the patient. An authorization may permit another provider to disclose PHI to you.¹²⁶

If a disclosure is part of an indirect treatment relationship, no additional consent is required, but the indirect treatment provider must use the information consistent with your privacy practices. Thus, if you consult with another provider, but you do not see the patient, you do not need a consent to use the information to provide the consultation.

The minimum necessary standard does not apply to disclosures by a provider for treatment.¹²⁷ Thus, you need not apply your minimum necessary policies and procedures in these circumstances. The minimum necessary standard also does not apply to authorizations requested by a covered provider for its own use and disclosure; authorizations requested by a covered entity for disclosures by others; authorizations for uses or disclosures of PHI created for research that includes treatment of the individual; or for uses or disclosures required by law.¹²⁸ Thus, to the extent you seek an authorization from a patient to obtain PHI from another provider, the disclosure does not have to be the minimum amount necessary, unless the authorization includes such a provision.

Your relationship with other providers may also be affected by your willingness to agree to restrictions on the use and disclosure of PHI requested by your patients. If you agree to a restriction you must abide by it and not disclose to a restricted provider unless the exception for emergency treatment applies.¹²⁹ See “Right to Request a Restriction”.

As always, if another provider requests de-identified information, you may disclose it without a consent or authorization.¹³⁰

Disclosures to a provider concerning the treatment of an individual are not considered disclosures to business associates and, therefore, no business associate contract or other satisfactory assurance document is required.¹³¹ Similarly, OHCA participants are not business associates.¹³² See “Special Concerns” for an explanation of OHCA’s.

If you do not know the provider to whom you are making the disclosure, you must verify the provider’s identity and authority.¹³³

II. Disclosures for Health Care Operations

Providers may also find themselves sharing information with other providers if they are part of affiliated organizations. OHCA participants are not business associates.¹³⁴ However, under certain circumstances, you may obtain joint consents that may be relied upon for uses and disclosures of PHI for the purpose of health care operations.¹³⁵

THE PROVIDER-HEALTH PLAN RELATIONSHIP

The relationship between providers and health plans will also be affected by the HIPAA regulations. The most significant changes result from the transaction, code sets, and identifiers regulations. If you rely upon a health care clearinghouse to code your claims and similar information sent to health plans, you will see little change in your daily operations. However, if you code your electronic communications yourself, you may experience some changes. The most important will be that there will be one set of codes for all health plans. This regulation is highly technical. In some cases, it may require adopting new computer software. You should consult with counsel or information technologists to evaluate what you may or may not need to do in light of these regulations. You do not have to adopt electronic transactions unless you wish. If you want to engage in electronic HIPAA transactions, the health plan must abide by your choice. It is likely that you may need to be aware of the new standard codes, obtain a provider identifier, and use, when appropriate, an employer identifier when submitting claims and similar information to health plans.

Until the security regulation is final, it is unclear the extent to which that regulation may impact the relationship between providers and health plans. The security regulation is likely to require the adoption of certain security and verification mechanisms.

The final privacy regulation also impacts the relationship between providers and health plans. You should be aware that health plans have special requirements under this regulation. This synopsis does not alert you to all of these requirements, but depending upon your interaction with health plans, you may wish to explore these unique provisions further.

I. Disclosures to Health Plans

A. Payments

Most of your interaction with health plans will be for payment purposes. Submitting claims and determining coverage require the exchange of PHI. When health plans function as the payers of health care services and products they are not business associates.¹³⁶ Your disclosures to them for purposes of payment or health care operations come within the scope of your consent.¹³⁷ You do not need to obtain an additional document for these disclosures. (Health plans are not required to obtain consents, but if they do, they are bound by the terms of these agreements.¹³⁸ You may not obtain a consent on behalf of health plan,¹³⁹ but you may seek an authorization on their behalf.¹⁴⁰ The regulation does not require you to obtain any documents for health plans.)

B. Health Care Operations

Other disclosures to health plans may require an authorization from the individual.¹⁴¹ For example, if you wish to disclose PHI to a health plan that it will use for marketing purposes, you or the health plan will need an authorization. Some disclosures may come within one of the regulatory exceptions.¹⁴² For example, you may disclose PHI to a health plan pursuant to a court order.¹⁴³

Because of the fact-specific nature of such requests, you should consult with counsel to determine when you may rely on such exceptions. You may always provide de-identified information without a consent or authorization.¹⁴⁴

C. Minimum Necessary

The minimum necessary standard does apply to disclosures to health plans. Thus, you need to develop procedures for dealing with the routine and recurring disclosures and describe them in your policies and procedures.¹⁴⁵ Special requests will require individual consideration.¹⁴⁶ Health plans may only request the minimum amount necessary.¹⁴⁷ When a health plan makes a request, you may rely, if such reliance is reasonable, on the assertion of the plan that the amount requested is the minimum necessary for the purpose stated.¹⁴⁸ Unless it is specially justified, you may not disclose the entire medical record.¹⁴⁹

If you do not know the plan official to which you are making the disclosure, you must verify the official's identity and authority.¹⁵⁰

II. Business Associate Contracts and Health Plans

Health plans are not business associates unless they act on your behalf or provided a specific service for you, such as data aggregation or administrative services.¹⁵¹ If a health plan is a business associate because it provides you with financial services, you will need to enter into a business associate contract with the plan.¹⁵² While these contracts may contain standard provisions, you should consider your privacy practices and incorporate them appropriately into your documents. See "The Provider-Business Associate Relationship".

THE PROVIDER-CLEARINGHOUSE RELATIONSHIP

The relationship between providers and health care clearinghouses will also be affected by the HIPAA regulations. The most significant changes result from the transaction, code sets, and identifiers regulations. If you rely upon a health care clearinghouse to code your claims and similar information, you may see little change in your daily operations. If you do not already rely upon a health care clearinghouse and wish to engage in electronic HIPAA transactions, you may wish to establish such a relationship.

Until the security regulation is final, it is unclear the extent to which that regulation may impact this relationship. The regulation is likely to require the adoption of certain security and verification mechanisms.

The final privacy regulation also impacts the relationship between providers and health care clearinghouses. You should be aware that health care clearinghouses must comply with the privacy regulation as well. These rules differ slightly based on their roles. This synopsis does not alert you to all of these differences, but depending upon your interaction with clearinghouses, you may wish to explore these unique provisions further.

Your interaction with health care clearinghouses is most likely going to be in a business associate relationship. For example, you may hire a clearinghouse to assist you with coding of various types of information you submit to insurers. Thus, you will need to enter into a business associate contract with the clearinghouse.¹⁵³ While these contracts may contain standard provisions, you should consider your privacy practices and incorporate them appropriately into such documents. See “The Provider-Business Associate Relationship”.

THE PROVIDER-BUSINESS ASSOCIATE RELATIONSHIP

The HIPAA regulations create a new term for relationships that exist between health care providers and others who assist them with delivering care. Although business associates are referred to in the transaction regulation, they are most important in the context of the security and privacy regulations. Until the security regulation is final, it is unclear what specific requirements will be placed on these relationships. However, it is likely something akin to the business associate contract will be required. The privacy regulation does not directly regulate business associates but does require covered providers to obtain adequate assurances that business associates will protect the privacy of the PHI they receive from a covered provider, consistent with that provider's policies and practices and the final regulation.

I. Identifying Business Associates

A business associate is a person who performs or assists in the performance of “a function or activity involving the use or disclosure of individually identifiable health information (IIHI) . . . or any other function or activity regulated by [the privacy regulation].” A business associate also may be a person, other than a member of the workforce, who provides one of the designated services, if the provision of the service involves the disclosure of IIHI from a covered entity or organized health care arrangement (OHCA) or from another business associate of such covered entity or arrangement, to the person.¹⁵⁴ A business associate may itself be a covered entity.

II. The Business Associate Contract

Before you may disclose PHI to a business associate or allow a business associate to create or receive PHI on your behalf, you must first obtain “satisfactory assurance” that the business associate will appropriately safeguard the information.¹⁵⁵ In most instances, a satisfactory assurance is a contract between you and the business associate.¹⁵⁶

At a minimum, this contract must:

- ◆ Establish the permitted and required uses and disclosures of PHI by the business associate (these may not exceed what the covered entity could do with the information, but may permit the business associate to use or disclose PHI for its own proper management and administrative functions and may permit the business associate to provide data aggregation services related to health care operations);
- ◆ Provide that the business associate will:
 - Not use or further disclose PHI other than as permitted or required by the contract or required by law;
 - Use appropriate safeguards to prevent the improper use or disclosure of PHI;

- Report to the covered entity any use or disclosure that is not provided for in the contract of which it is aware;
 - Ensure that any agents (including subcontractors) to whom it provides PHI from the covered entity (or its business associate) agrees to the same restrictions and conditions that apply to the business associate with regard to the information;
 - Make PHI available in accordance with the right to access;
 - Make PHI available in accordance with the right to amend and incorporate amendments;
 - Make available information required to provide an accounting of disclosures;
 - Make available internal practices, books, and records relating to the use and disclosure of PHI obtained from or on behalf of the provider to the Secretary of HHS to determine compliance by the provider with the privacy regulation;
 - Return or destroy, if feasible, all PHI received from, or created or received on behalf of, the provider that the business associate maintains in any form at the termination of the contract; if it is not feasible, the business associate must extend the protections of the contract to the information and limit further uses and disclosures to purposes that make the return or destruction infeasible; and
- ◆ Authorize termination of the contract by the provider if the provider determines that the business associate has violated a material term of the contract.¹⁵⁷

III. Other Responsibilities of Business Associates

As your agent, a business associate is responsible for protecting the PHI it creates, receives, and maintains on your behalf. If a business associate maintains designated record sets, it is obligated to assist you with providing individuals with the rights established in the privacy regulation. A business associate's disclosures should also be part of your accounting of disclosures. Consents and authorizations you obtain cover the activities of your business associates. These relationships are highly fact specific and should be examined in detail when developing a compliance plan.

ADMINISTRATIVE REQUIREMENTS

As noted throughout, the privacy regulation, unlike the transaction, code sets, and identifiers regulations, contains specific administrative requirements. At this point, it is unclear whether the security regulation will also contain similar provisions.

The privacy regulation requires you to implement certain administrative requirements to ensure compliance with the rule. These include:

- ◆ Designating a privacy official;
- ◆ Training your workforce;
- ◆ Implementing appropriate administrative, technical, and physical safeguards;
- ◆ Establishing a complaint process for individuals;
- ◆ Sanctioning members of the workforce who violate the privacy regulation or your privacy practices (policies and procedures);
- ◆ Refraining from intimidating or retaliatory acts against individuals;
- ◆ Refraining from requiring individual's to waive their rights under the privacy regulation;
- ◆ Implementing policies and procedures designed to comply with the privacy regulation; and
- ◆ Maintaining appropriate documentation for six years.

The Guide explains these requirements in detail in the "First Steps."

SPECIAL PRIVACY CONCERNS

I. De-identification

The privacy regulation describes how covered entities and their business associates may avoid having to comply with the regulation. If a covered entity or a business associate “de-identifies” PHI, the final regulation does not apply to that information.¹⁵⁸ De-identified information is information for which there is no reasonable basis to believe the information can be used to identify an individual.¹⁵⁹ Under the final rules, information is de-identified if certain designated identifiers specified in the rule are removed.¹⁶⁰ PHI may also be de-identified if a person qualified under the rule determines that “the risk is very small that the information could be used to identify the individual.”¹⁶¹ Covered entities may rely upon codes or other means of record identification to permit eventual re-identification.¹⁶² These codes or identification means must not be used or disclosed for other purposes.¹⁶³

II. Personal Representatives

Providers should also be aware that they must treat a personal representative as the individual for purposes of the privacy regulation.¹⁶⁴ Personal representatives are defined by State law. Providers treating minors should also consult the personal representative provisions and the law of the State in which they practice to determine if any special accommodations are appropriate.

III. Affiliated Entities

The privacy regulation permits legally separate covered entities that are affiliated (or the health care components of such entities) to designate themselves as a single covered entity.¹⁶⁵ Such designations are permissible only “if all of the covered entities designated are under common ownership and control.”¹⁶⁶ Common ownership means an entity (or entities) “posses an ownership or equity interest of 5 percent or more in another entity.”¹⁶⁷ Common control means, “an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.”¹⁶⁸

Affiliated covered entities may comply with the rules as if they were a single covered entity.¹⁶⁹ For example, if you qualify as an affiliated entity, you and your affiliates may provide a single shared notice that meets the requirements of the notice provisions. To obtain these advantages, you must document the affiliation.¹⁷⁰ Each affiliated must also ensure that its use and disclosure of PHI complies with the applicable requirements of the privacy regulation. The covered entities that join to make the affiliated covered entity are separately subject to liability.¹⁷¹

To determine whether you can take advantage of these provisions, you should consult with counsel.

IV. Organized Health Care Arrangements (OHCAs)

The privacy regulation also contains special provisions to help providers in clinically integrated care settings in which patients typically receive treatment from more than one provider.¹⁷²

OHCAs also include organized systems of health care “in which more than one covered entity participates” and in which these entities participate in joint activities that include at least one of the following:

- ◆ Utilization review that includes review by other participating covered entities or third parties on their behalf;
- ◆ Quality assessment and improvement activities in which the treatment is assessed by other participating covered entities or third parties on their behalf; and
- ◆ Payment activities if the financial risk is shared by the covered entities and other covered entities review PHI to determine this risk.

Certain group health plan arrangements may also be designated as OHCAs.

The major benefits of being part of an OHCA are the ability to issue joint consents and joint notices. For example, if you work with hospitals and are a contractor, but not an employee, you may be able to rely upon the consents obtained and notices provided by the hospital to the patients you see in the hospital.¹⁷³ If you see patients privately, you may need to obtain consents from and provide notices to these individuals, even if the hospital already obtained or provided the documents. You should consult with counsel to determine if you can come within these special provisions.

V. Hybrid Entities

A hybrid entity is a “single legal entity that is a covered entity and whose covered functions are not its primary functions.”¹⁷⁴ Covered functions are “those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.”¹⁷⁵ For example, a company that makes light bulbs as its primary function, but that maintains an employee health clinic that engages in electronic HIPAA transactions is a hybrid entity. It is a covered entity because it functions as a covered health care provider. It is a hybrid entity, however, because its primary function, making light bulbs, is not a covered function – making light bulbs is not the function that makes it a health care provider, rather its operation of the employee health clinic (a covered provider) is the covered function.

As a hybrid entity, it “is responsible for designating the components that are part of one or more health care components.”¹⁷⁶ The health care component is the component of the covered entity that performs covered functions.¹⁷⁷ Once designated, the health care component is subject to the requirements of the privacy regulation. The covered entity/hybrid entity is responsible for other functions as well, such as constructing “firewalls” to ensure that the PHI of the health care component is handled in accordance with the rules. However, it is the health care component, in practical terms that must comply on a day to day basis with the regulation.

To determine whether you can take advantage of these provisions, you should consult with counsel. However, it is extremely unlikely they will apply to most providers.

THE INTERNET

The HIPAA transaction, code sets, and identifiers regulation will impact your interactions with the Internet only to the extent you submit claims or perform other specific HIPAA transactions via the Internet. You are not required to use these codes or identifiers if you are simply maintaining a content-based web site or emailing with your patients.

Until the security regulation is final, it is unclear the extent to which that regulation may impact your Internet activities. It is very likely you will need to consider using specific security and verification methods, such as electronic signatures.

The final privacy regulation requirements apply to the Internet. For example, when appropriate, you may wish to obtain consents and authorization via the Internet. You may also deliver notices by posting them on a website or delivering them via email. If you operate a web site in which PHI is created, received, or maintained, you should consult with counsel to determine how particular activities may be affected by the rule.

CONCLUSION

This Guide does not provide a complete assessment of the impact of the HIPAA regulations on your practice. Developing such an analysis requires a fact-specific inquiry, which we encourage you to engage in with appropriate counsel. This Guide, however, should provide you with a basic understanding of the issues you may face as you seek to come into compliance with these regulations.

APPENDIX OF FORMS

This appendix contains the forms presented in the various sections of this Guide. These forms are model documents and should not be used without consultation with counsel. The forms provide you with an idea of the information your individualized documents should contain. In some cases, as noted within the model, you may need to add other provisions.

Consent

You agree to permit your protected health information to be used and disclosed for purposes of treatment, payment, and health care operations. For more details about these uses and disclosures, please see our Privacy Notice.

We reserve the right to change our privacy policies described in the Privacy Notice. You may call us to receive an updated Notice.

You have the right to request that we restrict how your protected health information is used or disclosed to carry out treatment, payment, or health care operations. We are not required to agree with this request, but if we do, we are bound by it.

You have the right to revoke your consent in writing. A revocation, however, will not apply to the extent we have taken action in reliance upon the use or disclosure of your information.

Signature

Date

Authorization

You agree to the use and/or disclosure of the following information:

A request for the use or disclosure of this information may be made by:

This information may be used or disclosed to:

This authorization expires on: _____

Information used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer protected by the Federal privacy regulation.

Signature

Date

[You may need to add other provisions if you are seeking an authorization to use or disclose the information yourself or if you are obtaining the authorization on behalf of another covered entity]

Notice: Effective _____

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.

We may use and disclose your protected health information for purposes of treatment, payment, and health care operations, as permitted by Federal law. **[provide a description of these uses and disclosures]**.

We may use and disclose your protected health information for purposes other than for treatment, payment, or health care operations without your consent or authorization, as permitted or required by the Federal law. **[provide a description of these uses and disclosures]**.

We will make other uses and disclosures only with your authorization; this authorization may be revoked.

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 **[necessary only if you (the provider) intend to engage in such activities]**

We may contact you to raise funds for our organization **[necessary only if you (the provider) intend to engage in such activities]**

You have the right to **access and amend** your protected health information that is used to make decisions about individuals. You have the right to receive an **accounting** of disclosures of your protected health information. You have the right to **request a restriction** on certain uses and disclosures of your protected health information. We are not required to grant your request. You have the right to receive **confidential communications** of your protected health information. You have the right to **obtain a paper copy of this notice** upon request. You may exercise these rights as follows:

We are required by law to maintain the privacy of protected health information and to provide you with notice of our legal duties and privacy practices with respect to protected health information.

We are required to abide by the terms of the most current notice in effect.

We reserve the right to change the terms of our notice and to make the new notice provisions effective for all protected health information that we maintains. We will provide you with a revised notice by _____ **[necessary only if you (the provider) intend to change a privacy practice that is listed in the notice]**

If you believe your privacy rights have been violated, you may complain to us or the Secretary of HHS. You may file a complaint in the following way: _____

We will not retaliate against you for filing a complaint.

For more information about this notice, contact: _____

[You may wish to include additional provisions]

APPENDIX OF DEFINITIONS

Affiliated entities – Entities that are legally distinct, but share common administration of organizationally differentiated, yet similar activities and are under common control or ownership (e.g., a hospital chain).¹⁷⁸

Authorizations – Legal permission given by an individual permitting a covered entity to use or disclose his/her PHI for purposes other than for treatment, payment, or health care operations. Must contain specific provisions outlined in the privacy regulation.¹⁷⁹

Business associate – An entity or person acting on behalf of a covered entity or performing one of the services specified in the privacy regulation for a covered entity when the provision of the service involves the disclosure of individually identifiable health information. These services are: legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. Business associates do not include members of a covered entity’s workforce.¹⁸⁰

Code sets regulation – Regulation issued by HHS adopting standards for codes used in electronic health care transactions.¹⁸¹

Common control – Common control exists if “an entity has the power, directly or indirectly, significantly to influence or direct the actions or policies of another entity.” (relates to the affiliated entity provisions).¹⁸²

Common ownership – Common ownership exists if an entity (or entities) “posses an ownership or equity interest of 5 percent or more in another entity.” (relates to the affiliated entity provisions).¹⁸³

Consents – Legal permission given by an individual permitting a covered entity to use or disclose his/her PHI for purposes of treatment, payment, or health care operations. Must contain specific provisions outlined in the privacy regulation.¹⁸⁴

Covered entity – Health care providers involved in electronic HIPAA transactions, health plans, and health care clearinghouses. The HIPAA regulations directly regulate these entities.¹⁸⁵

De-identified information – Information for which there is no reasonable basis to believe that the information can be used to identify an individual or information that no longer contains any of the identifiers listed in the privacy regulation.¹⁸⁶

Designated record sets – A group of records maintained by a covered entity or its business associate(s) that are used to make decisions about individuals.¹⁸⁷

Electronic HIPAA transactions – Electronic health-related transactions for which HHS under the authority of HIPAA has adopted specific standards. (See page 7 for a list of the current HIPAA transactions.)

Health care operations – Health care operations include the following activities, “to the extent the activities are related to covered functions.” These activities are: conducting quality assessment and improvement activities (which includes population-based activities relating to improving health or reducing health care costs and cases management); reviewing the competence or qualifications of

health care professionals and similar activities; underwriting, premium rating, and other similar activities; conducting or arrangement for medical review, legal services, and auditing functions; business planning and development; and business management and general administrative activities.¹⁸⁸ Covered entities may use and disclose PHI for purposes of health care operations only with a consent.

Hybrid entities – A covered entity whose covered, health care-related functions are not its primary functions.¹⁸⁹

Identifiers regulations – Regulations issued by HHS adopting identifiers for health care providers, employers, and health plans to be used in electronic transactions. Although HIPAA calls for the adoption of an identifier for individuals, Congress has yet to allocate funds to HHS to promulgate an individual identifier rule.

Indirect treatment relationship – A relationship between a provider and an individual in which the 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.”¹⁹⁰

Individually identifiable health information (IIHI) – Health information, including demographic information collected from an individual, that “(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (2) 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; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.”¹⁹¹

Minimum necessary standard – Generally, the policies and procedures a covered entity adopts to ensure that only the minimum amount of information necessary for the purpose of a use or disclosure is, in fact, used or disclosed. Only in rare instances will covered entities need to use the standard on a case-by-case basis.¹⁹²

Notices – Written documents containing an entity’s privacy practices that covered entities must provide to individuals.¹⁹³

Organized health care arrangements (OHCAs) – Entities that are “(1) a clinically integrated care setting in which individuals typically receive health care from more than one health care provider; (2) an organized system of health care in which more than one covered entity participates, and in which the participating covered entities” engaged in certain activities jointly, as specified in the privacy regulation, such as utilization review, quality assessment activities, and payment activities; or (3) certain group health plans.¹⁹⁴

Payment – Payment includes the following activities “(1) activities undertaken by: (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or (ii) a covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) the activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited

to: (i) determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (ii) risk adjusting amounts due based on enrollee health status and demographic characteristics; (iii) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing; (iv) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (v) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (vi) disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement: (A) name and address; (B) date of birth; (C) social security number; (D) payment history; (E) account number; and (F) name and address of the health care provider and/or health plan.”¹⁹⁵ Covered entities may use and disclose PHI for purposes of payment only with a consent.

Privacy official – An individual who oversees the development and implementation of the policies and procedures, receives complaints from individuals, and provides further information about the notice provided to patients.¹⁹⁶

Protected health information (PHI) – All individually identifiable health information, including information that is in oral, written, and electronic form, except for certain information defined in the Family Educational Right and Privacy Act.¹⁹⁷

Transaction – The transmission of information between two parties to carry out financial or administrative activities related to health care.¹⁹⁸

Transaction regulation – Regulation issued by HHS adopting standards for eight electronic transactions by covered entities.¹⁹⁹

Treatment – Treatment includes the following activities: “the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.”²⁰⁰ Covered entities may use and disclose PHI for purposes of only with a consent.

ENDNOTES

¹ 45 C.F.R. § 160.103.

² *Id.*

³ *Id.* at § 164.530(i).

⁴ *Id.* at § 164.514(d).

⁵ *Id.*

⁶ *Id.* at § 164.501.

⁷ *Id.* at § 164.530(a).

⁸ *Id.* at § 164.530(b).

⁹ *Id.* at § 164.502(j).

¹⁰ *Id.* at § 164.530(g).

¹¹ *Id.* at § 164.530(e).

¹² *Id.* at § 164.530(a)(1)(ii).

¹³ *Id.* at § 164.530(d).

¹⁴ *Id.*

¹⁵ *Id.* at § 164.532.

¹⁶ 65 Fed. Reg. 82944 (2000).

¹⁷ 45 C.F.R. § 164.501.

¹⁸ *Id.*

¹⁹ *Id.*

²⁰ It is important for providers to realize that health plans and health care clearinghouses are not required to obtain an individual's consent to use or disclose PHI for purposes of treatment, payment, or health care operations. *Id.* at § 164.506(a)(4). This difference is due to the fact that health plans and health care clearinghouses do not have a direct relationship with most individuals. However, to the extent one of these entities seeks a consent, it is bound by an individual's decision to deny such consent. *Id.*

²¹ *Id.* at §§ 164.506(a)(5) & 164.506(f).

²² *Id.* at § 164.501

²³ *Id.* at § 164.506(a)(2).

²⁴ *Id.* at § 164.506(a)(3).

²⁵ *Id.* at § 164.506(d).

²⁶ *Id.* at § 164.506(b)(1).

²⁷ *Id.* at § 164.506(b)(3).

²⁸ *Id.* at § 164.506(b)(4).

²⁹ *Id.* at § 164.506(b)(5).

³⁰ *Id.* at § 164.530(j).

³¹ *Id.* at § 164.508.

³² *Id.* at § 164.508(a)(2). There are some exceptions to this general rule.

³³ *Id.* at § 506(d).

³⁴ *Id.* at § 506(e).

³⁵ *Id.* at § 506(c).

³⁶ For a complete list of these requirements, see *id.* at § 506(d) & (e).

³⁷ *Id.* at § 164.508(c).

³⁸ *Id.* at § 164.508(d).

³⁹ *Id.* at § 164.508(e).

⁴⁰ *Id.* at § 164.508(b)(4).

⁴¹ *Id.* at § 164.508(b)(4)(iv).

⁴² *Id.* at § 164.508(b)(3).

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ *Id.* at § 164.530(j).

⁴⁶ *Id.* at § 164.506(e).

⁴⁷ *Id.*

⁴⁸ *Id.* at § 164.510(a). This opportunity may be as simple as a conversation between the provider and the patient.

⁴⁹ *Id.* at § 164.510(b).
⁵⁰ *Id.* at § 164.512(a).
⁵¹ *Id.* at § 164.512(b).
⁵² *Id.* at § 164.512(c).
⁵³ *Id.* at § 164.512(d).
⁵⁴ *Id.* at § 164.512(e).
⁵⁵ *Id.* at § 164.512(f).
⁵⁶ *Id.* at § 164.512(g).
⁵⁷ *Id.* at § 164.512(h).
⁵⁸ *Id.* at § 164.512(i).
⁵⁹ *Id.* at § 164.512(j).
⁶⁰ *Id.* at § 164.512(k).
⁶¹ *Id.* at § 164.512(l).
⁶² *Id.* at § 164.514(e).
⁶³ *Id.* at § 164.520(a).
⁶⁴ *Id.* at § 164.520(c)(2).
⁶⁵ *Id.*
⁶⁶ *Id.*
⁶⁷ *Id.*
⁶⁸ *Id.* at § 164.520(c)(3).
⁶⁹ *Id.*
⁷⁰ *Id.* at § 164.520(d).
⁷¹ If another law prohibits or materially limits by other law, these descriptions must reflect the more stringent law.
⁷² If another law prohibits or materially limits by other law, these descriptions must reflect the more stringent law.
⁷³ *Id.* at § 164.520(b).
⁷⁴ *Id.* at § 164.530(j).
⁷⁵ *Id.* at § 164.501.
⁷⁶ *Id.* at § 164.524(a).
⁷⁷ *Id.*
⁷⁸ *Id.* at § 164.524(a)(2).
⁷⁹ *Id.* at § 164.524(a)(3).
⁸⁰ *Id.* at § 164.524(a)(4).
⁸¹ *Id.* at § 164.524(d).
⁸² *Id.*
⁸³ *Id.*
⁸⁴ *Id.* at § 164.524(b). This time may be altered slightly in accordance with the rules.
⁸⁵ *Id.* at § 164.524(c).
⁸⁶ *Id.*
⁸⁷ *Id.*
⁸⁸ *Id.*
⁸⁹ *Id.*
⁹⁰ *Id.* at § 164.524(e).
⁹¹ *Id.* at § 164.526(a).
⁹² *Id.*
⁹³ *Id.* at § 164.526(b).
⁹⁴ *Id.* If it is impossible to act within 60 days, there are provisions for an extension of the period, so long as the individual is notified.
⁹⁵ *Id.* at § 164.526(a)(2).
⁹⁶ *Id.* at § 164.526(d).
⁹⁷ *Id.* at § 164.526(d)(3).
⁹⁸ *Id.* at § 164.526(d)(4).
⁹⁹ *Id.* at § 164.526(d)(5). If the disclosure is via a standard transaction that does not permit the inclusion of additional information, these documents may be sent separately.
¹⁰⁰ *Id.* at § 164.526(c).
¹⁰¹ *Id.*
¹⁰² *Id.* at § 164.526(e).

-
- ¹⁰³ *Id.* at § 164.526(f).
¹⁰⁴ *Id.* at § 164.528.
¹⁰⁵ *Id.*
¹⁰⁶ *Id.*
¹⁰⁷ *Id.*
¹⁰⁸ *Id.*
¹⁰⁹ *Id.* at § 164.528(b).
¹¹⁰ *Id.*
¹¹¹ *Id.* at § 164.528(c). If it is impossible to act within 60 days, there are provisions for an extension of the period, so long as the individual is notified.
¹¹² *Id.*
¹¹³ *Id.* at § 164.528(d).
¹¹⁴ *Id.* at § 164.522(a).
¹¹⁵ *Id.*
¹¹⁶ *Id.*
¹¹⁷ *Id.*
¹¹⁸ *Id.*
¹¹⁹ *Id.*
¹²⁰ *Id.* at § 164.522(b).
¹²¹ *Id.*
¹²² *Id.*
¹²³ *Id.*
¹²⁴ *Id.* at § 164.506(a).
¹²⁵ *Id.* at § 164.506(a)(5).
¹²⁶ *Id.* at § 164.508(e).
¹²⁷ *Id.* at § 164.502(b).
¹²⁸ *Id.*
¹²⁹ *Id.* at § 164.502(c).
¹³⁰ *Id.* at § 164.514(a)-(c).
¹³¹ *Id.* at § 164.502(e).
¹³² *Id.* at § 160.103.
¹³³ *Id.* at § 164.514(h).
¹³⁴ *Id.* at § 160.103.
¹³⁵ *Id.* at § 164.506(f).
¹³⁶ *See id.* at § 160.103.
¹³⁷ *Id.* at § 164.506.
¹³⁸ *Id.* at § 164.506.
¹³⁹ *Id.* at § 164.506(e).
¹⁴⁰ *Id.* at § 164.508
¹⁴¹ *Id.* at § 164.508.
¹⁴² *See id.* at §§ 164.510 & 164.512.
¹⁴³ *See id.* at § 164.512(e).
¹⁴⁴ *Id.* at § 164.502(d).
¹⁴⁵ *Id.* at § 164.502(b).
¹⁴⁶ *Id.* at § 164.514(d).
¹⁴⁷ *Id.* at § 164.514(d).
¹⁴⁸ *Id.* at § 164.514(b)(3)(iii).
¹⁴⁹ *Id.* at § 164.514(b)(5).
¹⁵⁰ *Id.* at § 164.514(h).
¹⁵¹ *Id.* at § 160.103.
¹⁵² *Id.* at § 164.502(e).
¹⁵³ *Id.* at § 164.502(e).
¹⁵⁴ These services are: legal, actuarial, accounting, consulting, data aggregation(as defined by the regulation), management, administrative, accreditation, or financial services. *Id.* at § 160.103.
¹⁵⁵ *Id.* at § 164.502(e).
¹⁵⁶ *Id.* at § 164.504(e).

157 *Id.* at §164.504(e)(2).
158 *Id.* at § 164.514(a).
159 *Id.* at § 164.514(b).
160 *Id.* at § 164.514 (b)(2).
161 *Id.* at § 164.514(b)(1).
162 *Id.* at § 164.514(c).
163 *Id.*
164 *Id.* at § 164.502(g).
165 *Id.* at § 164.504(d).
166 *Id.*
167 *Id.* at § 164.504(a).
168 *Id.*
169 *See* 65 Fed. Reg. at 82503.
170 *Id.* at § 164.504(d)(2).
171 *Id.* at § 164.504(d).
172 *Id.* at § 164.501.
173 *Id.* at §§164.506(f) & 164.520(d).
174 *Id.* at § 164.504(a).
175 *Id.* at § 164.501.
176 *Id.* at § 164.504(c)(3)(iii).
177 *Id.* at § 164.504(a).
178 65 Fed. Reg. at 82503.
179 *Id.* at 82513.
180 45 C.F.R. § 160.103.
181 65 Fed. Reg. 50312 (2000).
182 65 Fed. Reg. 82462, 82503 (2000).
183 *Id.*
184 *Id.* at 82509.
185 *Id.* at 82476.
186 *Id.* at 82542.
187 *Id.* at 82489.
188 *Id.*
189 *Id.* at 82502.
190 *Id.* at 82492.
191 45 C.F.R. § 164.501.
192 65 Fed. Reg. at 82544.
193 *Id.* at 82547.
194 *Id.* at 82494.
195 45 C.F.R. § 164.501.
196 65 Fed. Reg. at 82561.
197 *Id.* at 82496.
198 *Id.* at 82480.
199 65 Fed. Reg. 50312 (2000).
200 45 C.F.R. § 164.501.