University of Kentucky
UKnowledge

Continuing Legal Education Materials | Kentucky Legal History

3-2002

Health Care Information Privacy: Workshop on HIPAA

Office of Continuing Legal Education at the University of Kentucky College of Law

Follow this and additional works at: https://uknowledge.uky.edu/uky_cle

Part of the Health Law and Policy Commons

Right click to open a feedback form in a new tab to let us know how this document benefits you.

Repository Citation
Office of Continuing Legal Education at the University of Kentucky College of Law, "Health Care Information Privacy: Workshop on HIPAA" (2002). *Continuing Legal Education Materials*. 46.
https://uknowledge.uky.edu/uky_cle/46

This Book is brought to you for free and open access by the Kentucky Legal History at UKnowledge. It has been accepted for inclusion in Continuing Legal Education Materials by an authorized administrator of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

UK CLE

HEALTH CARE INFORMATION PRIVACY

- WORKSHOP ON HIPAA -

March 2002

UK
CLE

HEALTH CARE INFORMATION PRIVACY

- WORKSHOP ON HIPAA -

March 2002

Presented by the
OFFICE OF CONTINUING LEGAL EDUCATION
UNIVERSITY OF KENTUCKY COLLEGE OF LAW

FROM THE LAW LIBRARY OF: _____

_____

Written materials and oral presentations offered through the University of Kentucky College of Law Office of Continuing Legal Education (UK/CLE) are designed to assist lawyers in maintaining their professional competence. The Office of Continuing Legal Education and its volunteer speakers and writers are not rendering legal or other professional services by their participation in continuing legal education activities. Attorneys and others using information obtained from UK/CLE publications or seminars must also fully research original and current sources of authority to properly serve their or their client's legal interests. The forms and sample documents contained in our continuing legal education publications are intended for use only in conjunction with the professional services and advice of licensed attorneys. All parties must cautiously consider whether a particular form or document is suited to specific needs. The legal research presented herein is believed to be accurate, but is not warranted to be so. These written materials and the comments of speakers in presentation of these materials may contain expressions of opinion which do not necessarily reflect the views of the Office of Continuing Legal Education, the University of Kentucky, the Commonwealth of Kentucky, or other governmental authorities. UK/CLE strives to make its written materials and speaker presentations gender-neutral; however, gender-specific references may remain where it would otherwise be awkward or unclear. It should be understood that in such references the female includes the male, and vice-versa.

Copyright 2002 by the University of Kentucky College of Law,
Office of Continuing Legal Education.
All rights reserved.

Printed in the United States of America

ABOUT...

UK CLE

The University of Kentucky College of Law, Office of Continuing Legal Education (UK/CLE) was organized in 1973 as the first permanently staffed, full-time continuing legal education program in the Commonwealth of Kentucky. It endures with the threefold purpose to: 1) assist lawyers in keeping abreast of changes in the law; 2) develop and sustain practical lawyering skills; and 3) maintain a high degree of professionalism in the practice of law. Revenues from seminar registrations and publication sales allow the Office to operate as a separately budgeted, self-supporting program of the College. No tax dollars, bar dues or public funds are budgeted in the Office's finances.

Courses

UK/CLE provides a variety of workshops, conferences, and institutes to satisfy the continuing education needs of lawyers and other professionals. Courses range from half-day programs in selected areas to in-depth programs extending over several days. While most courses are conducted at the College of Law in Lexington, UK/CLE has a longstanding statewide commitment. Since its first year of operation, beginning with a criminal law program in Madisonville, Kentucky, the Office has continued to bring the highest quality continuing education to attorneys across Kentucky, the Midsouth, the Midwest, and the nation.

Publications

Each course is accompanied by extensive speaker-prepared course materials. These bound materials are offered for sale following courses and are consistently regarded as valuable, affordable references for lawyers. In 1987, UK/CLE began producing a series of publications which now consist of Practice Handbooks, Monographs, and Compendiums. Each Practice Handbook is an extensively referenced, fully indexed practice guide consisting of separately authored chapters, sequenced for the comprehensive coverage of a distinct body of law. Their format allows for updating through supplements and cumulative indexes. Each Monograph is a concisely written practice guide, usually prepared by a single author, designed to cover a topic of narrower scope than Practice Handbooks. Compendiums contain both official forms and sample documents. Designed to assist the lawyer by suggesting specific structures and language to consider in drafting documents, these publications are beneficial in the resolution of legal drafting concerns. The Compendiums are often used most effectively in conjunction with UK/CLE Practice Handbooks and Monographs.

Professional Management

UK/CLE serves the needs of the bar from its offices on the University of Kentucky campus in Lexington. Its staff manages course planning, publication content planning, course registrations, publications sales, course and publication marketing, publication composition and printing, as well as internal budgeting, accounting, and financial reporting. As an "income based" program, UK/CLE's course tuitions and publications sales are designed to generate sufficient revenues for self-support.

Commitment to Quality and Creativity

UK/CLE is a member of the Association for Continuing Legal Education (ACLEA). As such, UK/CLE subscribes to the Standards of Operation for Continuing Legal Education Organizations, and the Standards of Fair Conduct and Voluntary Cooperation administered under the auspices of the American Law Institute-American Bar Association Committee on Continuing Professional Education. Throughout its existence UK/CLE has been actively involved in the activities of and discourse sponsored by ACLEA. UK/CLE's association with national and international CLE professionals has afforded it the opportunity to continually reassess instructional methods, quality in publications, and effective means of delivering CLE services at consistently high levels of quality.

An Integral Part of the Legal Profession's Tradition of Service

An enormous debt is owed to the practitioners, professors, judges and other professionals who generously donate their time and talent to continuing legal education. Their knowledge and experience provide the fundamental components of our seminars and publications. Without their motivation and freely given assistance in dedication to the legal profession, high quality continuing legal education would not exist. As a non-profit organization, UK/CLE relies upon the traditional spirit of service to the profession that attorneys have so long demonstrated. We are constantly striving to increase attorney involvement in the continuing legal education process. If you would like to participate as a volunteer speaker or writer, please contact us and indicate your areas of interest and experience.

UK/CLE: A Self-Supporting Entity

The University of Kentucky Office of Continuing Legal Education (UK/CLE) is an income-based office of the University of Kentucky College of Law. As such, it is separately budgeted and financially self-supporting. UK/CLE operations are similar to not-for-profit organizations, paying all direct expenses, salaries and overhead solely from revenues. No public funds or tax dollars are allocated to its budget. Revenues are obtained from registrant enrollment fees, and the sale of publications. Our sole function is to provide professional development services. In the event surplus funds become available, they are utilized to offset deficits or retained in our budget to improve the quality and variety of services we provide.

UNIVERSITY OF KENTUCKY
COLLEGE OF LAW

OFFICE OF CONTINUING LEGAL EDUCATION

Suite 260 Law Building
Lexington, Kentucky 40506-0048

Phone
(859) 257-2921

Facsimile
(859) 323-9790

Web Address
www.uky.edu/Law/CLE

PRESIDENT, UNIVERSITY OF KENTUCKY:	Lee T. Todd, Jr.
DEAN, COLLEGE OF LAW:	Allan W. Vestal

DIRECTOR OF CLE:	Kevin P. Bucknam
ASSISTANT DIRECTOR OF CLE	David L. Kinsella
ADMINISTRATIVE/BUSINESS MANAGER:	Melinda E. Rawlings
EDITORIAL/MARKETING ASSISTANT:	William G. Nims

HEALTH CARE INFORMATION PRIVACY

A "NUTS & BOLTS" WORKSHOP ON HIPAA

AN OVERVIEW OF HIPAA AND COMPLIANCE WITH THE NEW PRIVACY RULES FOR PATIENT HEALTH INFORMATION ..... SECTION A
Douglas L. McSwain
Jennifer C. Philpot

PRIVACY NOTICES, CONSENTS, AND AUTHORIZATIONS ..... SECTION B
Erin Brisbay McMahon

SELECTION OF THE PRIVACY OFFICER AND AN ANALYSIS OF THE PRIVACY OFFICER'S DUTIES ..... SECTION C
Jacqueline C. Kingsolver

THE MINIMUM NECESSARY STANDARD ..... SECTION D
Edward L. Schoenbaechler

HIPAA PRIVACY COMPLIANCE PROGRAMS ..... SECTION E
Vickie Yates Brown

AMENDMENT OF PROTECTED HEALTH INFORMATION ..... SECTION F
Dennis P. Kennedy

BUSINESS ASSOCIATES ..... SECTION G
Carole D. Christian

MARKETING & FUNDRAISING ..... SECTION H
Janet A. Craig
Jennifer L. Elliott

AN OVERVIEW OF HIPAA AND COMPLIANCE WITH THE NEW PRIVACY RULES FOR PATIENT HEALTH INFORMATION

Douglas L. McSwain
and
Jennifer C. Philpot
Sturgill, Turner, Barker & Moloney, PLLC
Lexington, Kentucky

Copyright 2002. Douglas L. McSwain, Jennifer C. Philpot. All rights reserved.

SECTION A

AN OVERVIEW OF HIPAA AND COMPLIANCE WITH THE NEW PRIVACY RULES FOR PATIENT HEALTH INFORMATION

I. INTRODUCTION A-1

A. Health Insurance Portability Act of 1996 ..... A-1

B. Administrative Simplification A-4

C. Why Do We Need HIPAA? A-4

D. Who Does HIPAA Regulate? A-5

E. What Information Is Regulated? A-5

F. When Do I Have To Comply With HIPAA? A-5

II. HOW WILL HIPAA CHANGE MY HEALTH CARE PRACTICE? A-5

A. The Basic Privacy Requirements Of HIPAA A-5

B. "Minimum Information Required" Standard A-7

C. Special Rules For Marketing Or Fundraising Purposes A-8

D. Important Differences Between Consent, Notice, And Authorization A-8

E. Psychotherapy Notes A-9

F. The "Business Associates" Rule A-9

G. Securing Patient Records And Health Information A-10

III. ENFORCEMENT OF HIPAA A-11

A. Generally A-11

B. Civil Monetary Penalties A-12

C. Criminal Penalties A-12

SECTION A

IV. GUIDELINES FOR IMPLEMENTING A HIPAA COMPLIANCE PROGRAM A-12

A. Knowledge A-12

B. Risk Assessment A-12

C. Identify Resources A-12

D. Get Professional Help A-12

E. Name Your Leader A-13

An Overview of HIPAA and Compliance with the New Privacy Rules for Patient Health Information

By

Douglas L. McSwain
and
Jennifer C. Philpot

Sturgill, Turner, Barker & Moloney, PLLC
Lexington, Kentucky

** ** ** ** ** ** ** ** ** ** ** ** ** **

I. INTRODUCTION

A. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§1320d - 1329d-8. How big is the "hippopotamus"? Five (5) Titles long:

1. Title I, Health Care Access, Portability and Renewability

2. Title II, Preventing Fraud and Abuse and Administrative Simplification (the latter of which could be claimed a misnomer)

(A) Subtitle F is the "Administrative Simplification" portion of the Act.

(B) "Administrative Simplification" provisions exist for 3 reasons:

(1) "to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information;"

(2) to improve the quality of care "by restoring

trust in the system" among consumers, providers and others involved in health care delivery;

(3) "to improve the efficiency and effectiveness of health care delivery by creating a national framework for health privacy protection." 65 Fed. Reg. 82642, 82643 (12/28/00).

(C) HIPAA's Administrative Simplification directive is to reduce costs in the health care system by standardizing electronic health care transactions. 42 U.S.C. §1320d-1(b).

(D) With increased electronic transmission of confidential health information, Congress perceived the need to act to protect against the potential of disclosure of private information. HIPAA's Administrative Simplification provisions are intended to address these concerns by providing ***standards***.

(1) E.g., Administrative Simplification requires the establishment of ***privacy standards***; and

(2) Administrative Simplification also requires the establishment of ***security standards***, among other standards.

(E) Status of HIPAA's various components in the promulgation of rules and regulations:

(1) Standards for electronic transactions: final regulations issued 8/17/00 (45 C.F.R. Parts 160 and 162).

(2) National standard health care provider identifier: proposed regulations, subject to public comment, published 5/7/98 (63 Fed. Reg. 25320).

(3) National standard employer identifier: proposed regulations, subject to public comment, published 6/16/98 (63 Fed. Reg. 32784).

(4) Security and electronic signature standards: proposed rules, subject to public comment, published 8/12/98 (63 Fed. Reg. 43242).

(5) Standards for privacy of individually identifiable information: final regulations issued 12/20/00, and effective 4/14/01(45 C.F.R. Parts 160 & 164).

(6) National Health Plan Identifiers: no regulations yet.

(7) Enforcement: no regulations proposed yet.

(8) Claims Attachments: no regulations proposed yet.

(9) National Individual Identifiers: no regulations proposed yet.

3. Title III, Tax-Related Provisions

4. Title IV, Application and Enforcement of Group Health Plan Requirements, and

5. Title V, Revenue Offsets.

B. Administrative Simplification - HIPAA's New Privacy Rules For Patient Health Information: An Overview of HIPAA Privacy Rule Compliance

1. The Final Rules Setting Standards for Privacy of Individually Identifiable Health Information provide the first comprehensive ***federal law*** basis for the protection of privacy and confidentiality of patient health information.

2. The Proposed and Final Rules under HIPAA's Administrative Simplification provisions are primarily concerned with ***STANDARDS***. Standards under HIPAA's Privacy Rule are concerned with safeguarding medical information and providing boundaries for the use of medical information, with accountability for non-compliance.

C. Why do we need HIPAA?

Current law allows the use and transmission of patient identifiable health information for nonmedical purposes. The information can and is used frequently by marketers, lenders, and employers, without patient consent. One study indicated that as many as 35% of Fortune 500 companies evaluate the medical records of their employees prior to making hiring, firing, and promotion decisions.[1]

D. Who does HIPAA regulate?

The final rule applies to Health Plans, health care clearinghouses (such as those which translate or process patient treatment data and codes), and those health care providers who conduct certain financial and administrative transactions, such as electronic billing and fund transfers.

E. What Information is regulated?

All patient medical records, along with any other patient identifiable data that is used or transmitted by a covered entity, regardless of whether transmission occurs electronically, orally, or on paper. The regulated information includes patient billing records, demographic information, and other administrative data that is identified by individual patient.

F. When do I have to comply with HIPAA?

Most health care providers have until April 14, 2003 to fully comply with the HIPAA privacy rules. Small health plans have until April 14, 2004 to comply.

II. How will HIPAA Change my Health Care Practice?

A. The Basic Privacy Requirements of HIPAA

1. HIPAA requires that health care providers obtain patient consent for disclosures of individual health information for purposes of treatment, payment, and other health care operations.[2]

2. In addition to consent, patients must receive notice of the provider's privacy policies, in a form that is distinct from the consent form. This

---

[1] *See* Paul Starr, "Health and the Right to Privacy," American Journal of Law and Medicine, Vol. 25, pp. 193-201 (1999).

[2] An entity covered by HIPAA "may not use or disclose an individual's protected health information ["PHI"] except as otherwise permitted or required by this subpart..." 45 Code of Federal Regulations 164.502(a).

notice must explain how the patient's information will be used and the ways in which it will be protected.

3. Permitted Uses and Disclosures Made with Patient Consent Include:

   a. Those made to the individual patient who is the subject of the information;

   b. Those made with the consent of the patient for purposes of treatment, payment, and health care operations;

   c. Disclosures made for purposes not related to health care, when the patient has given the provider specific authorization for such use.

4. Permitted Uses and Disclosures made without Patient Consent include:

   a. Those made in limited cases, such as emergencies, for purposes of treatment, payment, and health care operations;

   b. Disclosures made without the individual's consent, and when the patient has not affirmatively objected, but has the opportunity to either agree or object prior to disclosure (such as when a provider believes that the patient's family members or caregivers should receive the information);

   c. Those made without consent, when those disclosures are to government agencies for purposes of ensuring compliance with regulatory standards;

   d. Disclosures made in the course of treatment when the provider is legally required to treat the individual;

   e. Disclosures made for purposes of law enforcement (such as pursuant to a subpoena), and that only give the minimum information necessary for enforcement purposes;

   f. Disclosures made to ensure the health and safety of the public, when the provider is reasonably certain that 1) a patient poses an imminent threat to the public, and 2) the person to whom the information is being disclosed can effectively avert or prevent such threatened danger from occurring;

g. Those made when the provider attempted to obtain consent, but was prevented from doing so due to substantial communication barriers with the patient. In such cases, the provider must believe that consent can be inferred from the circumstances;

h. Disclosures made for purposes such as research, as long as the patient data has been de-identified so that it cannot be traced to the individual;

I. Disclosures to public health officials for purposes of preventing or controlling disease, injury, or maintaining birth or death statistics; and

j. Uses and disclosures made when the provider has an **indirect** treatment relationship with the patient, such as when the provider is a laboratory technician or a pathologist. No consent is required in this situation because it is assumed that the patient's primary provider has obtained consent for the use of the information for health care purposes.

B. "Minimum Information Required" Standard

1. Disclosures must be made with the minimum information necessary to accomplish the intended purpose.

2. Requires that providers use their professional judgment and make reasonable efforts to determine the minimum amount of information that can be disclosed.

3. **Does not apply** to disclosures made to another health care provider for treatment purposes, or requests for patient information made by another health care provider for treatment purposes.

4. **Does apply** to all disclosures made for purposes of payment, billing, and other administrative health care operations.

5. **Does not apply** to requests by the individual for his or her own information, or to disclosures to HIPAA enforcement officials.

6. Requires that covered entities develop protocols, procedures, and standards for determining what information is necessary for disclosure, and that they restrict access to use of patient information based on the specific roles of the provider's workforce.

a. Physicians or specialists typically may be given access to the entire medical record;

b. Nurses or other providers might only have access while they are on duty providing care for the individual patient.

7. Allows disclosure of the entire medical record only when there is explicit justification for such wide disclosure by the requesting entity.

C. Special Rules for Marketing or Fundraising Purposes

1. Providers may use personal health information **without patient authorization** under very narrow circumstances:

a. When the marketing is done under the specific name of the provider, and when fundraising is for the provider's own benefit, as long as the materials identify that the provider is the source of the marketing, and state whether the provider is receiving compensation from a third party (such as a drug manufacturer) for the marketing.

b. When the marketing occurs during a face-to-face encounter with the patient for health treatment purposes, such as during a consultation or appointment (including instances in which a provider might suggest that a patient try a certain drug or other specifically named health care product).

c. When the marketing involves products or services of nominal value, such as pens, notepads, or infant formula samples for new or expectant mothers.

d. Fundraising material can only include demographic information and the dates treatment was provided.

2. In all of the foregoing marketing scenarios, the patient must be given the opportunity to "opt out" of receiving future marketing material or promotional items.

D. Important Differences Between Consent, Notice, and Authorization

All providers with direct treatment relationships with patients are responsible for implementing procedures for obtaining patient consent, for offering access to Notice provisions, and obtaining Authorizations when necessary:

1. A Consent document generally gives health care providers who have a direct treatment relationship with the patient permission to use and disclose patient health information for purposes of providing treatment. The Consent must refer to the Notice Document, and specify that the patient has the right to review the entity's privacy practices prior to signing the consent. HIPAA does not require that the individual either read the Notice, or that the entity explain each element of the Notice prior to the time the patient gives Consent. The patient must simply be informed in the Consent that he or she has the right to review the Notice if desired.

2. The Notice document must include a statement of the permitted uses of patient information, the individual's rights, and the entity's legal obligations with regard to ensuring the privacy of the information. The Notice must prominently incorporate the statement, "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please read it carefully." 45 CFR 164.520(b)(1)(i). The Notice must be provided to each patient individually, and also must be posted in the provider's office. Unlike the Consent document, the Notice document only needs to be provided to patients upon their request.

3. Covered entities must obtain Authorizations for all uses and disclosures of patient information that are not for purposes of payment, treatment, or healthcare operations. This Authorization document must be obtained separate from and in addition to the Consent document. Purposes for which an authorization must be obtained include research and release of patient names for marketing purposes that are not otherwise allowed under the HIPAA rules.

E. Psychotherapy Notes

Psychotherapy Notes are subject to a heightened degree of privacy protection under HIPAA. For disclosure or use of such notes, a covered entity must obtain patient authorization for any disclosure that is not for the purpose of treatment by the mental health provider. Such provider may also deny the individual patient access to their own records if, in the professional judgment of the mental health provider, allowing the patient access will be detrimental to the patient. Patient authorization does not have to be obtained from the individual if the provider needs the information for defense of a legal action against the provider brought by the patient.

F. The "Business Associates" Rule

1. A Business Associate is defined under HIPAA as anyone who performs services for a covered entity that involves the use or disclosure of patient information. Examples of Business Associates include lawyers, accountants, billing administrators, and accrediting bodies.

2. Covered entities must do two things when dealing with Business Associates:

   a. Enter into a written contract containing satisfactory assurances that the business associate will safeguard any patient health information it receives from the covered entity. The contract must require the business associate to 1) comply with the terms of the contract for protection of patient health information, and 2) initiate appropriate internal procedures and practices to ensure such compliance.

   b. The terms of the written contract must provide that the relationship between the covered entity and the business associate may be terminated if the covered entity concludes that the business associate has violated the privacy requirements of the contract. Covered entities must then take steps to remedy the violation by the business associate when possible.

3. As long as the disclosure is for treatment purposes, a covered entity is NOT required to enter into a business associate contract with the recipient of the patient information. Treatment is defined under HIPAA as the provision of health care services to an individual by one or more providers, coordination of treatment between providers, and patient referrals for health care services.

G. Securing Patient Records and Health Information

1. HIPAA requires that health care providers design their own plan for securing patient records. The standard is flexible and is intended to allow providers to create and implement a plan that is reasonable for their practice. The requirements allow providers to design compliance programs that are appropriate for the size and scope of their organization. Specific requirements for securing patient information include:

   a. Adopt Written Procedures: Covered entities must develop written polices for designating how patient information will be used within their organization, who will have access to that information, and how and when the information may be disclosed.

b. Train Employees: Providers must ensure that their employees have been appropriately trained regarding HIPAA privacy rules and compliance procedures. All covered entities must designate an employee who will be responsible for implementing and maintaining HIPAA compliance for the organization.

c. Limit Employee Access to Patient Records: Providers must make reasonable efforts to limit access to patient information to their employees based on the roles those employees play within the organization. This may include:

i. Configuring computer data systems in a way that only allows certain employees access to patient information. Providers should develop a password system that allows employees access to no more of the patient's information than is necessary for performance of their job duties.

ii. Securing Patient paper files in an isolated area, out of the view of other patients, and placing all patient files in cabinets that may be locked.

iii. Conduct oral communications with patients in rooms or areas that allow as much privacy as is reasonable for the practitioner. In taking into consideration whether a provider has complied with HIPAA, the Department of Health and Human Services will evaluate all circumstances unique to the provider, including the effect increased privacy protection would have on the quality of care provided.

2. HIPAA does not require that providers physically restructure their work environments, retrofit patient consultation areas, or overhaul computer systems. Instead, the privacy rules are intended to make providers evaluate their organization and implement reasonable safeguards based on the particularities of their organization.

III. Enforcement of HIPAA

A. HIPAA provides civil and criminal penalties for covered entities that improperly disclose patient health information. If a patient or any other individual believes that health information has been improperly used or disclosed, then they may file a complaint with the Office of Civil Rights ("OCR") of the Department for Health and Human Services ("DHHS"). DHHS may then initiate an investigation that may encompass the provider's entire compliance program, in addition to the

circumstances surrounding the Complaint. If such an investigation is initiated, then the provider is required to allow DHHS access to its facilities, books, accounts, and patient information. If DHHS determines that the potential violation is extreme enough, they have the right to gain access to the provider's facility and records at any time and without notice to the provider. 45 CFR 160.310.

B. Civil Monetary Penalties: DHHS has authority to assign providers with monetary penalties up to $100 per violation, and up to $25,000 per year.

C. Criminal Penalties: HIPAA provides for criminal penalties of up to $50,000 and/or imprisonment for up to one year for an entity that knowingly and intentionally violates a privacy rule. The penalty increases to $100,000 and/or imprisonment for up to five years for violations under false pretenses, and increases further to a limit of $250,000 and/or imprisonment for up to ten years for any provider who discloses or uses patient health information with the intent to sell, transfer, or otherwise use the information for commercial gain.

IV. Guidelines for Implementing a HIPAA Compliance Program

A. Knowledge: Develop a working knowledge of HIPAA requirements and how they will affect your practice. Understanding the regulations and knowing what they do require, as well as what they don't require, is the most important factor in initiating HIPAA compliance.

B. Risk Assessment: Conduct an internal risk assessment to evaluate your current health care records and patient information practices. Develop a list of problem areas, and start thinking now about how those problems can be remedied.

C. Identify Resources: There are many Guidance and publications generated by DHHS that are intended to ease the transition into HIPAA compliance. An excellent Guidance in the form of frequently asked questions may be found at http://aspe.os.dhhs.gov/admnsimp/final/pvcguide1.htm. The OCR website offers a mailing list for those who wish to kept informed about developments in the proposed amendments to HIPAA. There are also many computer software programs designed for facilitation of HIPAA compliance.

D. Get Professional Help: Hire a health care lawyer to either assist you in putting together a compliance program, or review the program you eventually implement. Since many of HIPAA's exceptions to the disclosure rules are dependent on the individual facts of the case, the aid of counsel will be instrumental in a good outcome.

E. Name Your Leader: Each covered entity is required to designate an employee who will be responsible for implementing and maintaining HIPAA compliance. The sooner you identify that person, the sooner your organization can integrate patient information practices that facilitate HIPAA Compliance.

PRIVACY NOTICES, CONSENTS, AND AUTHORIZATIONS

Erin Brisbay McMahon
Wyatt, Tarrant & Combs, LLP
Lexington, Kentucky

Copyright 2002. Erin Brisbay McMahon. All rights reserved.

SECTION B

PRIVACY NOTICES, CONSENTS, AND AUTHORIZATIONS

I. CONSENTS B-1

A. General Rule B-1

B. Exceptions B-1

C. May's, Shall's And Shan't's B-2
1. May's B-2
2. Shall's B-2
3. Shan't's B-2

D. So What Does A Consent Have To Look Like? B-3

II. AUTHORIZATIONS B-3

A. Distinction Between Consents And Authorizations B-3

B. Valid Authorizations Must Contain B-5

C. Additional Requirements For Authorizations Requested By A Covered Entity For Its Own Uses And Disclosures B-5

D. Additional Requirements For Authorizations Requested By A Covered Entity For Disclosures By Others B-6

E. Additional Requirements For Authorizations For Uses And Disclosures Of PHI Created For Research That Includes Treatment Of The Individual B-7

F. Authorizations Required For Psychotherapy Notes B-7

G. Resolving Conflicting Consents And Authorizations B-8

H. Compound Authorizations B-8

I. Prohibition On Conditioning Of Authorizations B-9

J. Revoking Authorizations B-10

K. Retention Of Authorizations B-10

L. Uses And Disclosures Requiring An Opportunity For The Individual To Agree Or Object B-10
1. Facility Directories B-10
2. Uses And Disclosures For Involvement In The Individual's Care And Notification Purposes B-11

M. Uses And Disclosures For Which Consent, An Authorization, Or Opportunity For The Individual To Agree Or Object Is Not Required B-12

N. Transition Provisions B-13
1. Effect Of Prior Consents And Authorizations B-13
2. Requirements For Retaining Effectiveness Of Prior Consents And Authorizations B-13

III. NOTICES B-15

A. Relationship Between Consents And Notices B-15

B. Right To Notice B-16
1. General Rule B-16
2. Exceptions B-16
a. Group Health Plans B-16
b. Inmates B-17

C. Required Contents Of Notice B-17

D. Optional Elements Of Notice B-19

E. Revisions To Notice B-20

F. Giving The Notice B-20
1. General Requirement B-20
2. Specific Requirements For Health Plans B-20
3. Specific Requirements For Certain Providers B-20
4. Specific Requirements For Electronic Notices B-21

G. Joint Notices By Separate Covered Entities B-22

H. Documentation And Retention Of Notices B-23

PRIVACY NOTICES, CONSENTS, AND AUTHORIZATIONS

Erin Brisbay McMahon
Wyatt, Tarrant & Combs, LLP
250 West Main St., Suite 1700
Lexington, Kentucky 40507
(859) 288-7452
emcmahon@wyattfirm.com

I. Consents (45 C.F.R. § 164.506)

A. General Rule

Under the Privacy Rule, healthcare **providers** with a "direct treatment relationship" must obtain a ***consent*** from patients to "use" (internal) or "disclose" (to outside persons/entities) protected health information ("PHI") for:

1. treatment (e.g., consultations between healthcare providers relating to a patient or the referral of a patient);
2. payment (e.g., obtaining reimbursement for the provision of health care); or
3. health care operations (i.e., quality assessment and improvement, case management, care coordination and peer review).

Health plans and health care clearinghouses, the other covered entities under the Privacy Rule, may use and disclose PHI for treatment, payment or health care operations ("TPO") without obtaining a consent. They may choose to obtain consents if they wish, but consents must meet the standards for a consent under 45 C.F.R. § 164.506.

B. Exceptions

1. There is an indirect treatment relationship with the patient. An "indirect treatment relationship" exists when a provider delivers health care to the patient based upon the orders of another provider and typically reports to the originating provider. Examples: x-rays, lab work.

2. The provider created or received the PHI in the course of providing health care to an inmate.

Note: In the following three situations, if consent is not obtained, the provider must document the attempt to obtain consent and the reason why consent was not obtained.

3. In emergency treatment situations, if the provider attempts to

obtain consent as soon as reasonably practicable after the delivery of treatment.

4. If the provider is required by law to treat the patient, and attempts to but is unable to obtain consent.

5. If a provider attempts but is unable to obtain consent due to substantial barriers to communicating with the patient, and the provider determines, in the exercise of professional judgment, that the patient's consent to treatment can be clearly inferred from the circumstances.

C. May's, Shall's and Shan't's

1. May's

a. A provider may condition treatment on the provision by the patient of a consent.

b. A health plan may condition enrollment on the provision by an individual of a consent sought in conjunction with enrollment.

c. A consent for may be combined with other types of written legal permission from the individual (e.g., an informed consent for treatment or a consent to assignment of benefits) if the consent is visually and organizationally separate from such other written legal permission and is separately signed and dated.

d. A consent for use or disclosure may be combined with a research authorization under 45 C.F.R. § 164.508(f), as long as the two are visually and organizationally separate and are separately signed and dated.

2. Shall's

a. A covered entity must document and retain any signed consent as required by 45 C.F.R. § 164.530(j), i.e., six years from the date of its creation or the date it was last in effect, whichever is later.

3. Shan't's

a. Consents obtained by one provider are not effective and cannot be used to permit another provider or covered entity to use or disclose the PHI to which the consent form relates.

D. So what does a consent have to look like?

1. Must be in plain language;

2. Be visually and organizationally separate from other written legal permission;

3. Be separately signed and dated by the individual;

4. Inform the individual that PHI may be used and disclosed to carry out treatment, payment, or health care operations;

5. Refer the individual to the notice he or she is entitled to under 45 C.F.R. §164.520 for a more complete description of uses and disclosures and state that the individual has the right to review the notice prior to signing the consent;

6. If the covered entity has reserved the right to change its privacy practices that are described in the notice given to the individual, state that the terms of the privacy notice may change and describe how the individual may obtain a revised notice;

7. State that the individual has the right to request that the covered entity restrict how PHI is used or disclosed to carry out treatment, payment or health care operations;

8. State that the covered entity is not required to agree to requested restrictions by the individual but that, if it does, the agreed-to requested restrictions are binding on the covered entity;

9. State that the individual has the right to revoke the consent in writing, except to the extent that the Covered Entity has taken action in reliance on it.

II. Authorizations (45 C.F.R. § 164.508)

A. Distinction Between Consents and Authorizations

The Department of Health and Human Services Office for Civil Rights, which is in charge of enforcing the Privacy Rule, issued a guidance paper on the Privacy Rule on July 6, 2001. The guidance paper may be found at http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm. It contained the following explanation of the difference between a consent and an authorization:

> A consent is a general document that gives health care

providers, which have a direct treatment relationship with a patient, permission to use and disclose all PHI for TPO. It gives permission only to that provider, not to any other person. Health care providers may condition the provision of treatment on the individual providing this consent. One consent may cover all uses and disclosures for TPO by that provider, indefinitely. A consent need not specify the particular information to be used or disclosed, nor the recipients of disclosed information.

Only doctors or other health care providers with a direct treatment relationship with a patient are required to obtain consent. Generally, a "direct treatment provider" is one that treats a patient directly, rather than based on the orders of another provider, and/or provides health care services or test results directly to patients. Other health care providers, health plans, and health care clearinghouses may use or disclose information for TPO without consent, or may choose to obtain a consent.

An authorization is a more customized document that gives covered entities permission to use specified PHI for specified purposes, which are generally other than TPO, or to disclose PHI to a third party specified by the individual. Covered entities may not condition treatment or coverage on the individual providing an authorization. An authorization is more detailed and specific than a consent. It covers only the uses and disclosures and only the PHI stipulated in the authorization; it has an expiration date; and, in some cases, it also states the purpose for which the information may be used or disclosed.

An authorization is required for use and disclosure of PHI not otherwise allowed by the rule. In general, this means an authorization is required for purposes that are not part of TPO and not described in § 164.510 (uses and disclosures that require an opportunity for the individual to agree or to object) or § 164.512 (uses and disclosures for which consent, authorization, or an opportunity to agree or to object is not required). . . .

All covered entities, not just direct treatment providers, must obtain an authorization to use or disclose PHI for these purposes. For example, a covered entity would need an authorization from individuals to sell a patient mailing list, to disclose information to an employer for employment decisions, or to disclose information for eligibility for life

insurance. A covered entity will never need to obtain both an individual's consent and authorization for a single use or disclosure. However, a provider may have to obtain consent and authorization from the same patient for different uses or disclosures. For example, an obstetrician may, under the consent obtained from the patient, send an appointment reminder to the patient, but would need authorization from the patient to send her name and address to a company marketing a diaper service.

B. Valid Authorizations Must Contain:

1. A description of the information to be used or disclosed that specifically and meaningfully identifies the information;

2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;

3. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure;

4. An expiration date or event that relates to the individual or the purpose of the use or disclosure;

5. A statement of the individual's right to revoke the authorization in writing and the exceptions of the right to revoke, together with a description of how to revoke the authorization;

6. A statement that the information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by this rule;

7. Signature of the individual and the date;

8. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual; and

9. The authorization must be written in plain language.

C. Additional Requirements for Authorizations Requested by a Covered Entity for Its Own Uses and Disclosures

If an authorization is requested by a covered entity for its own use or disclosure of PHI that it maintains, the covered entity's authorization must comply with the following:

1. requirements II.B.1-9 above for a valid authorization;

2. a statement that the covered entity will not condition treatment, payment, enrollment in a health plan, or eligibility for benefits on the individual's agreement to authorize the requested use or disclosure, but only if the authorization is one to which 45 C.F.R. 164.508(b)(4)'s prohibition on conditioning applies;

3. a description of each purpose of the requested use or disclosure;

4. a statement that the individual may:

   a. inspect or copy the PHI to be used or disclosed as provided in 45 C.F.R. § 164.524; and

   b. refuse to sign the authorization;

5. if use or disclosure of the requested information will result in direct or indirect remuneration to the covered entity from a third party, a statement that such remuneration will result; and

6. the covered entity must provide the individual with a copy of the signed authorization.

D. Additional Requirements for Authorizations Requested by a Covered Entity for Disclosures by Others

If an authorization is requested by a covered entity for another covered entity to disclose PHI to the covered entity requesting the authorization to carry out TPO, the covered entity requesting the authorization must comply with the following requirements:

1. requirements II.B.1-9 above for a valid authorization;

2. a description of each purpose of the requested use or disclosure;

3. except for an authorization on which payment may be conditioned under 45 C.F.R. § 164.508(b)(4)(iii), a statement that the covered entity will not condition treatment, payment, enrollment in a health plan, or eligibility for benefits on the individual's providing authorization for the requested use or disclosure;

4. a statement that the individual may refuse to sign the authorization; and

5. the covered entity must provide the individual with a copy of the

signed authorization.

E. Additional Requirements for Authorizations for Uses and Disclosures of PHI Created for Research That Includes Treatment of the Individual.

Except as otherwise permitted by 45 C.F.R. § 164.512(i), a covered entity that creates PHI for the purpose, in whole or in part, of research that includes treatment of individuals must obtain an authorization for the use or disclosure of such information. Such authorization must:

1. for uses and disclosures not otherwise permitted or required under Subpart E of the Privacy Rule, meet the requirements of II.B. and II.C;

2. contain a description of the extent to which such PHI will be used or disclosed to carry out TPO;

3. contain a description of any PHI that will not be used or disclosed for purposes permitted in accordance with 45 C.F.R. §§ 164.510 and 164.512, provided that the covered entity may not include a limitation affecting its right to make a use or disclosure required by law or permitted by 45 C.F.R. § 164.512(j)(1)(i); and

4. if the covered entity has obtained or intends to obtain the individual's consent under 45 C.F.R. § 164.506, or has provided or intends to provide the individual with a notice under 45 C.F.R. § 164.520, the authorization must refer to that consent or notice, as applicable, and state that the statements made pursuant to 45 C.F.R. § 164.508 are binding.

This type of authorization may be in the same document as a consent to participate in the research, a consent to use or disclose PHI to carry out TPO, or a notice of privacy practices.

F. Authorizations Required for Psychotherapy Notes

Notwithstanding any other provisions of subpart E of the Privacy Rule other than the transition provisions in 45 C.F.R. § 164.532, a covered entity must obtain an authorization for any use or disclosure of psychotherapy notes, except:

1. To carry out the following TPO consistent with the consent requirements of 45 C.F.R. § 164.506:

    a. use by the originator of psychotherapy notes for treatment;

b. use or disclosure by the covered entity in training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

c. use or disclosure by the covered entity to defend a legal action or other proceeding brought by the individual; and

2. A use or disclosure that is required by 45 C.F.R. § 164.502(a)(2)(ii) or permitted by 45 C.F.R. § 164.512(a); 45 C.F.R. § 164.512(d) with respect to the oversight of the originator of the psychotherapy notes; 45 C.F.R. § 164.512(g)(1); or 45 C.F.R. § 164.512(j)(1)(i).

Note that this provision means that a provider would need to obtain authorization and not consent to use or disclose PHI maintained in psychotherapy notes for treatment by persons other than the originator of the notes, for payment, or for health care operations purposes, except as specified in the Privacy Rule (§ 164.508(a)(2)).

G. Resolving Conflicting Consents and Authorizations

1. If a covered entity has obtained a consent under 45 C.F.R. § 164.506 and receives any other authorization or written legal permission from the individual for a disclosure of PHI to carry out TPO, the covered entity may disclose such PHI only in accordance with the more restrictive consent, authorization, or other written legal permission from the individual.

2. A covered entity may attempt to resolve a conflict between a consent and an authorization or other written legal permission from the individual described in paragraph 1 of this section by:

   a. Obtaining a new consent from the individual under 45 C.F.R. § 164.506 for the disclosure to carry out TPO; or

   b. Communicating orally or in writing with the individual in order to determine the individual's preference in resolving the conflict. The covered entity must document the individual's preference and may only disclose PHI in accordance with the individual's preference.

H. Compound Authorizations

An authorization may not be combined with any other document to create a compound authorization, except as follows:

1. An authorization for the use or disclosure of PHI created for

research that includes treatment of the individual may be combined as permitted by 45 C.F.R. § 164.506(b)(4)(ii) or 45 C.F.R. § 164.508(f);

2. An authorization for the use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

3. An authorization, other than an authorization for the use or disclosure of psychotherapy notes, may be combined with any other authorization, except when a covered entity has conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits under § 164.508(b)(4) on the provision of one of the authorizations.

I. Prohibition on Conditioning of Authorizations

A covered entity may not condition the provision to an individual of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except:

1. A provider may condition the provision of research-related treatment on the provision of an authorization under 45 C.F.R. § 164.508(f);

2. A health plan may condition enrollment in the health plan or eligibility for benefits on provision of an authorization requested by the health plan prior to an individual's enrollment in the health plan, if:

   a. the authorization sought is for the health plan's eligibility or enrollment determinations relating to the individual or for its underwriting or risk rating determinations; and

   b. the authorization is not for a use or disclosure of psychotherapy notes;

3. A health plan may condition payment of a claim for specified benefits on provision of an authorization under 45 C.F.R. § 164.508(e) if:

   a. the disclosure is necessary to determine payment of such claim; and

   b. the authorization is not for a use or disclosure of psychotherapy notes; and

4. A covered entity may condition the provision of health care that is

solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to the third party.

J. Revoking Authorizations

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

1. the covered entity has taken action in reliance on it; or

2. if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy.

K. Retention of Authorizations

A covered entity must document and retain any signed authorization as required by 45 C.F.R. § 164.530(j), i.e., six years from the date of its creation or the date it was last in effect, whichever is later.

L. Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object (45 C.F.R. § 164.510)

A covered entity may use or disclose PHI without the written consent or authorization of the individual provided that the individual is informed in advance of the use or disclosure and has the opportunity to agree to or prohibit or restrict the disclosure in accordance with the applicable requirements of 45 C.F.R. § 164.510. The covered entity may orally inform the individual of and obtain the individual's oral agreement or objection to a use or disclosure permitted by 45 C.F.R. § 164.510.

1. Facility Directories

a. Except when an objection is expressed, a provider may use the following PHI to maintain a directory of individuals in its facility:

   i. the individual's name;
   ii. the individual's location in the facility;
   iii. the individual's condition described in general terms that does not communicate specific medical information about the individual; and
   iv. the individual's religious affiliation.

b. Except when an objection is expressed, the provider may

disclose for directory purposes the information in (a) above to:

i. members of the clergy; or
ii. except for religious affiliation, to other persons who ask for the individual by name.

c. A provider must inform an individual of the PHI it may include in a directory and the persons to whom it may disclose such PHI and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures permitted by (a) and (b) above. If the opportunity to object cannot practicably be provided because of the individual's incapacity or an emergency treatment situation, a provider may use or disclose some or all of the PHI permitted by (a) above, if such disclosure is:

i. consistent with a prior expressed preference of the individual, if any, that is known to the provider; and

ii. in the individual's best interest as determined by the provider in the exercise of professional judgment.

The provider must inform the individual of the uses and disclosures made during the individual's incapacity or an emergency treatment situation when it becomes practicable to do so and must give the individual an opportunity to object to further uses or disclosures for directory purposes at that time.

2. Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes.

a. A covered entity may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.

b. A covered entity may use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Any such use or disclosure of PHI for such notification purposes must be in accordance with paragraphs (c), (d), or

(e) below, as applicable.

c. If the individual is present for, or otherwise available prior to, a use or disclosure permitted by paragraph (a) or (b) above and has the capacity to make health care decisions, the covered entity may use or disclose the PHI if it:

   i. Obtains the individual's agreement;

   ii. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

   iii. Reasonably infers from the circumstances, based the exercise of professional judgment, that the individual does not object to the disclosure.

d. If the individual is not present, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the covered entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual and, if so, disclose only the PHI that is directly relevant to the person's involvement with the individual's health care. A covered entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

e. A covered entity may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted by paragraph (b) above. The requirements in paragraphs (c) and (d) above apply to such uses and disclosures to the extent that the covered entity, in the exercise of professional judgment, determines that the requirements do not interfere with the ability to respond to the emergency circumstances.

M. Uses and Disclosures for which Consent, an Authorization, or Opportunity for the Individual to Agree or Object Is Not Required (45 C.F.R. § 164.512)

Note: This section does not explore this particular regulation in depth, as parts of it will be addressed by other speakers. This section consumes 6 pages of the Federal Register; therefore, please consult the regulation for

detailed requirements concerning the listed exceptions.

1. Uses and disclosures required by law
2. Uses and disclosures for public health activities
3. Disclosures about victims of abuse, neglect, or domestic violence
4. Uses and disclosures for health oversight activities
5. Disclosures for judicial and administrative proceedings
6. Disclosures for law enforcement purposes
7. Uses and disclosures about decedents
8. Uses and disclosures for cadaveric organ, eye, or tissue donation purposes
9. Uses and disclosures for research purposes
10. Uses and disclosures to avert a serious threat to health or safety
11. Uses and disclosures for specialized government functions
12. Disclosures for workers' compensation

N. Transition Provisions (Prior Consents and Authorizations - 45 C.F.R. § 164.532)

1. Effect of prior consents and authorizations.

A covered entity may continue to use or disclose PHI pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of PHI that does not comply with 45 C.F.R. §§ 164.506 or 164.508 consistent with paragraph 2 of this section.

2. Requirements for retaining effectiveness of prior consents and authorizations.

The following provisions apply to use or disclosure by a covered entity of PHI pursuant to a consent, authorization, or other express legal permission obtained from an individual permitting the use or disclosure of PHI, if the consent, authorization, or other express legal permission was obtained from an individual before the applicable compliance date of the Privacy Rule and does not

comply with 45 C.F.R. §§ 164.506 or 164.508.

a. If the consent, authorization, or other express legal permission obtained from an individual permits a use or disclosure for purposes of carrying out TPO, the covered entity may, with respect to PHI that it created or received before the applicable compliance date of the Privacy Rule and to which the consent, authorization, or other express legal permission obtained from an individual applies, use or disclose such information for purposes of carrying out TPO, provided that:

   i. The covered entity does may not make any use or disclosure that is expressly excluded from the a consent, authorization, or other express legal permission obtained from an individual; and

   ii. The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

b. If the consent, authorization, or other express legal permission obtained from an individual specifically permits a use or disclosure for a purpose other than to carry out TPO, the covered entity may, with respect to PHI that it created or received before the applicable compliance date of the Privacy Rule and to which the consent, authorization, or other express legal permission obtained from an individual applies, make such use or disclosure, provided that:

   i. The covered entity does not make any use or disclosure that is expressly excluded from the consent, authorization, or other express legal permission obtained from an individual; and

   ii. The covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

c. In the case of a consent, authorization, or other express legal permission obtained from an individual that identifies a specific research project that includes treatment of individuals:

   i. If the consent, authorization, or other express legal

permission obtained from an individual specifically permits a use or disclosure for purposes of the project, the covered entity may, with respect to PHI that it created or received either before or after the applicable compliance date of the Privacy Rule and to which the consent or authorization applies, make such use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

ii. If the consent, authorization, or other express legal permission obtained from an individual is a general consent to participate in the project, and a covered entity is conducting or participating in the research, such covered entity may, with respect to PHI that it created or received as part of the project before or after the applicable compliance date of the Privacy Rule, make a use or disclosure for purposes of that project, provided that the covered entity complies with all limitations placed by the consent, authorization, or other express legal permission obtained from an individual.

d. If, after the applicable compliance date of the Privacy Rule, a covered entity agrees to a restriction requested by an individual under 45 C.F.R. § 164.522(a), a subsequent use or disclosure of PHI that is subject to the restriction based on a consent, authorization, or other express legal permission obtained from an individual as given effect by this section, must comply with such restriction.

III. Notices (45 C.F.R. § 164.520)

A. Relationship Between Consents and Notices

When asked to explain the interrelationship between consents and notices, the Department of Health and Human Services Office for Civil Rights, which is in charge of enforcing the Privacy Rule, answered as follows in a guidance paper on the Privacy Rule on July 6, 2001:

> The consent and the notice of privacy practices are two distinct documents. A consent document is brief (may be less than one page). It must refer to the notice and must inform the individual that he [or she] has the opportunity to review the notice prior to signing the consent. The Privacy Rule does not require that the individual read the notice or

that the covered entity explain each item in the notice before the individual provides consent. We expect that some patients will simply sign the consent while others will read the notice carefully and discuss some of the practices with the covered entity.

B. Right to Notice

1. General Rule

An individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the covered entity, and of the individual's rights and the covered entity's legal duties with respect to protected health information.

2. Exceptions

a. Group Health Plans

i. An individual enrolled in a group health plan has a right to notice:

(A) From the group health plan, if, and to the extent that, such an individual does not receive health benefits under the group health plan through an insurance contract with a health insurance issuer or HMO; or

(B) From the health insurance issuer or HMO with respect to the group health plan through which such individuals receive their health benefits under the group health plan.

ii. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and that creates or receives PHI in addition to summary health information as defined in 45 C.F.R. § 164.504(a) or information on whether the individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, must:

(A) Maintain a notice under this section; and

(B) Provide such notice upon request to any person. The provisions of 45 C.F.R. §

164.520(c)(1) do not apply to such group health plan.

iii. A group health plan that provides health benefits solely through an insurance contract with a health insurance issuer or HMO, and does not create or receive PHI other than summary health information as defined in 45 C.F.R. § 164.504(a) or information on whether an individual is participating in the group health plan, or is enrolled in or has disenrolled from a health insurance issuer or HMO offered by the plan, is not required to maintain or provide a notice under this section.

b. Inmates

An inmate does not have a right to a notice of privacy practices, and the requirements of 45 C.F.R. § 164.520 do not apply to a correctional institution that is a covered entity.

C. Required Contents of Notice

The notice must be written in plain language and must contain the following elements:

1. the following statement as a header or otherwise prominently displayed: "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."

2. A description, including at least one example, of the types of uses and disclosures that the covered entity is permitted by Subpart E of the Privacy Rule to make for each of the following purposes: treatment, payment, and health care operations. If a use or disclosure for any purpose described is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the "more stringent" law as that term is defined in 45 C.F.R. §160.202. For each purpose described, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by Subpart E of the Privacy Rule and other applicable law.

3. A description of each of the other purposes for which the covered entity is permitted or required by Subpart E of the Privacy Rule to use or disclose PHI without the individual's written consent or

authorization. If a use or disclosure for any purpose described is prohibited or materially limited by other applicable law, the description of such use or disclosure must reflect the "more stringent" law as that term is defined in 45 C.F.R. §160.202. For each purpose described, the description must include sufficient detail to place the individual on notice of the uses and disclosures that are permitted or required by Subpart E of the Privacy Rule and other applicable law.

4. A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such authorization as provided by 45 C.F.R. § 164.508(b)(5).

5. If the covered entity intends to engage in any of the following activities, the description required by paragraph 2 above must include a separate statement, as applicable, that:

   a. The covered entity 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;

   b. The covered entity may contact the individual to raise funds for the covered entity; or

   c. A group health plan, or a health insurance issuer or HMO with respect to a group health plan, may disclose protected health information to the sponsor of the plan.

6. A statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

   a. The right to request restrictions on certain uses and disclosures of PHI as provided by 45 C.F.R. § 164.522(a), including a statement that the covered entity is not required to agree to a requested restriction;

   b. The right to receive confidential communications of PHI as provided by 45 C.F.R. § 164.522(b), as applicable;

   c. The right to inspect and copy PHI as provided by 45 C.F.R. § 164.524;

   d. The right to amend PHI as provided by 45 C.F.R. § 164.526;

e. The right to receive an accounting of disclosures of PHI as provided by 45 C.F.R. § 164.528; and

f. The right of an individual, including an individual who has agreed to receive the notice electronically in accordance with paragraph 45 C.F.R. § 164.520(c)(3), to obtain a paper copy of the notice from the covered entity upon request.

7. A statement that the covered entity is 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;

8. A statement that the covered entity is required to abide by the terms of the notice currently in effect;

9. For the covered entity to change a practice described in the notice to PHI that the covered entity created or received prior to issuing a revised notice, in accordance with 45 C.F.R. § 164.530(i)(2)(ii), a statement that it reserves the right to change the terms of its notice and to make the new notice provisions effective for all PHI it maintains. The covered entity must also describe how it will provide individuals with a revised notice;

10. A statement that individuals may complain to the covered entity and to 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 the covered entity, and a statement that the individual will not be retaliated against for filing a complaint.

11. The name, or title, and telephone number of a person or office to contact for further information as required by 45 C.F.R. § 164.530 (a)(1)(ii).

12. The date on which the notice is first in effect, which may not be earlier than the date on which the notice is printed or otherwise published.

D. Optional Elements of Notice

If a covered entity elects to limit the uses or disclosures that it is permitted to make under Subpart E of the Privacy Rule, the covered entity may describe its more limited uses or disclosures in its notice, provided that the covered entity may not include in its notice a limitation affecting its right to make a use or disclosure that is required by law or permitted by 45 C.F.R. § 164.512(j)(1)(i). For the covered entity to apply a change in its more limited uses and disclosures to PHI created or received prior to

issuing a revised notice, in accordance with 45 C.F.R. § 164.530(i)(2)(ii), the notice must include the statements required by paragraph 9 above.

E. Revisions to Notice

The covered entity must promptly revise and distribute its notice whenever there is a material change to the uses or disclosures, the individual's rights, the covered entity's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected.

F. Giving the Notice

1. General Requirement

A covered entity must make the notice required by the Privacy Rule available on request to any person.

2. Specific Requirements for Health Plans

a. A health plan must provide notice:

i. No later than the compliance date for the health plan, to individuals then covered by the plan;

ii. Thereafter, at the time of enrollment, to individuals who are new enrollees; and

i. Within 60 days of a material revision to the notice, to individuals then covered by the plan.

b. No less frequently than once every three years, the health plan must notify individuals then covered by the plan of the availability of the notice and how to obtain the notice.

c. The health plan satisfies the requirements of this section if notice is provided to the named insured of a policy under which coverage is provided to the named insured and one or more dependents.

d. If a health plan has more than one notice, it satisfies the requirements of this section by providing the notice that is relevant to the individual or other person requesting the notice.

3. Specific Requirements for Certain Providers

A covered health care provider that has a direct treatment relationship with an individual must:

a. Provide the notice no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the provider;

b. If the provider maintains a physical service delivery site:

   i. Have the notice available at the service delivery site for individuals to request to take with them; and

   ii. Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider to be able to read the notice; and

c. Whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the requirements of paragraph (b) immediately above, if applicable.

4. Specific Requirements for Electronic Notices

a. A covered entity that maintains a web site that provides information about the covered entity's customer services or benefits must prominently post its notice on the web site and make the notice available electronically through the web site.

b. A covered entity may provide the notice required by this section to an individual by e-mail, if the individual agrees to electronic notice and such agreement has not been withdrawn. If the covered entity knows that the e-mail transmission has failed, a paper copy of the notice must be provided to the individual. Provision of electronic notice by the covered entity will satisfy the provision requirements of 45 C.F.R. § 164.520(c) when timely made in accordance with the rules governing specific requirements for notices given by health plans or the rules governing specific requirements for notices given by providers listed above.

c. For purposes of paragraph (3)(a) above, if the first service delivery to an individual is delivered electronically, the covered health care provider must provide electronic notice automatically and contemporaneously in response to the

individual's first request for service.

d. The individual who is the recipient of electronic notice retains the right to obtain a paper copy of the notice from a covered entity upon request.

G. Joint Notices by Separate Covered Entities

Covered entities that participate in organized health care arrangements may comply with 45 C.F.R. § 164.520 by a joint notice, provided that:

1. The covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to PHI created or received by the covered entity as part of its participation in the organized health care arrangement;

2. The joint notice meets the implementation specifications in III.C., except that the statements required by that section may be altered to reflect the fact that the notice covers more than one covered entity; and

   a. Describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies;

   b. Describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and

   c. If applicable, states that the covered entities participating in the organized health care arrangement will share PHI with each other, as necessary to carry out TPO relating to the organized health care arrangement.

3. The covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of III.F. Provision of the joint notice to an individual by any one of the covered entities included in the joint notice will satisfy the provision requirement of III.F. with respect to all others covered by the joint notice.

Note: Covered entities that participate in an organized health care arrangement and have a joint notice may use a joint consent form. A joint consent must:

- Include the name or other specific identification of the covered entities, or classes of covered entities, to which the joint consent applies; and

- Meet the requirements of 45 C.F.R. § 164.506, except that the statements required by that section may be altered to reflect the fact that the consent covers more than one covered entity.

If an individual revokes a joint consent, the covered entity that receives the revocation must inform the other entities covered by the joint consent of the revocation as soon as is practicable. See 45 C.F.R. § 164.506(f).

H. Documentation and Retention of Notices

A covered entity must document compliance with the notice requirements by retaining copies of the notices issued by the covered entity as required by § 164.530(j), i.e., six years from the date of the creation of the notice or the date it was last in effect, whichever is later.

SELECTION OF THE PRIVACY OFFICER AND AN ANALYSIS OF THE PRIVACY OFFICER'S DUTIES

Jacqueline C. Kingsolver
Associate General Counsel
Norton Healthcare
Louisville, Kentucky

Copyright 2002. Jacqueline C. Kingsolver. All rights reserved.

SECTION C

SELECTION OF THE PRIVACY OFFICER AND AN ANALYSIS OF THE PRIVACY OFFICER'S DUTIES

I. Requirements Of HIPAA Regulations C-1

II. Selection Of The Privacy Officer C-1

A. Who is the Privacy Officer? C-2
B. What Are the Criteria for the Job? C-3
C. What are Reasonable Expectations of the Privacy Officer? C-4

III. Responsibilities Of The Privacy Officer C-4

A. Regulations C-4
1. Development of Privacy Policies C-5
2. Other Initial Tasks C-5
3. Follow-Up Responsibilities C-6

B. Additional Responsibilities C-7
1. Other HIPAA Obligations C-7

C. Looking Ahead C-9

Additional Resources C-11

SELECTION OF THE PRIVACY OFFICER AND AN ANALYSIS OF THE PRIVACY OFFICER'S DUTIES

March 15, 2002

Jacqueline C. Kingsolver
Associate General Counsel
Norton Healthcare
Louisville, Kentucky

I. Requirements of HIPAA Regulations

A. Section 164.530(a)(1) of the HIPAA regulations provides as follows:

Standard: personnel designations. (i) a covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.

B. Section (2) of the same regulation provides:

Implementation specification: personnel designations. A covered entity must document the personnel designations in paragraph (a)(1) of this section as required by paragraph (j) of this section.

C. Paragraph (j)(1) of this same regulation provides:

Standard: documentation. A covered entity must:

(i) . . .

(ii) . . .

(iii) If an action, activity, or designation is required by this subpart to be documented, maintain a written or electronic record of such action, activity or designation.

D. Paragraph (j)(2) of the same regulation provides:

Implementation specification: retention period. A covered entity must retain the documentation required by paragraph (j)(1) of this section for six years from the date of its creation or the date when it last was in effect, whichever is later.

II. Selection of the Privacy Officer

A. Who Is the Privacy Officer? In much the same fashion as the compliance officer of an entity, the privacy officer holds a position which serves the entire entity and is a front line of defense to assure the entity is meeting its obligations under the law. The federal regulations do not include a job description for the privacy officer.

1. The comments to the federal regulations [65 FR 82462, *82744, (December 28, 2000)] acknowledge that the privacy officer role may be an additional responsibility given to an existing employee, such as an office manager in a small entity (a physician's office), or an information officer, or even the compliance officer. In smaller organizations, this will be the most likely arrangement. It should be noted, however, that the HIPAA-required information security officer role is not compatible with that of the privacy officer, and may not be a natural fit when combining roles. The security officer is responsible for assuring the technical security of confidential information and, as a rule, will be drawn from persons with expertise in information systems. This person may not have the familiarity with actual patient records or processes for amending them or handling patient complaints regarding their confidential information. The privacy officer should have an understanding of the organization's operations (like medical records processes).

2. The comments do point out, however, that the privacy officer role must serve as the single focal point for accountability. While the duties may be delegated and shared, the single focal point must be established. Multi-facility organizations may elect to have a single privacy officer, but identify a contact person at each facility, such as the chief nursing officer or the health information director, to handle patient requests to obtain copies of their records, or to amend their records, as well as to coordinate complaints associated with the use of confidential patient information. Staff on site at the facilities will be better able to address such matters in a timely manner than an off-site privacy officer.

3. Likewise, the comments to the regulations acknowledge that the privacy officer at one covered entity may also serve as the privacy officer at another covered entity, so long as each entity otherwise meets the requirements of the regulations.

4. The comments to the regulations acknowledge that entities with multiple subsidiaries which meet the definition of "covered entity" do not need to have a separate privacy officer for each such subsidiary if they are designated by the entity as part of a single covered entity. The rules permit such a designation to be made [see Section 164.504 (b) for the rules relating to this designation]. If only one covered

entity is designated for the subsidiaries, only one privacy officer is needed.

5. The privacy officer must be a member of or have ready, unfettered access to senior management as the leader of the organization's privacy program, in the same manner as does the compliance officer. This access is necessary to assure the privacy officer's authority in the organization is sufficient to enable him/her to coordinate the various departments' responses to privacy issues and to oversee the ongoing enforcement of privacy policies and education of staff. This authority is especially essential in the relationship between the privacy officer and medical staff members and enhances the privacy officer's ability to inform and educate the governing board about privacy responsibilities and the financial obligations associated with meeting HIPAA requirements. This may involve a direct reporting relationship to the chief executive officer, the chief financial officer, a committee of the organization's governing board, or the managing partner in a practice group. A reporting relationship to the compliance officer could also be established for the privacy officer.

B. What Are the Criteria for the Job?

1. Facilities which are hiring to fill the newly-established position of privacy officer must determine the educational and experience requirements for the position. Even facilities which will not create a new position of privacy officer must evaluate the qualifications of those to whom the additional tasks of privacy officer are to be assigned and select someone who has requisite skills.

2. Educational background can include persons with public health degrees, medical ethics, law, or health administration, nursing or other terminal degrees. Research and academic facilities may prefer candidates who have degrees in particular fields of science, in addition to the other noted degrees.

3. Relevant experience should include health care administrative experience, excellent oral and written communications and organizational skills. An important attribute in the role of privacy officer will be the ability to work collaboratively with others as well as the ability to problem-solve. The ability to understand, interpret, implement and communicate federal regulations is also critical. If the responsibility for education of the facility workforce on HIPAA is not delegated, then the privacy officer should be experienced in training or public speaking and in the development of training materials. The privacy officer should also be able to manage the budget allocated for privacy compliance efforts.

4. Privacy officers should be capable of assuming their role quickly, as there is a steep learning curve associated with the position. In the context of both education of staff and interface with management and the board, the privacy officer should be capable of handling issues as they develop and exercising authority.

5. Salary ranges for privacy officers will vary widely, according to the size of the organization and the position of the privacy officer within the organization. A reasonable comparison would be to the salary of the entity's compliance officer.

C. What are Reasonable Expectations of the Privacy Officer?

1. To enable the privacy officer to accomplish the assigned tasks, the entity must assure that the officer has the support of the governing board and management. This support involves not only financial support to meet HIPAA requirements, but also the means to access top level decision makers. Board members and senior management must be informed about the requirements of HIPAA and the role the privacy officer is obligated to play in meeting those requirements. Minutes of governing board meetings should reflect that the privacy program of the entity has been explained to the board and its overall direction approved and should reflect board approval of the job description for the privacy officer and may also include actual approval of the person selected for that position, to comply with the documentation requirements of Section j(1) noted above. Individual policies to support its implementation do not require board approval, however.

2. The governing board should also clarify that the privacy officer, when acting in that capacity on behalf of the entity, is covered by the entity's directors and officers liability insurance coverage. The HIPAA regulations do not assign personal liability to the privacy officer for violations, although the entity can be subject to fines. Under the criminal liability provisions of the law, the risk of personal liability is greater since an organization cannot be held criminally liable. Such occurrences would be rare, however, as in when a person takes confidential patient information and sells it for profit. So long as the privacy officer acts under the auspices and direction of the governing board, there should not be personal liability attributable to the officer.

III. Responsibilities of the Privacy Officer

A. Regulations. The regulations, and the accompanying commentary, charge the privacy officer with serving as the central point of accountability within each

covered entity for privacy-related issues.

1. Development of Privacy Policies.

   a. Creation of privacy policies requires an initial assessment of the entity's existing policies-what does it already have in place which relates to confidentiality and privacy of patient information and which can be modified to meet HIPAA requirements? What gaps need to be filled with new policies and procedures? The privacy officer should lead this initial assessment.

   b. The privacy officer should bring together internal resources of the entity, those with a stake in the handling of patient information, as a task force or committee. Those stakeholders include representatives of health information systems, human resources, information systems, legal, operations, nursing, finance, risk management, marketing, fund-raising, security, and public relations.

   c. The privacy office, as head of this task force, should have the authority to facilitate integration between the various stakeholders in the organization as they jointly develop the necessary policies and procedures.

   d. The privacy officer must also be familiar with any applicable state laws which impact privacy and how they must be correlated with HIPAA's requirements in the entity's policies and procedures.

2. Other Initial Tasks

   a. Either through the assistance of task force members or, in smaller entities, on his/her own, the privacy officer is responsible for such initial tasks as developing an inventory of the locations in the entity where patient information is received, generated, stored and transmitted. Such locations can include billing databases, personal computers and handheld computers, and medical records transcription sites.

   b. Another start-up responsibility is the development of the facility's own Privacy Notice, as required under the HIPAA regulations. This notice should identify the privacy officer and other privacy contacts at the entity, so patients can obtain additional information or make requests permitted under HIPAA regarding the handling and release of their confidential information. The regulations outline the basic required elements of the notice, but many optional areas exist which the privacy officer must review and determine how the facility will respond. For example, HIPAA offers facilities the opportunity to release information to law enforcement officials

which may be more liberal in approach than the existing approach of many facilities. The privacy officer must lead the entity through an analysis of its current practices and determine whether it wants to broaden or narrow its policies on release of information to law enforcement agencies. This can involve an evaluation of the entity's ongoing need for a good relationship with law enforcement agencies and the public as balanced with the obligations to respect and protect the privacy of patient information. This policy must be addressed in the Privacy Notice.

c. Under the privacy officer's direction, the entity must prepare to educate its workforce in HIPAA requirements for confidentiality of patient information. This includes orientation for new employees and training of existing personnel. Of equal importance will be education of physicians and other health care practitioners who routinely require access to confidential patient information maintained by the entity and of the governing body of the entity, which is ultimately responsible for assuring compliance with HIPAA requirements. Facilities with medical directors should include this position in any HIPAA task force or committee to coordinate educational efforts to the medical staff.

d. Identification of current business associates of the entity is an additional initial responsibility of the privacy officer. Inventories are necessary of existing agreements to determine what contracts are in place, who has copies of them, which arrangements have not been memorialized in writing, which arrangements meet the regulatory definitions of business associate arrangements, and which will require amendments or new contracts to accommodate the business associate regulations. The privacy officer may develop standard language to be incorporated into amendments to existing agreements and in new agreements as they are developed.

e. The privacy officer will also be accountable for performing a gap analysis which identifies those areas in which compliance with HIPAA has not yet been met and the assignment of personnel and resources necessary to bridge those gaps in compliance. Parts of this gap analysis will involve assessing existing policies, procedures and practices on the creation, use, storage and release of patient health information.

3. Follow-up Responsibilities

a. Once the initial inventory responsibilities have been completed, the privacy officer must oversee the implementation of policies.

b. As new arrangements are entered into by the entity with third

parties which will require access to protected patient information, the privacy officer will be responsible for reviewing these arrangements for compliance with HIPAA requirements.

c. The privacy officer will have ongoing responsibility for monitoring and auditing entity activities and polices for compliance with HIPAA and the entity's own privacy policies.

d. The privacy officer will be responsible for monitoring existing arrangements with business associates and identifying new organizations which are business associates to assure contracts include the appropriate HIPAA provisions to protect confidential patient information shared with these business associates.

e. Any changes in the privacy policies of the entity will necessitate revision of the Privacy Notice, which, as a rule, will be the responsibility of the privacy officer.

f. The privacy officer must coordinate efforts with the information security officer to avoid duplication of efforts. Whenever possible, joint development of policies and implementation of training should be the goal. For example, as noted below, establishing the minimum necessary information to which each employee should have access is a responsibility of the privacy officer, but the implementation of security restrictions (access codes, etc.) is the responsibility of the information security officer. These two functions should be coordinated to avoid the creation of policies to protect privacy which cannot be fulfilled due to information system limitations.

g. Many of these follow-up responsibilities can be overseen by the privacy officer in conjunction with a privacy oversight committee, made up of representatives from the same areas of responsibility as may have served on an initial HIPAA task force or committee. These include human resources, health information management, information systems and legal. The privacy officer would direct and lead this committee.

B. Additional Responsibilities

1. Other HIPAA Obligations

a. HIPAA requires covered entities to establish complaint processes, to establish processes under which patients can ask to amend their medical records and to seek an accounting of disclosures of their

protected health information. In small facilities or physician offices, it is likely that these responsibilities will fall to the privacy officer. HIPAA regulations do not require that these be the obligation of the privacy officer, however, and there may be reasons to resist the temptation to impose them upon the privacy officer, particularly in larger organizations. For example, the volume of requests for access to records to review and amend them for an accounting of disclosures could be large and consume the privacy officer's time. Coordination with medical records personnel in responding to these requests will be necessary in most facilities and medical records personnel are usually accustomed to responding to requests for records and better equipped to handle such requests. The privacy officer could review all such requests and forward them for action to medical records, followed with a review of the records by the privacy officer before they are released.

b. Section 164.502(b) of the regulations require covered entities to make all reasonable efforts not to use or disclose more than the minimum amount of protected health information necessary to accomplish the intended purpose, use or disclosure. While the regulations include six significant exceptions to this requirement, there remains the obligation to determine "minimum necessary". It should not be the privacy officer who makes the individual decisions, although the officer should oversee the development of a policy for the entity. The privacy officer may delegate the everyday responsibility for these decisions to "experts" within the organization with clinical expertise to determine the minimum necessary information for various jobs. This could include nurse directors and medical records personnel. A key spot in the processes of most entities at which this decision can be made and communicated to employees is at the level of new hires. The hiring manager or supervisor can identify the information to which the new hire will have access and communicate this to the new employee. Computer access restrictions can be used in this context to limit access. This process serves as an interface between the privacy function and the information security function. The privacy officer can oversee this process and serve as a problem-solver, while day-to-day decisions and implementation can be assigned to front-line managers and supervisors.

c. The regulations require covered entities to develop their own internal system of sanctions for violations by employees and business associates. These can and should include termination of employees and the termination of agreements with business associates. The privacy officer, in conjunction with the human resources department, should monitor employee violations and related discipline. The ability to report on such disciplinary actions

arising from HIPAA violations is important to the privacy officer's ability to affirm the entity's efforts at enforcement. The privacy officer should be the responsible party for enforcement against business associates and coordinate regular audits of their activities, with reports also available of these audit activities and actions taken in response to violations.

C. Looking Ahead

1. The privacy officer will be responsible for addressing future problems in compliance with HIPAA. Potential problems an entity may face include delays in meeting the privacy compliance deadline, including getting new policies in place and completing necessary education; breaches of confidentiality by employees, business associates and others; failing to promptly and correctly respond to patient request permitted under HIPAA (including requests for accountings of releases of information and requests to amend patient medical records). The privacy officer, with the assistance of a privacy committee, should have in place contingency plans to assist in reacting to such problems. This would include the processes for enlisting additional resources, handling media inquiries, reporting breaches, as required, to appropriate authorities, coordinating disciplinary actions and terminations of agreements with business associates.

2. Coordination with marketing and public relations personnel will be important for those entities which choose to promote to the public the entity's advances in technology, security and privacy.

3. The privacy officer will be responsible for meeting requirements of JCAHO as it expands its accreditation standards to incorporate the requirements of HIPAA. Surveys after April 2003 likely will consider the entity's compliance with privacy standards. Preparation for surveys will require inclusion of HIPAA compliance and review of implementing policies. Audits by the Office of Civil Rights of CMS, which is charged with enforcement of HIPAA, will include surveys of HIPAA compliance as well.

ADDITIONAL RESOURCES

For more information about HIPAA in general and about the rules relating to privacy officers, the following web sites are available resources:

www.hcfa.gov/facts/f9702as.htm
www.hhs.gov/ocr/hipaa
http://aspe.os.dhhs.gov/admnsimp/
www.himinfo.com
www.ahima.org/hipaa/PrivacyOfficer2001.htm
www.aha.org/hipaa
www.healthlawyers.org
www.healthprivacy.org

THE MINIMUM NECESSARY STANDARD
[45 C.F.R. §§ 164.502(b), 164.514(d)]

Edward L. Schoenbaechler
Hall, Render, Killian, Heath & Lyman, PSC
Louisville, Kentucky

Copyright 2002. Edward L. Schoenbaechler. All rights reserved.

SECTION D

THE MINIMUM NECESSARY STANDARD
[45 C.F.R. §§ 164.502(b), 164.514(d)]

1. The Minimum Necessary Standard - § 164.502(b) D-1

A. Standard, Generally D-1

B. Requirement Does Not Apply To D-1

2. Implementing The Minimum Necessary Standard - § 164.514(d) D-2

A. Covered Entity Must Reasonably Ensure Requirements Met D-2

B. Minimum Necessary Uses Of Protected Health Information D-2

C. Minimum Necessary Disclosures Of Protected Health Information D-4

D. Minimum Necessary Requests For Protected Health Information D-6

E. Other Content Requirements - § 164.514(d)(5) D-6

F. The Minimum Necessary Standard For Financial Transactions - § 164.510(i) D-7

OCR HIPAA Privacy
TA 164.502B.001, July 6, 2001 ..... D-9

Edward L. Schoenbaechler
HALL, RENDER, KILLIAN, HEATH & LYMAN, PSC
The KHA Building, Suite 102
2501 Nelson Miller Parkway
Louisville, Kentucky 40223
(502) 253-1114

1. The Minimum Necessary Standard - § 164.502(b)

A. When using or disclosing Protected Health Information, or when requesting Protected Health Information from another Covered Entity, a Covered Entity must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure of request.

Comment: The Final Rule deleted the requirement that the Covered Entity make "all" reasonable efforts to limit necessary disclosures.

Comment: This is a flexible standard which takes into account the ability of the Covered Entity to configure its record system to allow selective access, such as limitations to only certain fields in a computerized information system, which may not be reasonable for a Covered Entity with a largely paper records system.

B. This requirement does <u>not</u> apply to:

<u>(i) Disclosures made to or by a health care provider for treatment</u>.

Comment: This exception to the disclosure rules also applies to mental health information. Providers may use existing ethical duties to limit the sharing of unnecessary medical information.

Comment: Note that the minimum necessary disclosure rules <u>do</u> apply to uses and disclosures for payment or health care operations.

(ii) Uses or disclosures made to the Individual, or pursuant to an Authorization, except for Authorizations requested by the Covered Entity under §§164.508(d), (e) or (f).

(iii) Disclosures made to the Secretary of HHS pursuant to a complaint brought under HIPAA in accordance with 45 CFR § 160, Subpart C.

(iv) Uses or disclosures required by law as described in §164.512(a).

Comment: Nothing in this rule permits Covered Entity to avoid disclosures required by other laws.

Comment: But, the rule does apply to disclosures to authorities which not required by law; but §164.514(h) allows Covered Entities to reasonably rely on the oral or written representation of public officials that a disclosure is required by law.

(v) Uses or disclosures required for compliance with applicable requirements of 45 CFR Subtitle A, Subchapter C, i.e., the required or situational data elements specified in the implementation guides for HIPAA administrative simplification standard transactions in the Transactions Rule.

Comment: The standard does apply to uses or disclosures in standard transactions that are made at the option of the Covered Entity.

2. Implementing the Minimum Necessary Standard - § 164.514(d)

A. A Covered Entity must reasonably ensure that the standards, requirements, and implementation specifications of §§164.502(b) and 164.514 relating to a request for or the use or disclosure of the minimum necessary Protected Health Information are met.

B. Minimum Necessary Uses of Protected Health Information

(i) A Covered Entity must identify:

(1) Those persons or classes of persons, as appropriate, in the workforce who need access to Protected Health Information to carry out their duties; and

(2) For each such person or class of persons, the category or categories of Protected Health Information to which access is needed and any conditions appropriate to such access.

(ii) A Covered Entity must make reasonable effort to limit the access of such persons or classes identified herein consistent with such classifications.

Comment: This requirement to implement policies and procedures is in lieu of making a minimum necessary determination on a case by case basis.

Comment: This is a substantial change from the proposed rule which required procedures to: (i) identify appropriate persons within the entity to determine what information should be disclosed consistent with the minimum necessary standard; (ii) ensure that those persons make the necessary determinations; and (iii) within the limits of the entity's technological capabilities, provide for the making of such determinations individually.

Comment: The proposed rule described certain criteria (which were not included in the regulatory text) which were used to determine what was a reasonable effort under this section: (i) the amount of information disclosed; (ii) the number of individuals who would then have access to the Protected Health Information; (iii) the likelihood that further uses or disclosures could occur; (iv) the importance of the use or disclosure; (v) the potential to achieve the same purpose with de-identified information; (vi) the technology available to limit the amount of Protected Health Information used or disclosed; (vii) the cost of limiting the use or disclosure; and (viii) any other factors that the entity believed were relevant to the determination.

Example: A hospital could permit nurses access to all Protected Health Information of patients in their ward while on duty, but should not permit appointment scheduling clerks free access to medical records.

Example: A health plan could permit its underwriting analyst unrestricted access to aggregate claims data, but require documented approval of a department manager to obtain identifiable records of a specific member for the purpose of determining a cause of

unexpected claims that could influence renewal premium rate setting.

Comment: Covered Entities are expected to allow persons involved in treatment to have access to the entire medical record.

C. Minimum Necessary Disclosures of Protected Health Information

(i) For any type of disclosure that it makes on a routine and recurring basis, a Covered Entity must implement policies and procedures (which may be standard protocols) that limit the Protected Health Information disclosed to the amount reasonably necessary to achieve the purpose of the disclosure.

Comment: Individual review is not required, but policies must identify the types of Protected Health Information to be disclosed, the types of person to receive the Protected Health Information, and the conditions for access.

Example: A Covered Entity may require a researcher requesting data contained in paper-based records to review the records on-site and to abstract only the information relevant to the research.

Example: With regard to Business Associates, a standard protocol could describe the subset of information that may be disclosed to medical transcription services.

(ii) For all other [i.e., non-routine] disclosures, a Covered Entity must:

(1) Develop [reasonable] criteria designed to limit the Protected Health Information disclosed to the information reasonably necessary to accomplish the purpose for which the disclosure is sought; and

(2) Review requests for disclosure on an individual basis in accordance with such criteria.

Comment: Disclosures to health care providers for treatment purposes are not subject to these requirements.

(iii) A Covered Entity may rely, if such reliance is reasonable under the circumstances, on a requested disclosure as the minimum necessary for the stated purpose when:

(1) Making disclosures to public officials that are permitted under §164.512, if the public official represents that the information requested is the minimum necessary for the stated purpose(s);

Comment: The Final Rule specifically allows Covered Entities to use or disclose Protected Health Information without individual agreement to federal, state or local government agencies, or private disaster assistance or relief organizations (such as the Red Cross), so as not to impede their mission to save lives and reunite loved ones and families in disaster situations. §164.51o(b)(4)

(2) The information is requested by another Covered Entity;

Comment: The disclosure rules apply to requests by Covered Entities, but one Covered Entity may rely on the assertion of a requesting Covered Entity that it is requesting only the minimum necessary Protected Health Information. Recall, however, that the disclosure rules do not apply to provider requests for treatment purposes.

(3) The information is requested by a professional who is a member of the workforce or is a Business Associate of the Covered Entity for the purpose of providing professional services to the Covered Entity, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or

Comment: The minimum necessary disclosure rules apply to Business Associates, although you can use standard protocols for routine disclosures and rely upon representations of professionals.

(4) Documentation or representations that comply with §164.512(i) have been provided by a person requesting the information for research purposes.

Comment: The documentation should come from an Institutional Review Board or privacy board, and should describe with sufficient specificity the

Protected Health Information necessary for the research.

D. Minimum Necessary Requests for Protected Health Information

i) A Covered Entity must limit any request for Protected Health Information to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from another Covered Entity.

(ii) For a request that is made on a routine or recurring basis, a Covered Entity must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

Comment: Creation and implementation of these policies is in lieu of making individualized determinations for each request.

(iii) For all other [i.e., non-routine] requests, a Covered Entity must review the request on an individual basis to determine that the Protected Health Information sought is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

E. Other Content Requirements - §164.514(d)(5) – For all uses, disclosures or requests to which the minimum necessary requirements apply, a Covered Entity may not use, disclose or request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure or request.

Example: Disclosure of all Protected Health Information to an accreditation group may be the "minimum necessary" for its purposes, thus justifying a policy for such disclosure.

Example: A health plan's request for all Protected Health Information from an applicant for insurance may be appropriate if the entire record is the "minimum necessary" for its purpose, thus justifying a policy for such request.

Comment: Disclosure of the entire medical record absent such documented justification is a presumptive violation of this rule.

F. The Minimum Necessary Standard for Financial Transactions - §164.510(i)

(i) A Covered Entity may disclose, in connection with routine banking activities or payment by debit, credit, or other payment card, or other payment means, the minimum amount of Protected Health Information necessary to complete a banking or payment activity to:

(1) A financial Institution (as defined by section 101 of the Right to Financial Privacy Act of 1978); or

(2) An entity engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting payments, for such a financial institution.

Comment: The information that will generally be needed : the name and address of the individual; the name and address of the payer or provider; the amount of the charge for the health service; the date on which the health service was rendered; the expiration date of the payment mechanism; the individual's signature; and relevant identification and account numbers.

Comment: We clarify that "pharmacy benefit cards," as well as other health benefit cards, are used for identification of individual, plan, and benefits and do not qualify as "other payment cards."

MINIMUM NECESSARY
[45 CFR §§ 164.502(b), 164.514(d)]

General Requirement

The Privacy Rule generally requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for protected health information (PHI) to the minimum necessary to accomplish the intended purpose. The minimum necessary provisions do not apply to the following:

- Disclosures to or requests by a health care provider for treatment purposes.
- Disclosures to the individual who is the subject of the information.
- Uses or disclosures made pursuant to an authorization requested by the individual.
- Uses or disclosures required for compliance with the standardized Health Insurance Portability and Accountability Act (HIPAA) transactions.
- Disclosures to the Department of Health and Human Services (HHS) when disclosure of information is required under the rule for enforcement purposes.
- Uses or disclosures that are required by other law.

The implementation specifications for this provision require a covered entity to develop and implement policies and procedures appropriate for its own organization, reflecting the entity's business practices and workforce. We understand this guidance will not answer all questions pertaining to the minimum necessary standard, especially as applied to specific industry practices. As more questions arise with regard to application of the minimum necessary standard to particular circumstances, we will provide more detailed guidance and clarification on this issue.

Uses and Disclosures of, and Requests for PHI

For uses of PHI, the policies and procedures must identify the persons or classes of persons within the covered entity who need access to the information to carry out their job duties, the categories or types of PHI needed, and conditions appropriate to such access. For example, hospitals may implement policies that permit doctors, nurses, or others involved in treatment to have access to the entire medical record, as needed. Case-by-case review of each use is not required. Where the entire medical record is necessary, the covered entity's policies and procedures must state so explicitly and include a justification.

For routine or recurring requests and disclosures, the policies and procedures may be standard protocols and must limit PHI disclosed or requested to that which is the minimum necessary for that particular type of disclosure or request. Individual review of each disclosure or request is not required.

For non-routine disclosures, covered entities must develop reasonable criteria for determining, and limiting disclosure to, only the minimum amount of PHI necessary to accomplish the purpose of a non-routine disclosure. Non-routine disclosures must be reviewed on an individual basis in accordance with these criteria. When making non-routine requests for PHI, the covered entity must review each request so as to ask for only that information reasonably necessary for the purpose of the request.

Reasonable Reliance

In certain circumstances, the Privacy Rule permits a covered entity to rely on the judgment of the party requesting the disclosure as to the minimum amount of information that is needed. Such reliance must be reasonable under the particular circumstances of the request. This reliance is permitted when the request is made by:

- A public official or agency for a disclosure permitted under §164.512 of the rule.
- Another covered entity.
- A professional who is a workforce member or business associate of the covered entity holding the information.
- A researcher with appropriate documentation from an Institutional Review Board (IRB) or Privacy Board.

The rule does not require such reliance, however, and the covered entity always retains discretion to make its own minimum necessary determination for disclosures to which the standard applies.

Treatment Settings

We understand that medical information must be conveyed freely and quickly in treatment settings, and thus understand the heightened concern that covered entities have about how the minimum necessary standard applies in such settings. Therefore, we are taking the following steps to clarify the application of the minimum necessary standard in treatment settings. First, we clarify some of the issues here, including the application of minimum necessary to specific practices, so that covered entities may begin implementation of the Privacy Rule. Second, we will propose corresponding changes to the regulation text, to increase the confidence of covered entities that they are free to engage in whatever communications are required for quick, effective, high quality health care. We understand that issues of this importance need to be addressed directly and clearly to eliminate any ambiguities.

Frequently Asked Questions

Q: How are covered entities expected to determine what is the minimum necessary information that can be used, disclosed, or requested for a particular purpose?

A: The Privacy Rule requires a covered entity to make reasonable efforts to limit use, disclosure of, and requests for PHI to the minimum necessary to accomplish the intended purpose. To allow covered entities the flexibility to address their unique circumstances, the rule requires covered entities to make their own assessment of what PHI is reasonably necessary for a particular purpose, given the characteristics of their business and workforce, and to implement policies and procedures accordingly. This is not a strict standard and covered entities need not limit information uses or disclosures to those that are absolutely needed to serve the purpose. Rather, this is a reasonableness standard that calls for an approach consistent with the best practices and guidelines already used by many providers today to limit the unnecessary sharing of medical information.

The minimum necessary standard is intended to make covered entities evaluate their practices and enhance protections as needed to prevent unnecessary or inappropriate access to PHI. It is intended to reflect and be consistent with, not override, professional judgment and standards. Therefore, we expect that covered entities will utilize the input of prudent professionals involved in health care activities when developing policies and procedures that appropriately will limit access to personal health information without sacrificing the quality of health care.

Q: Won't the minimum necessary restrictions impede the delivery of quality health care by preventing or hindering necessary exchanges of patient medical information among health care providers involved in treatment?

A: No. Disclosures for treatment purposes (including requests for disclosures) between health care providers are explicitly exempted from the minimum necessary requirements.

The Privacy Rule provides the covered entity with substantial discretion as to how to implement the minimum necessary standard, and appropriately and reasonably limit access to the use of identifiable health information within the covered entity. The rule recognizes that the covered entity is in the best position to know and determine who in its workforce needs access to personal health information to perform their jobs. Therefore, the covered entity can develop role-based access policies that allow its health care providers and other employees, as appropriate, access to patient information, including entire medical records, for treatment purposes.

Q: Do the minimum necessary requirements prohibit medical residents, medical students, nursing students, and other medical trainees from accessing patients' medical information in the course of their training?

A: No. The definition of "health care operations" in the rule provides for "conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers." Covered entities can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients' medical information, including entire medical records.

Q: Must minimum necessary be applied to disclosures to third parties that are authorized by an individual?

A: No, unless the authorization was requested by a covered entity for its own purposes. The Privacy Rule exempts from the minimum necessary requirements most uses or disclosures that are authorized by an individual. This includes authorizations covered entities may receive directly from third parties, such as life, disability, or casualty insurers pursuant to the patient's application for or claim under an insurance policy. For example, if a covered health care provider receives an individual's authorization to disclose medical information to a life insurer for underwriting purposes, the provider is permitted to disclose the information requested on the authorization without making any minimum necessary determination. The authorization must meet the requirements of §164.508.

However, minimum necessary does apply to authorizations requested by the covered entity for its own purposes (see §164.508(d), (e), and (f)).

Q: Are providers required to make a minimum necessary determination to disclose to federal or state agencies, such as the Social Security Administration (SSA) or its affiliated state agencies, for individuals' applications for federal or state benefits?

A: No. These disclosures must be authorized by an individual and, therefore, are exempt from the minimum necessary requirements. Further, use of the provider's own authorization form is not required. Providers can accept an agency's authorization form as long as it meets the requirements of §164.508 of the rule. For example, disclosures to SSA (or its affiliated state agencies) for purposes of determining eligibility for disability benefits are currently made subject to an individual's completed SSA authorization form. After the compliance date, the current process may continue subject only to modest changes in the SSA authorization form to conform to the requirements in §164.508.

Q: Doesn't the minimum necessary standard conflict with the Transactions standards? Does minimum necessary apply to the standard transactions?

A: No, because the Privacy Rule exempts from the minimum necessary standard any uses or disclosures that are required for compliance with the applicable requirements of the subchapter. This includes all data elements that are required or situationally required in the standard transactions. However, in many cases, covered entities have significant discretion as to the information included in these transactions. This standard does apply to those optional data elements.

Q: Does the rule strictly prohibit use, disclosure, or requests of an entire medical record? Does the rule prevent use, disclosure, or requests of entire medical records without case-by-case justification?

A: No. The Privacy Rule does not prohibit use, disclosure, or requests of an entire medical record. A covered entity may use, disclose, or request an entire medical record, without a case-by-case justification, if the covered entity has documented in its policies and procedures that the entire medical record is the amount reasonably necessary for certain identified purposes. For uses, the policies and procedures would identify those persons or classes of person in the workforce that need to see the entire medical record and the conditions, if any, that are appropriate for such access. Policies and procedures for routine disclosures and requests and the criteria used for non-routine disclosures would identify the circumstances under which disclosing or requesting the entire medical record is reasonably necessary for particular purposes. In making non-routine requests, the covered entity may also establish and utilize criteria to assist in determining when to request the entire medical record.

The Privacy Rule does not require that a justification be provided with respect to each distinct medical record.

Finally, no justification is needed in those instances where the minimum necessary standard does not apply, such as disclosures to or requests by a health care provider for treatment or disclosures to the individual.

Q: In limiting access, are covered entities required to completely restructure existing workflow systems, including redesigns of office space and upgrades of computer systems, in order to comply with the minimum necessary requirements?

A: No. The basic standard for minimum necessary uses requires that covered entities make reasonable efforts to limit access to PHI to those in the workforce that need access based on their roles in the covered entity.

The Department generally does not consider facility redesigns as necessary to meet the reasonableness standard for minimum necessary uses. However, covered entities may need to make certain adjustments to their facilities to minimize access, such as isolating and locking file cabinets or records rooms, or providing additional security, such as passwords, on computers maintaining personal information.

Covered entities should also take into account their ability to configure their record systems to allow access to only certain fields, and the practicality of organizing systems to allow this capacity. For example, it may not be reasonable for a small, solo practitioner who has largely a paper-based records system to limit access of employees with certain functions to only limited fields in a patient record, while other employees have access to the complete record. Alternatively, a hospital with an electronic patient record system may reasonably implement such controls, and therefore, may choose to limit access in this manner to comply with the rule.

Q: Do the minimum necessary requirements prohibit covered entities from maintaining patient medical charts at bedside, require that covered entities shred empty prescription vials, or require that X-ray light boards be isolated?

A: No. The minimum necessary standards do not require that covered entities take any of these specific measures. Covered entities must, in accordance with other provisions of the Privacy Rule, take reasonable precautions to prevent inadvertent or unnecessary disclosures. For example, while the Privacy Rule does not require that X-ray boards be totally isolated from all other functions, it does require covered entities to take reasonable precautions to protect X-rays from being accessible to the public. We understand that these and similar matters are of special concern to many covered entities, and we will propose modifications to the rule to increase covered entities' confidence that these practices are not prohibited.

Q: Will doctors' and physicians' offices be allowed to continue using sign-in sheets in waiting rooms?

A: We did not intend to prohibit the use of sign-in sheets, but understand that the Privacy Rule is ambiguous about this common practice. We, therefore, intend to propose modifications to the rule to clarify that this and similar practices are permissible.

Q: What happens when a covered entity believes that a request is seeking more than the minimum necessary PHI?

A: In such a situation, the Privacy Rule requires a covered entity to limit the disclosure to the minimum necessary as determined by the disclosing entity. Where the rule permits covered entities to rely on the judgment of the person requesting the information, and if such reliance is

reasonable despite the covered entity's concerns, the covered entity may make the disclosure as requested.

Nothing in the Privacy Rule prevents a covered entity from discussing its concerns with the person making the request, and negotiating an information exchange that meets the needs of both parties. Such discussions occur today and may continue after the compliance date of the Privacy Rule.

HIPAA PRIVACY COMPLIANCE PROGRAMS

Vickie Yates Brown
Greenebaum Doll & McDonald PLLC
Louisville, Kentucky

Copyright 2002. Vickie Yates Brown. All rights reserved.

SECTION E

KENTUCKY HEALTH LAW

A "NUTS & BOLTS" WORKSHOP ON HIPAA
(The Health Insurance Portability and Accountability Act)

University of Kentucky College of Law
Office of Continuing Legal Education

Lexington, Kentucky

Friday, March 15, 2002

HIPAA PRIVACY COMPLIANCE PLANS

by:

VICKIE YATES BROWN
GREENEBAUM DOLL & MCDONALD PLLC

Vickie Yates Brown
Chair, Health Care and Insurance Practice Group
Greenebaum Doll & McDonald PLLC
3300 National City Tower
101 South Fifth Street
Louisville, KY 40202
vyb@gdm.com
(502) 587-3578
Fax: (502) 540-2171

Rebekah K. Casteel
Associate, Health Care and Insurance
Greenebaum Doll & McDonald PLLC
3300 National City Tower
101 South Fifth Street
Louisville, KY 40202
rkc@gdm.com
(502) 587-3670
Fax: (502) 588-1310

HIPAA PRIVACY COMPLIANCE PROGRAMS

INTRODUCTION E-1

I. PHASE 1: HIPAA OVERVIEW AND PROGRAM INITIATION E-2

1. Appointment of a Privacy Officer E-2
2. Understand HIPAA's Requirements E-3
3. Educate Management E-3
4. Reporting Structure E-3
5. Identify Applicable Requirements E-3
6. Evaluation of Other Laws Including a Preemption Analysis E-4
7. Budget Considerations E-4
8. Attorney-Client Privilege E-5

II. PHASE 2: COMPLIANCE / RISK ASSESSMENT & GAP ANALYSIS E-6

III. PHASE 3: MANAGEMENT REVIEW E-11

IV. PHASE 4: COMPLIANCE IMPLEMENTATION E-13

I. Patient Rights E-15
1. Notice of Privacy Practices for Confidential Information E-15
2. Access of Individuals to Confidential Information E-15
3. Amendment of Confidential Information E-16
4. Accounting for Disclosures E-17
5. Complaints to the Covered Entity E-17
6. Waiver of Rights E-17

II. Government Requirements E-17
1. Uses and Disclosures of Confidential Information E-18
2. Business Associates E-18
3. Mitigation E-19
4. Refraining from Intimidating or Retaliatory Acts E-19
5. Ensuring Confidential Information is Secure E-19
6. Training E-19
7. Sanctions E-20

V. PHASE 5: TROUBLESHOOTING AND AUDITING E-21

CONCLUSION E-22

BIBLIOGRAPHY E-24

HIPAA PRIVACY COMPLIANCE PLANS

On December 28, 2000, the Department for Health and Human Services ("DHHS") published a final rule regarding the privacy of protected health information ("PHI").[1] The new privacy standard authorized by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), governs a covered entity's[2] use and disclosure of PHI [hereinafter the "Privacy Rule" or "Privacy Regulation"]. The Privacy Rule also grants individuals certain rights with respect to their own PHI.

> The privacy standard ... is destined to revolutionize the way patients, health care providers and insurers relate to one another. In asserting that privacy is a "fundamental right," the rule has the potential to transform the very way Americans view their right to control all information concerning themselves.[3]

For a covered entity, becoming "HIPAA-compliant" entails much more than drafting a few agreements and securing patient files. Much like the corporate compliance plans providers and others are already accustomed to developing in response to federal fraud and abuse laws, the HIPAA regulations require covered entities to formulate and maintain a framework, including structured policies and procedures, for maintaining responsible privacy practices. A HIPAA compliance plan, then, is a mechanism which can help guide an organization to HIPAA compliance.

The deadline for compliance with the HIPAA privacy regulations is April 14, 2003. With about 12 months to prepare, covered entities have only a short time left to comply with HIPAA. Although admittedly a daunting task, breaking compliance into manageable pieces is possible. This

---

[1] *See* 65 Fed. Reg. 82462 - 82944.

[2] *Covered Entity* means: (1) A health plan. (2) A health care clearinghouse. (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter. 45 CFR 160.103.

[3] HIPAA Patient Privacy Compliance Guide, Frances R. Fernald, ed., Atlantic Information Services, Inc., 100:4 (2002).

paper breaks compliance into five separate but interdependent phases. The time allotted for each phase will vary depending on the size and function of the entity. The goal of the first three phases is to prepare a "workplan." The workplan will utilize an organization's knowledge of the HIPAA regulations as it relates to their functions (Phase One), it will provide an overview of the organization's current privacy practices (Phase Two), and it will define the risks of noncompliance and prioritize the goals for the final two phases of HIPAA compliance (Phase Three). Phase Four is dedicated to actually implementing the internal changes identified as needing improvement and/or formulation during the previous phases. The final phase follows implementation, and allows the organization to adjust and troubleshoot any of the changes and also begin to comply with HIPAA's audit and monitoring requirements.

I. Phase 1: HIPAA Overview and Program Initiation

Most health care entities understand that they will be affected by HIPAA's privacy regulations. Most, however, do not comprehend the extent to which the regulations will change the way the entity operates. Because it is so important to get off to a good start with your organization's HIPAA compliance efforts, Phase One is dedicated to understanding and communicating HIPAA basics. Activities done in Phase One should all focus on improving the entity's knowledge of HIPAA's requirements and designating those to lead your entity to compliance. Therefore, Phase One of your compliance efforts should entail at least the following:

(1) **Appointment of a Privacy Officer:** Not only is the appointment of a privacy officer mandated by the regulations, but this will be the person who will lead your organization's compliance effort. 45 CFR §164.530(a)(1). Leadership in this process is essential to getting started, to make continued progress and to sustain the change.

(A) The privacy officer will oversee compliance for the entire organization. This will include access to, and uses, disclosures, and disposition of, PHI and will entail significant interaction and collaboration with department, committee, and clinical personnel.

(B) The privacy officer should be given enough responsibility to be capable of implementing and overseeing your entire organization's compliance.

(C) Larger organizations may also need to establish one or more committees to assist the privacy officer with the development and day-to-day operations regarding HIPAA compliance. Members of these committees could include personnel from human resources, purchasing, claims and billing, and the medical staff.

(2) **Understand HIPAA's Requirements**: The Privacy Officer and others responsible for HIPAA compliance need to acquire knowledge and training regarding HIPAA's requirements.

(3) **Educate Management**: Even if the management of your organization is not participating directly in the compliance process, they also need to be educated regarding the basic requirements and scope of HIPAA compliance.

(4) **Reporting Structure**: Management needs to determine how it will oversee privacy compliance.

(5) **Identify Applicable Requirements**: Review the regulations to identify policy elements and determine which ones are applicable to your organization's select business functions. The HIPAA privacy regulations recognize that many covered entities perform other functions which are not covered by HIPAA or are affiliated in some way with other covered entities. Because of this, your entity may be able to take advantage of the compliance-related efficiencies provided in the regulations. If your organization is considered a (1) hybrid entity, an (2) affiliated entity or is an (3) organized health care arrangement ("OHCA") you may be able to isolate and/or coordinate certain compliance-related functions. To determine if your organization fits any of these organizational structures, you will need to thoroughly assess, probably with the aid of counsel, the entire organization and its operations from both a technical or legal perspective and also from a practical and strategic perspective. Requirements affecting ALL covered entities include:

(A) Appointment of a privacy official and privacy contact;

(B) Development, implementation and documentation of privacy policies and procedures;

(C) Workforce training on privacy;

(D) Adoption of privacy safeguards for PHI;

(E) Implementation of minimum necessary guidelines for the use and disclosure of PHI;

(F) Establishment of a complaint process for privacy violations; and

(G) Establishment of sanctions for privacy violations.

(6) **Evaluation of Other Laws Including a Preemption Analysis**: At this stage it is also important to assess other laws that affect how your organization is run. Many other state and federal statutes, rules and regulations, and state constitutions may potentially impact your organization. It is important to keep in mind that Congress gave HIPAA preemptive effect over certain contrary provisions of State law.[4] Statutory parts of HIPAA and any standard or implementation specification adopted by the regulation shall supersede any contrary provision of State law, including a provision of State law that requires medical or health plan records (including billing information) to be maintained or transmitted in written rather than electronic form. If your organization determines it is also subject to a State law which is potentially contrary to any of HIPAA's requirements, the organization should obtain advice from legal counsel concerning your obligations.

(7) **Budget Considerations**: Although the Department of Health and Human Services ("DHHS") anticipates that the "net impact of the [privacy] rules will be a net savings to the health care system," every organization can expect a significant cost expenditure for HIPAA compliance. Your organization needs to be aware of the potential cost involved and needs to commit funds to complete your compliance plan. When your organization determines its compliance budget be sure to also include the cost of any attorneys and/or consultants your organization plans to employ for this process. In addition to budgeting for consultants DHHS has identified the following 14 cost components to HIPAA privacy compliance applicable to every covered entity:[5]

---

[4] *See* 45 CFR § 160.201 *et seq.*

[5] *See* 65 Fed.Reg. 82765-82776.

(A) Policy development

(B) Minimum necessary

(C) Privacy official(s)

(D) Disclosure tracking/history

(E) Business associates

(F) Notice distribution

(G) Consent

(H) Inspection/Copying

(I) Amendment

(J) Requirements on research

(K) Training

(L) De-identification of information

(M) Employers with insured group health plans

(N) Internal complaints

(8) **Attorney-Client Privilege**: Phase two of your compliance plan requires an internal risk assessment of your organization's current business practices. Because the internal assessment may uncover potentially sensitive information about your organization, the organization should consider engaging legal counsel to invoke the attorney-client privilege with respect to any findings.

Phase One Check-List

- ❑ Privacy officer appointed
- ❑ HIPAA requirements reviewed and all requirements which pertain to your organization are identified
- ❑ Other laws which may affect your compliance efforts are identified and evaluated
- ❑ Compliance budget prepared

II. Phase 2: Compliance/Risk Assessment & Gap Analysis

Phase Two involves performing an internal assessment to determine exactly how your organization's current level of privacy compares to the HIPAA requirements. A comprehensive risk assessment includes thoroughly reviewing every operating policy, examining every contractual arrangement, capturing where and how PHI is created, stored, transferred and shared, identifying key personnel, and reviewing the degree of compliance among your business associates.

The first aspect of the internal HIPAA assessment should be to generate a checklist or questionnaire which will help guide you through your organization's structure and allow you to ask the right questions of the right people including requesting all of the needed documentation. Your checklist can and should be created by going through your list of HIPAA requirements generated in Phase One. Specific requirements of the Privacy Rule that every covered entity needs to address in this phase include, but are not limited to, the following:

(1) Consents for the use and disclosure of PHI to carry out treatment, payment or health care operations;[6]

(2) Uses and disclosures of PHI for which an Authorization is required;[7]

---

[6] 45 CFR § 164.506

[7] 45 CFR § 164.508

(3) Uses and disclosures of PHI requiring an opportunity for the individual to agree or to object;[8]

(4) Uses and disclosures of PHI for which consent, authorization or opportunity to agree or object is not required;[9]

(5) Notice of privacy practices;[10]

(6) Patient's right to request privacy protection for their PHI;[11]

(7) Patient's right of access to their PHI;[12]

(8) Amendment of PHI;[13]

(9) Accounting of disclosures of PHI;[14]

(10) Contractual requirements for business associate relationships;[15]

(11) Personnel training regarding privacy policies and procedures;[16] and

(12) Formal written policies and procedures concerning the entities privacy policies and procedures;[17]

---

[8] 45 CFR § 164.510

[9] 45 CFR § 164.512

[10] 45 CFR § 164.520

[11] 45 CFR § 164.522

[12] 45 CFR § 164.524

[13] 45 CFR § 164.526

[14] 45 CFR § 164.528

[15] 45 CFR § 164.504(e)

[16] 45 CFR § 164.530(b)

[17] 45 CFR § 164.530(j)

After putting together a complete checklist of HIPAA requirements, you need to determine, according to the functions of your organization, what information you will need to know to assess your current privacy practices. For example, the HIPAA privacy regulations require covered entities to obtain an authorization from the individual for every use or disclosure of PHI not related to the treatment, payment or health care operations for that individual. 45 CFR §164.508(a). An appropriate HIPAA analysis, then, needs to include a determination of how, when and by whom an organization uses and discloses PHI in order to determine not only the current level of compliance, but also eventually what practices need to be changed. The sample HIPAA analysis questionnaire in Example One demonstrates this concept.

Example 1: HIPAA Analysis Questionnaire

HIPAA Requirement	
(1) Authorization. 45 CFR §164.508(a)	1. Does the organization use PHI for purposes other than treatment, payment or health care operations? Answer: 2. If yes, how? Answer: 3. Does the organization obtain any form of authorization prior to the use or disclosure? Answer: 4. If yes, before every use or disclosure? Answer: 5. Is the authorization a form or is it individualized? Answer: 6. Attach copy of any and all authorizations used. Answer:

It is important to be particularly diligent in assessing the organization's relationships with entities designated as "business associates" by the privacy rule.[18] Because the Privacy Rule does not directly regulate business associates, it places the responsibility of monitoring business associate conduct on the covered entity. The Privacy Rule states that a covered entity is not in compliance with the Rule's requirements "if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement ..."[19] The business associate provisions will undoubtedly cause your organization to reevaluate and renegotiate many of its contractual relationships.[20] Depending on the size of your organization, the process of identifying all business associates and drafting new contracts or adding HIPAA compliant provisions could be a substantial undertaking and therefore should be started as soon as possible.

Some common business practices may not automatically be viewed as potential compliance issues. The following are examples of some practices your organization should consider when drafting and performing the risk assessment:

(1) Where are patient sign up sheets with name and other information kept?

(2) Where are patient schedules stored? Are they left in plain view?

(3) Do confidential conversations take place in areas where they can be overheard?

(4) Are computer screens with PHI of patients left in plain view?

---

[18] 45 CFR § 164.504(e).

[19] 45 CFR §164.504(e)(ii).

[20] *See* 45 CFR §164.504(e) for Privacy Rule requirements for Business Associate Contracts.

(5) Do office staff members regularly change their passwords and safeguard access to their work areas?

(6) Where are medical records and lab reports kept? If these documents are disclosed, what is the policy and to whom may these documents be disclosed?

(7) Are there safeguards that are documented regarding the transfer of PHI as paper medical records, orders, images, and lab specimens?

(8) Is there an employee handbook or other human resources documentation that can be expanded to cover HIPAA requirements?

(9) Are there documented policies and procedures when an employee is terminated? Does this include the return of all keys, cards, and change codes and locks, as necessary?

After generating an internal HIPAA compliance checklist and actually performing the assessment, the organization needs to conduct a **gap analysis**. The gap analysis is a comprehensive report that outlines the gap between the organization's current state of privacy and the required level needed to meet HIPAA regulations. From this gap analysis, the organization can begin to develop priorities, work plans, and budgets to meet the HIPAA mandate. Example Two illustrates how the gap analysis works together with the HIPAA analysis questionnaire.

Example 2: HIPAA Gap Analysis

HIPAA Requirement	Questionnaire	Deficiencies	Solutions	Resource Estimate
(1) Authorization. 45 CFR §164.508(a)	1. Does the organization use PHI for purposes other than treatment, payment or health care operations? Answer: Yes 2. If yes, how? Answer: Marketing and Research 3. Does the organization obtain any form of authorization prior to the use or disclosure? Answer: No 4. If yes, before <u>every</u> use or disclosure? Answer: 5. Is the authorization a form or is it individualized? Answer: 6. Attach copy of any and all authorizations used.	1. No policy or procedure for obtaining authorizations	1. Prior to every disclosure of PHI organization needs to obtain HIPAA compliant authorization. 2. Need written policies and procedures for obtaining authorization. 3. Need to formulate HIPAA compliant authorization to be adapted and used by appropriate personnel.	Estimated attorney hours to complete: Estimated cost:

Phase Two Check-List

- ❑ HIPAA analysis questionnaire developed
- ❑ Internal risk/compliance assessment performed
- ❑ Gap analysis completed

III. Phase 3: Management Review

The management review phase is conducted once the assessment and gap analysis are complete. Although in many practices "management" actually prepared or helped prepare the assessment and gap analysis, this phase is still very important because it is at this point that organizational consensus is gained and priorities are set. Failure to achieve consensus and organize priorities may lead to problems that will hinder your organization's overall progress. This step is essential in keeping your organization from being consumed with turf battles and resource allocation (or re-allocation) issues, instead of working toward HIPAA compliance.

Phase Three should allow those in charge of HIPAA compliance to compile and present compliance recommendations to management as well as back up the recommendations with factual information (the risk assessment and gap analysis). If senior management has not been involved with the assessment and gap analysis, it is their turn to provide direction and communicate priorities which require action. At the end of phase three, most, if not all, of the aspects of your workplan should be identified. For example:

Example 3: Workplan

HIPAA Requirement	HIPAA Questionnaire	Solution	Whose Responsibility?	Target Start Date	Actual Start Date	Target End Date	Task Status
Authorization 45 CFR §164.508(a)	1. Does the Practice use PHI for purposes other than treatment, payment or health care operations? Answer: Yes 2. How? Answer: Marketing and Research 3. Does the Practice obtain any form of authorization prior to the use or disclosure? Answer: No	1. Prior to every disclosure of PHI organization needs to obtain HIPAA compliant authorization. 2. Need written policies and procedures for obtaining authorization. 3. Need to formulate HIPAA compliant authorization to be adapted and used by appropriate personnel.	Organization's Attorney	1/01/03		2/01/03	

Phase Three Check-List

- ❑ Findings from HIPAA assessment and gap analysis presented to management
- ❑ Priorities and direction for HIPAA compliance articulated by management.
- ❑ Workplan is complete.

IV. Phase 4: Compliance Implementation

Although your organization may perform an excellent job of assessing its current privacy practices and determining what needs to be done, poor implementation of the necessary improvements will have a detrimental impact on achieving HIPAA compliance. Phase Four is where the planning and assessment activities end, and the implementation begins.

It is in this phase where your organization must develop or refine its privacy practices, policies and procedures. In addition to actually developing HIPAA-compliant consents, authorizations, notice of information practices and business associate contracts, formal written policies and procedures for all aspects of PHI privacy need to be created and implemented and employees, staff and management need to be trained as to the new policies and procedures. This phase will most likely need to be allotted the most time and resources.

Under the title of Administrative Requirements, the Privacy Rule requires that:

> a covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specifications, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size of and the type of activities that relate to protected health information undertaken by the covered entity, to ensure such compliance. 45 CFR. §164.503(i).

The Privacy Regulation also requires a covered entity to change its policies and procedures when "necessary and appropriate" to comply with changes in the law and/or changes in the entity's privacy practice.[21] The documentation of policies and procedures may be either in written or electronic form.[22] In addition, a covered entity must retain the documentation for six (6) years from the date it was created or was last in effect whichever is later.[23] Since the privacy rules are designed to be flexible and scalable, larger, more technologically sophisticated entities are required to implement more extensive and more stringent privacy policies and procedures. Although an entity's decisions regarding the scope of its policies and procedures can be influenced by physical factors

---

[21] 45 CFR §164.530(i)(2).

[22] 45 CFR §164.530(j)(1).

[23] 45 CFR §164.530(j)(2).

such as size and by business factors such as acceptable levels of risk, please note that even the smallest entity must implement the policies and procedures required to protect the PHI in its care.

It may be helpful at this stage for your organization to categorize the policies and procedures required by the Privacy Rule. The first category of policies and procedures relate to a patient's rights regarding the privacy of their PHI. The second category of policies and procedures is comprised of governmental requirements concerning the protection of PHI. The following is an outline of the policies and procedures, by category, which must be implemented and documented by all covered entities.

I. Patient Rights:

(1) **Notice of Privacy Practices for Confidential Information**: The Privacy Rule states that "an individual has a right to adequate notice of the uses and disclosures of protected health inforamtion that may be made by the covered entity, and of the individual rights and the covered entity's legal duties with respect to protected health information."[24] The elements required for a HIPAA-compliant notice of privacy practices are found in the regulation at 45 CFR §164.520(b) and your organization's privacy policy must contain every element. The policy manual must include a reference to the Notice and procedures outlined in the manual must be consistent with the Notice, including procedures for notifying patients of changes in the Notice.

(2) **Access of Individuals to Confidential Information**: Individuals have the right to inspect and obtain a copy of their confidential information, for as

[24] 45 CFR §164.520(a).

long as the covered entity maintains the information. Covered entities must have in place policies defining the following:[25]

(A) To what confidential information individuals have access;

(B) Who can request the information;

(C) The procedures for requesting information;

(D) The time frames for responding to a request;

(E) When the covered entity can deny access; and

(F) How an individual may appeal a decision to deny access.

(3) **Amendment of Confidential Information**: An individual has a right to have a covered entity amend confidential information about the individual so long as the covered entity maintains the information. The written policies must conform to the Privacy Rule requirements and must address:[26]

(A) The process for accepting a request for and making an amendment of confidential information;[27]

(B) How quickly a covered entity must respond to an amendment request;[28]

(C) How to proceed if the originator of the information is no longer available; and

(D) The process for denying a request for amendment.[29]

---

[25] *See* 45 CFR §164.524.

[26] *See* 45 CFR §164.526.

[27] *See* 45 CFR §164.526(b)(1).

[28] *See* 45 CFR §164.526(b)(2).

[29] *See* 45 CFR §164.526(d)(1).

(4) **Accounting for Disclosures**: Individuals have a right to receive an accounting of all disclosures of confidential information. Disclosure information must be made available for a six (6) year period. A record of disclosure does not have to be made when those disclosures are:

(A) To carry out treatment, payment or health care operations;

(B) To individuals of confidential information about them;

(C) For the covered entity's directory or to persons involved in the individual's care;

(D) For national security or intelligence purposes; or

(E) To correctional institutions or law enforcement personnel.

(5) **Complaints to the Covered Entity**: A covered entity must provide a process for individuals to make complaints concerning the entity's policies and procedures required under the privacy rule.[30] The entity must:

(A) Have a procedure in place to document all complaints received, and their disposition, if any; and

(B) Work to mitigate any problems known to the entity.

(6) **Waiver of Rights**: A covered entity may not require an individual to waive his/her rights under the privacy rule as a condition of the provision of treatment.[31]

II. Government Requirements:

---

[30] *See* 45 CFR §164.530(d)(1).

[31] *See* 45 CFR §164.530(h)

(1) **Uses and Disclosures of Confidential Information**: The policy manual must reflect and be consistent with the Notice of Privacy Practices, the Consent Form, and the Authorization Form. The policy manual must also reflect and implement policies regarding the following:

(A) Fund Raising Restrictions;[32]

(B) Marketing Restrictions;[33]

(C) "Minimum Necessary" Provisions;[34]

(D) "De-Identification" of Confidential Information;[35]

(E) Exceptions to the requirement to obtain Consents or Authorizations;[36]

(F) Uses and Disclosures for when an Authorization is required;[37] and

(G) Consent for uses and disclosures to carry out treatment, payment or health care operations.[38]

(2) **Business Associates**: Before a covered entity may disclose confidential information to a business associate, it must obtain satisfactory assurances that the business associate will appropriately safeguard the information. The assurances must be provided in a written contract or agreement that

---

[32] 45 CFR §164.514(f)(1).

[33] 45 CFR §164.514(e)(1).

[34] 45 CFR §164.514(d)(1).

[35] 45 CFR §164.514(a)-(b).

[36] 45 CFR §164.512.

[37] 45 CFR §164.508.

[38] 45 CFR §164.506.

documents the permitted and required uses and disclosures of confidential information by the business associate. The contract between the covered entity and the business associate must meet the explicit requirements set out in the Privacy Rule at 45 CFR §164504(e)(2) or (e)(3).

(3) **Mitigation**: A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the entity of a use or disclosure of confidential information in violation of its policies or procedures or the requirements of the rule or any of its business associates.[39]

(4) **Refraining from Intimidating or Retaliatory Acts**: A covered entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals or others for any reason.[40]

(5) **Ensuring Confidential Information is Secure**: A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of confidential information.[41]

(6) **Training**: Covered entities must train all members of its workforce on the policies and procedures with respect to confidential information, as necessary and appropriate for each member of the workforce to carry out his/her function within the entity.[42] The training must:

---

[39] *See* 45 CFR §164.530(f).

[40] *See* 45 CFR §164.530(g).

[41] *See* 45 CFR §164.530(c).

[42] *See* 45 CFR §164.530(b).

(A) be provided to each member of the workforce by no later than the compliance date for the entity;

(B) be provided thereafter, to each new member of the workforce within a reasonable period of time after the person joins the entity's workforce; and

(C) be provided to each member of the entity's workforce whose functions are affected by a material change in the policies or procedures required by this rule, within a reasonable period of time after the material change becomes effective.

(7) **Sanctions**: A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the entity and the requirements of the rule.[43]

Phase Four Check-List

- ❑ HIPAA compliant Consents, Authorizations, Notice of Privacy Practices and Business Associate Contracts have been developed
- ❑ All policies and procedures mandated by the Privacy Rule have been developed and implemented
- ❑ All appropriate personnel have been trained regarding the new privacy practices, policies and procedures
- ❑ All business associate contracts have been enacted
- ❑ Safeguards for protecting the privacy of PHI have been adopted

[43] *See* 45 CFR §164.530(e).

V. Phase 5: Troubleshooting and Auditing

After a covered entity finishes the implementation process, the entity should provide itself time to adjust to the new policies, procedures and administrative requirements of the HIPAA regulations. The final compliance deadline is April, 2003 and any deviation from the requirements after that point would be considered a violation of HIPAA. The penalties for a covered entity's failure to abide by HIPAA's guidelines can mean harsh civil monetary and/or criminal penalties.[44] The criminal penalties for violating the HIPAA privacy standards state:

> a. Offense.—
>
> A person who knowingly and in violation of this part—
> (1) uses or causes to be used a unique health identifier;
> (2) obtains individually identifiable health information relating to an individual; or
> (3) discloses individually identifiable health information to another person,
> shall be punished as provided in subsection (b).
>
> b. Penalties.—
>
> A person described in subsection (a) shall—
> (1) be fined not more than $50,000, imprisoned not more than 1 year, or both;
> (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and
> (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both."[45]

There are also civil penalties for violating HIPAA's privacy guidelines. The civil penalties include fines of $100 for each violation, up to a maximum of $25,000 for violating a particular requirement of the law.[46]

---

[44] HIPAA's enforcement provisions are found at 24 USC §§ 1320d-5 & 1320d-6

[45] 42 USC §1320d-6.

[46] 42 USC §1320d-5.

In addition to initially making sure your organization complies with the Privacy Rule by April 2003, the Privacy Rule also requires organizations to continually audit their compliance. The continuing compliance responsibility of covered enitities, once an effective compliance plan is implemented, requires the following of covered entities:

(1) Covered entities must keep records and reports documenting compliance;

(2) Covered enitities must cooperate with the Secretary of Health and Human Services [hereinafter the "Secretary] if the Secretary decides to to review the polices, procedures or practices of the covered entity; and

(3) Covered entities must permit the Secretary access to its records and facilities if the Secretary undertakes such a review.[47]

Phase Five Check-List

- ❑ All requirements of the Privacy Rule have been identified, implemented and all implementation problems identified and solved
- ❑ Internal audit process has been developed and implemented

Conclusion

Undoubtedly HIPAA's privacy provisions will drastically change how most covered entities interract with eachother, with the government and with patients. The Privacy Rule requires that these changes be documented. However, because the DHHS has not yet provided covered entities with a model HIPAA privacy compliance plan, organization's must review the Privacy Rule requirements and tailor a compliance plan to fit the organiation's individual needs. The five phases

[47] 45 CFR § 160.310.

identified in this paper should guide your organization through this process. Once the process is complete, your compliance plan should contain at least the following elements:

(1) Privacy Officer designation;

(2) Documented and implemented privacy policies.

(3) Workforce training regarding the organization's privacy policies and procedures;

(4) Safeguards adopted to protect PHI;

(5) Complaint process established for privacy violations;

(6) Organizational ban on retaliation against individuals for privacy complaints;

(7) Sanctions for privacy violations;

(8) Organizational procedures to lessen the harmful effect of damage from known privacy violations; and

(9) Organizational acknowledgement regarding an indivuals unwaivable right to complain.

Bibliography

1. Portions of this paper were drawn extensively from information on the the following websites:

- http://snip.wedi.org: Webiste contains information and white papers regarding HIPAA compliance.
- http://www.hipaa-u.com: Website provides a model compliance program.
- http://www.healthkey.org: Funded by the Robert Woods Johnson Foundation, HealthKey is an ehealth initiative that focuses on HIPAAs privacy and security standards.

GREENEBAUM

A "Nuts & Bolts" Workshop on HIPAA
HIPAA Transaction Issues

Compliance with HIPAA Transaction Standards and Code Sets Regulation

- Compliance Deadline: October 16, 2002
- "Administrative Simplification Compliance Act" pushed compliance to October 16, 2003 if you submit a compliance plan to HHS no later than October 16, 2002.
- Government's compliance form to be accessible by March 31, 2002 at:
  - http://www.aspe.hhs.gov/admnsimp/
- Helpful HIPAA websites:
  - http://www.hipaa-iq.com
  - http://www.hipaadvisory.com

GREENEBAUM

Transaction Standards Compliance Plans

- Compliance plans must summarize the following:
  - An analysis reflecting the extent to which, and the reasons why, the entity is not in compliance;
  - A budget, schedule, work plan, and implementation strategy for achieving compliance;
  - Whether the entity plans to use or might use a contractor or other vendor to assist the entity in achieving compliance; and
  - A time frame for testing that begins no later than April 16, 2003.

GREENEBAUM

Enforcement of Deadline

- Covered entities that fail to submit compliance plans are required to comply with the electronic standards no later than the original deadline of October 16, 2002.
- Failure to comply and/or submit a compliance plan may mean exclusion from Medicare in addition to all other penalties permissible under HIPAA.
- DOES NOT affect the April 2003 compliance date for privacy.

GREENEBAUM

Compliance with HIPAA Privacy Regulation

- Effective Date – April 14, 2001
- Compliance Date – April 14, 2003

GREENEBAUM

Covered Entity Compliance with HIPAA Privacy Regulation

- Appoint a privacy official and a privacy contact.
- Develop, implement and document privacy policies and procedures.
- Train workforce on privacy.
- Adopt privacy safeguards for protected health information.
- Establish a complaint process for privacy violations.
- No retaliation allowed against individuals for privacy complaints.
- Set sanctions for privacy violations.
- Lessen harmful effects of damage from known privacy violations.
- No waiver of individual right to complain allowed.

GREENEBAUM

Phase I – Overview and Initiation of Program

- Begin educating Board/Trustees and upper management about HIPAA compliance and its potential impact.
- Identify key individuals within the organization to form a HIPAA Steering Committee.
- Appoint a privacy official. This person will oversee and coordinate training and compliance programs.
- Become familiar with the privacy requirements and identify the types of information that are protected.
- Review your state's applicable law. HIPAA is a baseline standard. Your state may require more.
- Assess impact on budget.
- Begin internal risk assessment of business – consider engaging legal counsel in order to invoke attorney/client privilege

GREENEBAUM

Phase II – Risk Assessment and GAP Analysis

- Collect all existing privacy policies and procedures regarding the handling of and access to private health information.
- Take inventory of data repositories where patient information is generated, stored, received or transmitted. Even palm pilots and personal computers may be repositories of PHI. Determine what PHI is collected, how it is maintained, who has access and how it is being used/disclosed.
- Make risk assessments. What services do you provide? What types of PHI do you routinely handle? What privacy precautions do you currently have in place?
- Begin working with legal counsel to develop basic HIPAA compliant business associate contracts and consent and authorization forms.

GREENEBAUM

Phase II – Risk Assessment and GAP Analysis

- Prepare checklist as guidance by using Phase I list of HIPAA requirements.
- Prepare GAP analysis in order to develop priorities, work plans and budgets.
- Put together an organizational chart and have HIPAA Steering Committee members work with senior management to characterize types of business lines the organization engages in and how information flows in and out of the organization.
- Prepare budgets to fund technological requirements, education, training and risk protection.

GREENEBAUM

Phase II – Risk Assessment and GAP Analysis

- Research:
  - Review research practices of the institution, IRB and individual researchers:
    - Schools
    - Departments
    - Labs
    - Protocol-by-protocol
  - Decide whether IRB will also function as a Privacy Board.
  - If Privacy Board is used, coordinate its examination of protocols with the IRB.
  - Revise consent forms currently being used to take advantage of transition rules.
    - Consent should specifically allow use/disclosure of subject's PHI for research purposes and for TPO.

GREENEBAUM

Phase III – Management Review

- Sit down with management in order to gain organizational consensus and set priorities.

GREENEBAUM

Phase IV – Compliance Implementation

- Prepare HIPAA compliance forms including consent, authorization and business associate forms and develop notices regarding individual patients' privacy rights.
- Begin developing a privacy compliance plan by establishing detailed, written privacy policies and procedures, making sure to reserve the right to revise the policies and procedures as needed due to changes in the law.

GREENEBAUM

Phase IV – Compliance Implementation

- Develop policies to ensure disclosure of the "minimum necessary" PHI as required by the final rule. Put in place procedures to deal with routine and recurring disclosures as well as a system to evaluate unique requests and disclosures. Personnel may be classified into groups according to the information they handle, and types of information created.
- Implement appropriate administrative, technical and physical safeguards to protect the privacy of PHI.
- Develop and negotiate required business associate contracts with third parties that provide services to the covered entity.

GREENEBAUM

Phase IV – Compliance Implementation

- Develop a policy and procedure mechanism to allow individuals to inspect and copy their PHI.
- Train workforce on privacy policies and procedures; document the training. Create education and communication programs for employees as a defensive measure to help minimize employee misunderstandings of patients' rights and avoid erroneous claims of privacy violations.
- Develop record-keeping systems to track and monitor access to and handling of protected information.
- Create security agreements/affidavits for signature by employees handling protected information.

GREENEBAUM

Phase IV – Compliance Implementation

- Include HIPAA compliance in the development of future business strategies.
- Review all existing insurance policies with respect to coverage of inappropriate uses or disclosures of health information.
- Establish a system to report privacy complaints, including the designation of a contact person or office that is responsible for receiving complaints and able to provide further information.
- Develop quick response procedures to investigate potential privacy breaches.
- Develop and apply discipline procedures for individuals and business associates who are found to have breached policies.

GREENEBAUM

Phase 9 - Troubleshooting and Auditing

- Mitigate, to the extent possible, the harmful effects of the inappropriate disclosure of PHI known to the covered entity or its business associates.
- Implement a process for the ongoing auditing and monitoring of the organization's privacy initiative and workforce training program.
- Leave a period of time in order to adjust to new policies and procedures and to make adjustments.

GREENEBAUM

Penalties

Penalties for violations:

- No private cause of action.
- Civil or criminal penalties possible.
  - Civil: $100 per violation up to $25,000 per person, per year for each negligent violation.
  - Criminal: penalties from $50,000 - $250,000 and 1 to 10 years in prison can be imposed for knowingly violating the Act.

GREENEBAUM

AMENDMENT OF PROTECTED HEALTH INFORMATION

Dennis P. Kennedy
Deters, Benzinger & LaVelle, P.S.C.
Covington, Kentucky

Copyright 2002. Dennis P. Kennedy. All rights reserved.

SECTION F

Amendment of Protected Health Information

- 45 CFR 164.526
- 1 Standard: The Right to Amend
- 5 Implementation Specifications
  1) Requests and timely action
  2) Accepting the amendment
  3) Denying the amendment
  4) Actions on notice of amendment
  5) Documentation

Standard: The Right to Amend

- Right to Amend
  - As long as PHI is maintained in the designated record set
- Denial of Amendment (4 grounds)
  1) PHI not created by Covered Entity
  2) PHI not part of the designated record set
  3) PHI not available for inspection under 164.524
  4) PHI is accurate and complete

Requests for Amendment

- Individual's Request
  - Covered Entity must allow requests
  - Covered Entity may require written requests for amendment to be made in writing

Deters, Benzinger & LaVelle, P.S.C.
2701 Turkeyfoot Road
Covington, KY 41017
(859) 341-1881

Timely Action

- Covered Entity must act within 60 days if:
  - Amendment granted, take action;
  - Amendment denied, provide notice
- If unable, extend for 30 days
  - Provide:
    - Reasons for delay;
    - Date by which Covered Entity will complete its action on the request;
- Only one extension permitted

Accepting the Amendment

- If amendment is accepted
  1) Either append or provide a link to the amendment.
  2) Inform the individual
  3) Inform others

Denying the Amendment

- 5 Components to the Denial
  1) The denial
  2) Statement of disagreement
  3) Rebuttal statement
  4) Recordkeeping
  5) Future disclosures

Deters, Benzinger & LaVelle, P.S.C.
2701 Turkeyfoot Road
Covington, KY 41017
(859) 341-1881

Denial

- Timely denial must be provided (60 days)
  - In writing
  - Plain language
  - Basis for denial
  - A statement regarding future disclosures
  - A description of the complaint process under 164.530

Statement of Disagreement

- Individual must be allowed to submit a written statement of disagreement
- Covered Entity may limit the length

Rebuttal Statement

- Covered Entity may prepare in response to individual's statement of disagreement
- Provide a copy to the individual

Deters, Benzinger & LaVelle, P.S.C.
2701 Turkeyfoot Road
Covington, KY 41017
(859) 341-1881

Recordkeeping

- Identify the record or PHI subject to disagreement
- Append or link the correspondence regarding the amendment to the designated record set

Future Disclosures

- If a statement of disagreement has been submitted:
  - Covered Entity must include the request and its denial (or a summary of such information) with any subsequent disclosure
- If no statement of disagreement has been submitted:
  - A Covered Entity is required to provide such information upon further disclosure only if individual requested such action.

Actions on Notices of Amendment

- A Covered Entity informed by another Covered Entity of an amendment must amend the PHI

Deters, Benzinger & LaVelle, P.S.C.
2701 Turkeyfoot Road
Covington, KY 41017
(859) 341-1881

Documentation

- Document titles of persons or offices responsible for receiving and processing requests for amendments
- Retain documentation

Questions & Answers

Deters, Benzinger & LaVelle, P.S.C.
2701 Turkeyfoot Road
Covington, KY 41017
(859) 341-1881

BUSINESS ASSOCIATES

Carole D. Christian
Wyatt, Tarrant & Combs, LLP
Louisville, Kentucky

Copyright 2002. Carole D. Christian. All rights reserved.

SECTION G

BUSINESS ASSOCIATES

I. PERMISSIVE USE OF PROTECTED HEALTH INFORMATION G-1

II. DEFINITION OF BUSINESS ASSOCIATE G-1

III. EXCLUSIONS FROM DEFINITION G-2

IV. REQUIRED ASSURANCES G-3

A. Written Contracts Must G-3

B. Written Contracts May G-4

C. Other Assurances G-4

D. Legally Required Business Associate Action G-4

V. MEASURING COMPLIANCE G-4

VI. CHANGES FROM PROPOSED RULE G-5

VII. OPTIONAL CONTRACT PROVISIONS TO CONSIDER G-5

VIII. COVERED ENTITY PLANNING CONCERNS G-6

IX. "CHAIN OF TRUST AGREEMENT" G-6

SAMPLE BUSINESS ASSOCIATE AGREEMENT G-9

BUSINESS ASSOCIATES

Carole D. Christian, Esq.
Wyatt, Tarrant & Combs, LLP
Suite 2700, PNC Plaza
500 West Jefferson Street
Louisville, Kentucky 40202
(502) 562-7588

I. Permissive Use of PHI: A Covered Entity may:

(1) Disclose protected health information ("PHI") to a business associate and

(2) Allow a business associate to create or receive PHI on its behalf

if the Covered Entity obtains satisfactory assurance that the business associate will safeguard the information. 45 CFR § 164.502 (e)(1).

II. Definition of Business Associate: (45 CFR § 160.103) With respect to or on behalf of a Covered Entity, but excluding members in the workforce of the Covered Entity, a person who:

[A] performs or assists in the performance of a function or activity involving the use or disclosure of individually identifiable health information.

Examples include:

- claims processing or administration
- data analysis
- utilization review
- quality assurance
- billing
- benefit management
- practice management
- repricing
- any other activity regulated by HIPAA

[B] provides any of the following specifically listed services to or for a Covered Entity if the service involves the disclosure of individually identifiable health information by the Covered Entity or another Business Associate.

- legal services
- actuarial services
- administrative Services
- accounting Services
- management Services
- consulting Services
- data aggregation (defined in 45 CFR § 164.501)
- financial services
- accreditation

A Covered Entity may also be a Business Associate of another Covered Entity.

III. Exclusions from Definition. Requirement for a written agreement does not apply to:

[A] Disclosures by a Covered Entity to a health care provider concerning the treatment of an individual.

[B] Disclosures by a group health plan or a health insurance issuer or HMO with respect to a group health plan to the plan sponsor, as long as the plan documents properly restrict such disclosures (see 45 CFR § 164.504).

[C] Disclosures to members of Covered Entity's workforce, "Workforce" means employees, volunteers, trainees and others whose work is under the "direct control" of the Covered Entity, whether or not paid. "Direct Control" requirement may exclude independent contractors and board members. (45 CFR § 160.103).

[D] Entities that perform services as part of an "organized health care arrangement," i.e., clinically integrated setting in which patients receive care from multiple health care providers.

[E] Entities that are merely conduits for information (e.g., U.S. Postal Service, electronic equivalents, couriers)

[F] A financial institution that is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling or collecting payments, e.g. credit card payment processing, check clearing, processing electronic funds transfer. (Distinguish from an institution operating an accounts payable system or other "back office" function on behalf of provider.)

IV. Required Assurances. 45 CFR § 164.504. Except in a few instances in which "other arrangements" are authorized (see below), a Covered Entity must enter into a written contract with a Business Associate in order to document satisfactory assurances that health information will be protected.

A. Written contracts must:

[1] Establish the permitted and required uses and disclosures of such information by the Business Associate. Disclosures can be identified by type or purpose. Note: Preamble states that covered entities may rely on the professional judgment of their business associates as to the type and amount of protected health information that is necessary to carry out a permitted activity.

[2] Authorize termination if the Covered Entity determines that the Business Associate has violated a material term of the contract, unless such termination is inconsistent with statutory obligations of either party.

[3] Provide that the Business Associate will:

[a] not use or disclose the information except as permitted by the contract or as required by law;

[b] use appropriate safeguards to prevent unpermitted use or disclosure of the information;

[c] report to the Covered Entity any use or disclosure of the information not allowed for by the contract of which the Business Associate becomes aware;

[d] ensure that any agent or subcontractor of the Business Associate who receives or creates protected health information on behalf of the Covered Entity agrees to the same contractual restrictions.

[e] honor the right of access by an individual to his own records upon request (see, 45 CFR § 164.524)

[f] make available protected health information for amendment and incorporate amendments into record (see, 45 CFR § 164.526)

[g] make available information required to provide an accounting of disclosures (see, 45 CFR § 164.528)

[h] make its internal practices, books, and records received from or created for the Covered Entity available to the Secretary for the purpose of determining the Covered Entity's compliance

[i] return or destroy all protected health information belonging to the Covered Entity at the termination of the contract, if feasible, or, if not, extend life of the contract and limit further uses and disclosures to necessary use.

B. Written Contracts May allow for uses by the Business Associate for the proper management and administration of the Business Associate or to carry out its legal responsibilities. It may allow for disclosures by the Business Associate (acting as a Business Associate) for the same purposes if disclosure is required by law; or if the Business Associate obtains reasonable assurances that the recipient will protect confidentiality and the recipient is required to notify the Business Associate of any breach. 45 C.F.R. 164.504(e)(4).

C. Other Assurances: If the Covered Entity and Business Associate are both governmental entities, they may enter a "Memorandum of Understanding" instead of contract. Alternatively, the Covered Entity may be governed by other laws (including promulgated regulations) that achieve the same objectives.

D. Legally Required Business Associate Action. If a Business Associate is required by law to perform a service on behalf of a Covered Entity, the Covered Entity may disclose information necessary to meet the legal requirement without giving assurances, if it documents inability to obtain satisfactory assurances from Business Associate in spite of good faith efforts.

V. Measuring Compliance.

A Covered Entity is noncompliant with the regulations if the Covered Entity knew of a pattern of activity or practice of the Business Associate that violated the contract, unless the Covered Entity took action to cure the breach. 45 CFR § 164.504(e).

"Knowledge" is not defined in the regulation but the preamble suggests it is triggered by "substantial and credible evidence."

If actions to cure the Business Associate's breach are unsuccessful the Covered Entity must:

[1] if feasible, terminate the contract

[2] if not feasible, report the problem to the Secretary. Feasibility is tested by whether there are viable alternatives, not whether other options are less convenient or more costly.

VI. Changes from Proposed Rule (see 65 Fed. Reg. 82503 to 82507; (Dec. 28, 2000)).

A. "Business Associate" instead of "Business Partner."

B. No third-party beneficiary language.

C. Expanded ability to disclose PHI for treatment purposes (rather than limitation to consultation or referral).

D. Excludes disclosure by group health plan satisfying 45 CFR § 164.504(f) to plan sponsor.

E. Reduced monitoring of Business Associates. "Reasonable steps to ensure" compliance removed; now focus is on curing breach.

F. Termination following violation required only "if feasible."

G. Permits "data aggregation" by Business Associate using data from multiple Covered Entities.

VII. Optional Contract Provisions to Consider:

- Detail concerning permissible uses, security and access controls
- Provision for Covered Entity to inspect records, security controls
- Procedures for Business Associate and Covered Entity to follow in event of request by individual for access or amendment
- Appendix for Business Associate to use in contracting with other entities
- Provisions for segregation of PHI in records of Business Associate
- Method of reporting known violations..

- Detail concerning Covered Entity's rights to enforce cure in event of breach
- Methods for Business Associate's disposal of information
- Indemnification provisions; Business Associate may want to consider getting subcontractor to indemnify for loss of Covered Entity's business due to violation.
- Coverage of Covered Entity as named insured on Business Associate's policies
- Effect of changes making law more onerous; necessity for new agreement
- "Placeholder provisions" - right to require a contract in the event contractor of uncertain status is deemed to be Business Associate

VIII. Covered Entity Planning Concerns.

A. Timing - Contracts being renewed now may not be reviewed again until after effective date
- Business Associate identification will affect other compliance, e.g. scope of authorization forms

B. Contractors Without Written Contracts

- May hamper identification
- Getting contract executed may be a change in the culture of relationship, take time

C. Contract Cross-Referencing, e.g., Stark II requirement that contracts between parties to personal services arrangements be in same document or cross-reference each other.

D. Monitoring Business Associates - What affirmative duties should privacy officer have?
- How to capture "Knowledge" of violation by employees who don't have a direct compliance function

E. "Whistle blowers" - Preamble notes that Business Associate may be a whistle blower on Covered Entity even though Business Associate is not directly required to correct violations.

IX. "Chain of Trust Agreement" - The proposed rules for Security and Electronic Signature Standards, 63 Fed. Reg 43241 (August 12, 2998) would require health plans and covered health care clearinghouses (i.e., those entities covered in proposed rule 45 CFR § 142.302) who transmit information to other persons electronically to have in place agreements in which both sender and

recipient agree to protect the integrity and confidentiality of the data. See also, definition of "Chain of Trust Partner Agreement" in Glossary, 63 Fed. Reg. 43272 (August 12, 1998).

- Scope of terms "Business Associate" and "Chain of Trust Partner" will overlap

- Little guidance available yet on Chain of Trust Agreements.

- Recommend requirement to comply with terms applicable to Chain of Trust partners in any Business Associate agreements entered now, if information will be exchanged electronically.

SAMPLE BUSINESS ASSOCIATE AGREEMENT
proposed by Wyatt, Tarrant & Combs, LLP
Suite 2700, PNC Plaza
500 West Jefferson Street
Louisville, Kentucky 40202
(502) 589-5235

This Agreement is entered into on this _____ day of _____, 2002, between _____ and _____.

WHEREAS, _____ is a "covered entity" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and any regulations promulgated thereunder or any amendment thereof;

WHEREAS, the parties' existing business relationship requires _____ to disclose to _____ , information that is confidential and must be afforded special treatment and protection in accordance with HIPAA, and the regulations promulgated thereunder at 45 CFR Parts 160 and 164;

NOW, THEREFORE, the parties agree as follows:

Section 1. Definitions. The following terms shall have the meaning ascribed to them in this Section.

a. *Business Associate* shall refer to _____.

b. *Covered Entity* shall refer to _____.

c. *HIPAA Privacy Regulations* shall mean the Code of Federal Regulations (C.F.R.) at Title 45, Parts 160 and 164.

d. *Protected Health Information or "PHI"* shall means any information, whether oral or recorded in any form or medium (i) that relates to the past, present or future physical or mental 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 (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term found at 45 C.F.R. § 164.501.

e. *Parties* shall mean Business Associate and Covered Entity.

f. *Secretary* shall mean the Secretary of the Department for Health and Human Services ("HHS") and any other officer or employee of HHS to whom the authority involved has been delegated.

Section 2. Business Associate's Rights and Obligations:

The Parties anticipate that, during the term of this Agreement, Business Associate will provide __[DESCRIBE SERVICES TO BE PROVIDED BY BUSINESS ASSOCIATE]__ Business Associate hereby agrees that it shall be prohibited from using or disclosing any PHI provided or made available to it by Covered Entity for any purpose other than the following _[LIST PERMISSIBLE USES AND DISCLOSURES; MAY BE LISTED BY TYPE OR PURPOSE]_

a. *Permitted Uses and Disclosures.* [Optional] In addition to the foregoing, Business Associate may use and/or disclose PHI provided or made available from Covered Entity as follows:

(1) Business Associate may provide data aggregation services relating to the health care operations of Covered Entity to Covered Entity;

(2) Business Associate may use or disclose PHI received by Business Associate in its capacity as a business associate to Covered Entity, if necessary (i)for the proper management and administration of Business Associate; or (ii) to carry out the legal responsibilities of Business Associate; provided, however, that Business Associate may disclose PHI for such purposes only if the disclosure is made in its capacity as a Business Associate and: (i) the disclosure is required by law; or (ii) Business Associate obtains reasonable assurances from the person to whom PHI is disclosed that [A] the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed; [B] the person will use appropriate safeguards to prevent use or disclosure of the information; and [C] the person will notify Business Associate of any instances of which it is aware that the confidentiality of the PHI has been breached.

b. *Obligations.* Without limiting the obligations of Business Associate under this Agreement or imposed by law, Business Associate agrees to comply with the HIPAA Privacy Regulations as they apply to this Agreement. Specifically, Business Associate shall:

(1) Not use or further disclose PHI disclosed to Business Associate by Covered Entity other than as permitted or as required by this Agreement or as required by law;

(2) Establish and maintain safeguards, including protection of the physical security of any records and electronic access to any computerized records, to prevent the use or disclosure of PHI, other than as provided for by this Agreement;

(3) Immediately report to Covered Entity any use or disclosure of PHI not allowed by this Agreement of which Business Associate becomes aware. In addition,

Business Associate shall take prompt corrective action to mitigate the effect of any unauthorized use or disclosure and to prevent recurrence.

(4) Ensure that any agents, including subcontractors, to whom Business Associate provides PHI received from, or created or received by Business Associate on behalf of, Covered Entity, enter a written agreement containing the same restrictions and conditions that apply to Business Associate with respect to PHI;

(5) Make PHI available: [A] to the individual whose PHI is at issue, in accordance with 45 C.F.R. § 164.524, as amended; [B] for amendment, and incorporate any amendments to PHI, in accordance with 45 C.F.R. § 164.526, as amended; and [C] to the extent it is required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528, as amended; and

(6) Make Business Associate's internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by, Business Associate on behalf of Covered Entity, available to the Secretary for the purpose of determining Covered Entity's compliance with the HIPAA and HIPAA Privacy Regulations promulgated thereunder or any amendments thereof.

Section 3. Amendment. The Parties acknowledge that the HIPAA Privacy Regulations may be modified from time to time. The Parties specifically agree to take such action as necessary to implement the standards and requirements of HIPAA, HIPAA Privacy Regulations and other applicable laws relating to the security and confidentiality of PHI. Upon Covered Entity's request, Business Associate agrees to promptly enter into negotiations with Covered Entity concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of HIPAA, HIPAA privacy regulations or other applicable law. Covered Entity may terminate this agreement and any other agreements between the parties upon [30] days' written notice in the event (i) Business Associate does not promptly enter into negotiations to amend this Agreement when requested by Covered Entity pursuant to this section, or (ii) Business Associate does not enter into an amendment to this Agreement providing assurances regarding the safeguarding of PHI that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of HIPAA or the HIPAA Privacy Regulations. Nothing herein shall be deemed to extend the term of any other Agreement between the parites.

[Alternative: The parties acknowledge that the HIPAA Privacy Regulations may be modified from time to time and that Covered Entity may be required by law to amend this Agreement as a condition of doing business with Business Associate. In the event of any amendments to HIPAA or the Privacy Regulations, Business Associate acknowledges that Covered Entity may notify it, in writing, of required additional terms that Covered Entity believes are necessary to amend this Agreement. Such terms shall amend and become part of this Agreement unless Business Associate objects, in writing, to the notice

provided by Covered Entity within thirty (30) days. In the event of such objection, the parties shall negotiate diligently and in good faith a mutually agreeable amendment to this Agreement. If the parties cannot reach agreement and Covered Entity reasonably determines that this Agreement without amendment will not satisfy its obligations under law, it may terminate the parties' relationship on thirty (30) days' written notice, except that nothing herein shall be deemed to extend the term of any other agreements between the parties].

Section 4. Termination.

a. *Material Breach.* Business Associate agrees that Covered Entity may terminate this Agreement, and any other agreements between the parties that require the disclosure of PHI, immediately if Covered Entity determines that Business Associate has violated a material term of this Agreement.

b. *Reasonable Steps to Cure Breach.* Alternatively, if Covered Entity learns of an activity or practice of Business Associate that could constitute a material breach or violation of its obligations under this Agreement, Covered Entity may make a demand that Business Associate take reasonable steps to cure such breach or end such violation, as applicable. If Business Associate fails to cure such breach or end such violation within thirty (30) days of notice, Covered Entity shall either: (i) terminate this Agreement and any other agreements between the parties requiring the disclosure of PHI, if feasible for Covered Entity, or (ii) if termination of this Agreement is not feasible, Covered Entity shall report Business Associate's breach or violation to the Secretary.

c *Effect of Termination.* Upon termination of the Agreement, for any reason, Business Associate shall return or destroy all PHI received from, or created and received by Business Associate on behalf of Covered Entity. Business Associate agrees not to retain copies of the PHI after termination of this Agreement. If return or destruction of the PHI is not feasible, Business Associate agrees to extend the protections of this Agreement for as long as necessary to protect the PHI, but Business Associate shall not use or disclose PHI except for the limited purposes for which extended retention of such records is necessary. If Business Associate elects to destroy the PHI, it shall certify to Covered Entity that the PHI has been destroyed.

Section 5. Indemnification. [Optional] Each Party will indemnify, hold harmless and defend the other party to this Agreement from and against any and all claims, losses, liabilities, costs, and other expenses incurred as a result of, or arising directly or indirectly out of or in connection with: (i) any misrepresentation, breach, or non-fulfillment of any undertaking on the part of the Party under this Agreement; and (ii) any claims, demands, awards, judgements, actions and proceedings made by any person or organization arising out of or in any way connected with the Party's performance under this Agreement.

Section 6 Binding Nature and Assignment. This Agreement shall be binding on the Parties and their successors and assigns, but neither Party may assign this Agreement without the prior written consent of the other, which consent shall not be unreasonably withheld.

Section 7. Interpretation. This Agreement shall be interpreted as broadly as necessary to implement and comply with HIPAA, the HIPAA Privacy Regulations and applicable state laws. The Parties agree that any ambiguity shall be resolved in favor of a meaning that complies and is consistent with HIPAA and the HIPAA Privacy Regulations.

IN WITNESS WHEREOF, Business Associate and Covered Entity have caused this Amendment to be signed and delivered by their duly authorized representatives, as of the date set forth above.

BUSINESS ASSOCIATE	**COVERED ENTITY**
_____	_____
BY:	**BY:**
ITS:	**ITS:**

HIPAA

MARKETING & FUNDRAISING:
What's Covered & What's Not?

Janet A. Craig
and
Jennifer L. Elliott
Stites & Harbison PLLC
Lexington, Kentucky

Copyright 2002. Janet A. Craig, Jennifer L. Elliott. All rights reserved.

SECTION H

Janet A. Craig
Jennifer L. Elliott
STITES & HARBISON PLLC
250 West Main Street
Suite 2300
Lexington, Kentucky 40507
(859) 226-2377
Email: jcraig@stites.com

HIPAA

MARKETING & FUNDRAISING: WHAT'S COVERED & WHAT'S NOT?

1. DEFINITIONS OF KEY TERMS H-1

a. Covered Entity H-1
b. Healthcare Operations H-1
c. Protected Health Information H-1

2. BACKGROUND ON HIPAA PRIVACY RULES AND CONSENT AND AUTHORIZATION REQUIREMENTS H-1

a. Basic HIPAA Privacy Requirement H-1
b. Permitted Uses And Disclosures H-2
c. Consents H-2
d. Authorizations H-2
e. Consent or Authorization? H-4

3. MARKETING H-6

a. Definition of Marketing and Exceptions H-6
b. Marketing Rules H-7
   i. General Rule H-7
   ii. Exceptions from Authorization Requirement H-8
c. Business Associates H-9
   i. Business Associates in General H-9
   ii. Disclosures to Business Associates for Marketing H-9

4. FUNDRAISING H-10

a. Permissible Fundraising Purposes H-10
b. Only Limited Protected Health Information May Be Used Or Disclosed H-10
c. Opt Out Provision H-11
d. Notice of Fundraising Practices H-11
e. Disclosures to Business Associates and Institutionally Related Foundations H-11

5. ENDNOTE H-12

1. DEFINITIONS OF KEY TERMS

(a) **Covered Entity**: Health plans; health care clearinghouses; and health care providers who transmit any health information in electronic form in connection with a covered transaction.

(b) **Healthcare Operations**: "any of the following activities of the covered entity to the extent that the activities are related to covered functions . . . (1) conducting quality assessment and improvement activities . . . (2) reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance . . . accreditation, certification, licensing, or credentialing activities; (3) underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance . . . (4) conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs; (5) business planning and development . . . and (6) business management and general administrative activities of the entity, including, but not limited to . . . *fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in § 164.514(a)(2)."* 42 C.F.R. § 164.501.

(c) **Protected Health Information**: generally "means individually identifiable health information[1] "that is transmitted by electronic media . . . or transmitted or maintained in any other form or medium." 42 C.F.R. § 164.501.

2. BACKGROUND ON HIPAA PRIVACY RULES AND CONSENT AND AUTHORIZATION REQUIREMENTS

(a) Basic HIPAA Privacy Requirement

The basic requirement of the final privacy rules (" Privacy Rules") is simply stated as follows: "A covered entity may not "use" or "disclose" [both terms broadly defined] an individual's protected health information, except as otherwise permitted or required by this subpart." 42 C.F.R. § 164.502(a). Fully understanding the definitions of who (covered entity)

[1] "Individually identifiable health information" is defined as health information "including demographic information collected from an individual, and: (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." 42 C.F.R. § 164.501.

and what (protected health information) are covered is the first step to being able to comply with this complex regulatory mandate

(b) Permitted Uses and Disclosures

A health care provider is permitted to use and disclose protected health information only as follows:

(i) To the individual who is the subject of the protected health information;

(ii) In compliance with the consent or authorization provided by the individual;

(iii) Without the consent or authorization of the individual, if not required under the rules;

(iv) Pursuant to an agreement with the individual under §164.510 which only requires that the individual have an opportunity to agree or object.

(c) Consents

The final Privacy Rules require a "consent" for uses and disclosures of protected health information for purposes of treatment, payment, and health care operations. Health care providers and other covered entities must obtain a separate "authorization" (discussed below) from the individual to use and disclose protected health information for other purposes. While the terms "consent" and "authorization" have often been used interchangeably in the health care context, they are defined terms under the Privacy Rules and differ substantially in their content. A "consent" is written in general terms and allows a health care provider to use or disclose protected health information only for treatment, payment, or health care operations purposes. There are a few minor exceptions to this general rule. For example, health care providers may use or disclose protected health information without a consent (1) in an emergency, (2) if required by law, (3) if the patient is an inmate, (4) or if the provider has an indirect treatment relationship with the patient.

(d) Authorizations

Unless an exception applies, a provider must obtain a patient's authorization to use or disclose protected health information for any reason *other than* treatment, payment, or healthcare operations. For example, if a provider wants *to request* protected health information

from another provider, the patient must first sign a valid "authorization" form. While the request may be for the purpose of treatment, a consent form only covers "uses and disclosures" of patient information created by that particular provider. *See* 65 Fed. Reg. 82,511.

Providers generally cannot condition treatment on a patient's signing of an authorization. Authorizations must be written in specific terms and are only valid if they contain the specific elements set out in the Privacy Rules. Therefore, most handwritten patient authorizations to release records will be invalid under the new rules as they will not contain an expiration date or a statement about the individual's right to revoke the authorization.

(e) Consent or Authorization?

Consent	Authorization
Purpose: To carry out Treatment, Payment, and Healthcare Operations ("TPO").	**Purpose**: To use or disclose protected health information for purposes other than TPO.
Exceptions: 1. Indirect treatment relation, 2. For inmates, 3. In emergency treatment situations, 4. If required by law to treat an individual, and where there are substantial communication barriers. (Attempt made to obtain consent and reason why consent was not obtained should be documented.)	**Inclusion**: A consent for uses and disclosures of protected health information is required for TPO. For use and disclosure beyond TPO, a specific authorization is required.
Conditioning: Provider *may* condition treatment on provision of consent.	**Conditioning**: A provider *may not* condition treatment or payment on an authorization except for research-related treatment and when the disclosure is necessary to determine payment of a claim.
Combination: 1. A consent may not be combined with the Notice of Privacy Practices. A consent may be combined with other types of legal permissions (e.g., informed consent for treatment) if it is visually and organizationally separate from the other permission, is separately signed. 2. Where there are conflicting consents, the more restrictive applies. Provider may attempt to resolve the conflict with a new consent or obtaining the individual's designated preference.	**Combination:** An authorization *may not* be combined with any other document except: 1. An authorization for protected health information created for research that includes treatment of the individual; 2. An authorization for the use or disclosure of psychotherapy notes may only be combined with another authorization for the use or disclosure of psychotherapy notes; or 3. An authorization may be combined with another authorization when the provision of treatment or payment has not been conditioned on the provision of one of the authorizations.

Consent	Authorization
Expiration: None	**Expiration**: Date or event that relates to the individual or purpose of use required. If expiration date not provided for, then authorization is defective.
Retention: Signed consent forms must be retained for six years.	**Retention**: Signed authorizations must be retained for six years.
Content requirements: 1. Inform individual in plain language of that protected health information may be used and disclosed for TPO, 2. Refer individual to Notice of Privacy Practices for more complete information and state that the individual has the right to review the Notice prior to signing the Consent, 3. State terms of Notice may change, if applicable, and describe how the individual may obtain a revised Notice, 4. State that individual has right to request restrictions but covered entity is not required to agree with request but if it does so, must abide by request, 5. State that the individual has the right to revoke the consent except to the extent that action has already been taken, and 6. Be signed and dated by the individual.	**Content requirements**: 1. Description in plain language of information to be used or disclosed that identifies the information in a specific and meaningful fashion, 2. Name or other identification of person or class of persons authorized to make the requested use or disclosure or to whom the provider may make the requested use or disclosure, 3. An expiration date or event, 4. A statement of the individual's right to and description of how to revoke the authorization, 5. A statement that information may be subject to redisclosure by the recipient and no longer be protected by the rule, 6. Signature and date, and (if signed by a personal representative) a description of representative's authority.
Defective consents: Are not valid and are those lacking any element of the content requirements.	**Defective consents**: Expiration date that has passed, is incomplete, has been revoked, lacks a required element, or contains information known to be false.
	Additional requirements: Specific to whether the authorization is for the provider to request information, others are requesting information from the provider, or the authorization is for research related to treatment.

3. MARKETING

In the proposed privacy regulations issued in November 1999, the Department of Health and Human Services (the "Department" or "HHS") would have required covered entities (i.e. health care providers, health plans, and health care clearinghouses) to have obtained an individual's "authorization[2]" prior to using or disclosing "protected health information" to market items and services. The final Privacy Rule is less restrictive, yet more complex.

The Privacy Rule establishes a general rule (subject to a few exceptions) that covered entities must obtain an individual's authorization before using or disclosing health information for marketing. 42 C.F.R. § 164.514(e). The term "marketing" is now defined and specifically excludes certain activities from its scope. The excepted activities are encompassed by the definitions of treatment, payment and health care operations. Covered entities, may therefore, use and disclose protected health information for these excepted activities pursuant to a general consent under 42 C.F.R. § 164.506 if required, rather than an authorization under 42 C.F.R. § 164.508. *See* 65 Fed. Reg. 82,462, 82,493 (Dec. 28, 2000).

(a) Definition of Marketing and Exceptions: 42 C.F.R. §164.501

"Marketing" is a "communication about a product or service a purpose of which is to encourage recipients of the communication to purchase or use the product or service." 42 C.F.R. § 164.501. It is important to note that if a covered entity receives direct or indirect remuneration from a third party for making a written communication, then the communication is not excluded from the definition of marketing. By definition, the following communications by a covered entity (which would otherwise meet the general definition of marketing) are not deemed marketing so long as they are either (1) made *orally* or (2) made in writing *if the covered entity does not receive direct or indirect remuneration* from a third party for making the communication:

(1) Communications by a covered entity for the purpose of describing the entities participating in a health care provider network;

(2) Communications by a covered entity for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits;

[2] *See discussion supra* at Part 2; 42 C.F.R. § 164.508.

(3) Communications by a covered entity that are tailored to the circumstances of a particular individual and the communications are made by a health care provider or health plan to an individual as part of the treatment of the individual and for the purpose of furthering the treatment of the individual; *OR*

(4) Communications by a covered entity that are tailored to the circumstances of a particular individual and the communications are made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

The Department explains that these exceptions express their intent "not to interfere with communications made to individuals about their health benefits . . . . [and] their treatment." 65 Fed. Reg. 82,493. The first two exceptions permit health plans to inform enrollees about which doctors and hospitals are preferred providers and are included in its network; about which providers offer a particular service; and that a new pharmacy has begun to accept its drug coverage. The third exception permits a provider to recommend specific brand-name or over-the-counter pharmaceuticals and to refer patients to other providers. The fourth exception permits a provider to send reminder notices for appointments, annual exams and prescription refills or to inform a smoker about an effective smoking-cessation program, even if that program is offered by someone other than the provider making the recommendation. *See* Office of Civil Rights, Health-Related Communications and Marketing Guidance at http://www.hhs.gov/ocr/hipaa/marketing.html (July 6, 2001).

(b) Marketing Rules: 42.C.F.R. § 164.514(e)

(i) **General Rule**:

A covered entity may not use or disclose protected health information for marketing without an authorization. § 164.514(e)(1). For example, a hospital or other provider may not provide patient lists to pharmaceutical companies for those companies' drug promotions without an authorization from each patient on the list. HHS assumes that the "requirement for obtaining authorizations for use or disclosure of protected health information for most marketing activity will make direct third-party marketing more difficult because covered entities may not want to obtain and track such authorizations, or they may obtain too

few to make the effort economically worthwhile." 65 Fed. Reg. 82,771.

(ii) **Exceptions from Authorization Requirement**

(1) Marketing communications that occur in a *face-to-face encounter* with the individual (e.g. sample products may be provided to a patient during an office visit);

(2) Marketing communications that concern products or services of *nominal value* (e.g. a provider can distribute pens, toothbrushes or key chains with the name of the covered entity or a health care product manufacturer on it); *OR*

(3) Marketing communications that concern the *health-related products and services* of the covered entity or of a third party, but only if the communication:

a. Identifies the covered entity that is making the communication;

b. Prominently states that the covered entity is receiving direct or indirect remuneration for making the communication, if applicable;

c. Except in the case of a general communication (e.g. newsletter), tells individuals how to opt-out of further marketing communications. The covered entity must make reasonable efforts to honor requests to opt-out;

d. Explains why individuals with specific conditions or characteristics (e.g. diabetics, smokers) have been targeted, if that is so, and how the product or service relates to the health of the individual. The covered entity must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted.

HHS clearly contemplates the final Privacy Rule permitting "an alternative arrangement: the covered entity can engage in health-related marketing on behalf of a third

party, presumably for a fee. Moreover, the covered entity could retain another party, through a business associate relationship, to conduct the actual health-related marketing, such as mailings or telemarketing, under the covered entity's name." 65 Fed. Reg. 82,771.

(c) Business Associates

(i) **Business Associates in General**

A Business Associate relationship arises when the right to use or disclose protected health information belongs to the "covered entity" (e.g. health care provider) and another person is using or disclosing that information to perform a function on behalf of, or to provide services to, that covered entity. Examples of business associates are firms conducting claims processing or administration; data analysis; utilization review; quality assurance; billing; practice management; or legal, accounting, management, administrative, accreditation, or financial services. In general, a covered entity or health care provider may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information, if the use or disclosure is permitted by the Privacy Rule. However, in order to disclose protected health information to its business associates, covered entities must obtain satisfactory assurances through written agreements ("business associate contracts") that the business associate will appropriately safeguard the information.

The required business associate contractual provisions include (1) limitations on the business associate's further use and disclosure of protected health information, (2) a requirement that the business associate must make the protected health information available for amendment and for audit of disclosures, (3) reporting requirements regarding any improper use or disclosure of which a business associate becomes aware, (4) the use of appropriate safeguards to comply with the contract and (5) a requirement that agents or subcontractors who receive protected health information from the business associate will also comply. The contract must also (6) require the return or destruction of all protected health information at termination of the contract, if feasible.

(ii) **Disclosures to Business Associates for Marketing**

Disclosure of protected health information for marketing purposes is limited to disclosure to business associates that undertake marketing activities *on behalf of the covered entity*. No other disclosure for marketing is permitted. Covered entities may not give away or sell lists of patients or enrollees without obtaining authorization from each person on the list. As with any disclosure to a business associate, the covered entity must obtain the

business associate's agreement to use the protected health information only for the covered entity's marketing activities. A covered entity may not give protected health information to a business associate for the business associate's own purposes.

4. FUNDRAISING: 42 C.F.R. § 164.514(f)

In the proposed privacy regulations issued in November 1999, the Department would have required covered entities to obtain authorizations from an individual in order to use his/her protected health information for fundraising activities. In the final Privacy Rule, certain "fundraising" activities on behalf of a covered entity are classified as health care operations[3] which would only require general consent. The Department modified the proposed rule after receiving comments arguing that the proposed rule would have adversely effected charitable giving. Additionally, it is worth noting that the fundraising provision is not limited to nonprofit covered entities. HHS considered comments, but ultimately rejected the proposition stating: "We do not agree that the profit status of a covered entity should determine its allowable use of protected health information for fundraising. Many for-profit entities provide the same services and have similar missions to not-for-profit entities. Therefore, the final rule does not make this distinction." 65 Fed. Reg. 82,718.

(a) Permissible Fundraising Purposes

Under the final Privacy Rule, a covered entity may use or disclose limited protected health information without an authorization for the sole *purpose of raising funds for its own benefit*. Permissible fundraising activities include appeals for money and sponsorship of events. HHS made clear in commentary that royalties and remittances for the sale of products of third parties are generally not considered permissible purposes. *See* 65 Fed. Reg. 82,718.

(b) Only Limited Protected Health Information May Be Used or Disclosed

Covered entities *may only use the following protected health information* without an authorization: 1) demographic information[4], and 2) dates health care services were provided.

---

[3] "Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions . . . : business management and general administrative activities of the entity, including, but not limited to . . . fundraising for the benefit of the covered entity." 42 C.F.R. § 164.501.

[4] "Demographic information" is not defined in the rule, but HHS noted that it "will generally include in this context name, address and other contact information, age, gender, and insurance status. The term does not include any information about the illness or treatment." 65 Fed. Reg. 82,718.

42 C.F.R. § 164.514(f)(1). Sensitive information such as diagnosis, nature of services, or treatment and other condition-specific information may not be used or disclosed.

(c) Opt Out Provision

Additionally, fundraising materials must include a description of how the individual may opt out of receiving any further fundraising communications, and covered entities are required to honor such requests. *Id.* § 164.514(f)(2)(ii)-(iii).

(d) Notice of Fundraising Practices

Finally, a covered entity may not take advantage of this provision for fundraising unless the covered entity's Notice of Privacy Practices clearly states that it may contact the individual to raise funds. *See id.* §§ 164.514(f)(2)(i); 164.520(b)(1)(iii)(B).

(e) Disclosures to Business Associates and Institutionally Related Foundations

Covered entities are permitted to disclose this limited protected health information, consistent with section 164.514(f), to "business associates" for fundraising on its own behalf and to an "institutionally related foundation." The "institutionally related foundation" provision was added to "accommodate tax code provisions which may not allow such foundations to be business associates of their associated covered entity." *See* 65 Fed. Reg. 82,718. In commentary, HHS explains that:

> By "institutionally related foundation," we mean a foundation that qualifies as a nonprofit charitable foundation under section 501(c)(3) of the Internal Revenue Code *and* that has in its charter statement of charitable purposes an explicit linkage to the covered entity. An institutionally related foundation may, *as explicitly stated in its charter,* support the covered entity as well as other covered entities or health care providers in its community. For example, a covered hospital may disclose for fundraising on its own behalf the specified protected health information to a nonprofit foundation established for the specific purpose of raising funds for the hospital or to a foundation that has as its mission the support of the members of a particular hospital chain that includes the covered hospital. *The term does not include an organization with a general charitable purpose,* such as to support research about or to provide treatment for certain diseases, that may give money to a covered entity, because its charitable purpose is not specific to the covered entity.

65 Fed. Reg. 82,546 (emphasis added).

5. ENDNOTE

While the new Privacy Rules are final, HHS has indicated that they make modify or change certain requirements in the future: "Congress specifically authorized HHS to make appropriate modifications in the first year after the final rule took effect in order to ensure the rule could be properly implemented in the real world. We are working as quickly as we can to identify where modifications are needed and what corrections need to be made so as to give covered entities as much time as possible to implement the rule." Office of Civil Rights, General Overview at http://www.hhs.gov/ocr/hipaa/genoverview.html (July 6, 2001). On July 6, 2001, HHS issued its first set of guidance to answer common questions and clarify confusion about the final Privacy Rule's provisions. *See* Office of Civil Rights, Technical Guidance at http://www.hhs.gov/ocr/hipaa/assist.html (July 6, 2001).

Additionally, the National Committee on Vital and Health Statistics ("NCVHS"), Subcommittee on Privacy and Confidentiality, has held a public hearings to receive information from the public on implementation of the Privacy Rule's provisions for use and disclosure of health information for marketing and fundraising. The NCVHS is a statutory public advisory body to the Secretary of HHS in the area of health data, statistics, and health information policy and advises the Secretary on the implementation of HIPAA. *See* 42 U.S.C. § 242k(k). Transcripts of recent public hearings as well as committee and subcommittee meetings may be found at www.ncvhs.hhs.gov.