PROGNOSIS

Volume 17, Number 2 ■ March 2001 ■ www.ncbar.org
PUBLISHED BY THE NCBA'S HEALTH LAW SECTION & THE NORTH CAROLINA SOCIETY OF HEALTH CARE ATTORNEYS

NORTH CAROLINA BAR ASSOCIATION
SEEKING LIBERTY & JUSTICE

HIPAA Privacy Regulations

Oh Brother! *What* Art Thou?*

BY ROY H. WYMAN

Attorneys typically predict the effect of a new statute or regulation by dissecting the language and considering how it might be applied to various situations. A complex analysis impacting many actors predicts a broad, complex application in reality.

The final HIPAA privacy regulations, however, do not easily lend themselves to straightforward dissection and analysis. Even a cursory review of the more than 1,500 pages of the regulations reveals a wide landscape of open and obvious challenges, the shadows of battles half-hidden and an endless variety of hiding places for the unknown.

For most "covered entities" other than small health plans, the implementation date for the regulations currently is April 14, 2003. Small health plans are granted an extra year. Given the complexity of the regulations, however, covered entities that do not begin preparation immediately may find themselves unprepared, in violation of the regulations, or otherwise at risk.

To gain an idea of the regulations' scope and requirements, this article briefly describes the range

See **Regulations** *page 3*

**With apologies to the Coen Brothers*

HIPAA Privacy Rule

New Requirements for Law Firm Engagements

BY MIKE HUBBARD

Fast forward to May 2003. Dr. Jones calls her lawyer, Mr. Smith, to seek legal advice regarding a surgery that Jones performed. Jones believes that the patient may file a medical malpractice lawsuit. Later the same day, Jones calls Smith again to seek his assistance in collecting a past-due account from another patient. Jones discloses patient health information to Smith in both calls. Jones has not obtained a written consent from these patients to disclose their health information, and Smith does not have a written engagement letter or agreement with Jones.

Six months later, the local assistant United States attorney is considering criminal prosecution of Jones for allegedly violating federal standards for the privacy of patient health information during the calls to Smith. Jones is shocked to learn that if she is indicted and convicted, the assistant United States attorney may request the court to impose a fine of up to $50,000 and one year in prison for the disclosure of health information regarding the potential malpractice plaintiff, and possibly a fine of up to $250,000 and 10 years imprisonment for the disclosure relating to her collection efforts.

Putting aside the uncertain grace of prosecutorial interest and discretion, the Jones hypothetical presents significant issues regarding how the new federal privacy standards will affect lawyers' relationships with their health industry clients.[1]

On Dec. 28, 2000, pursuant to a mandate under the "Administrative Simplification" provisions of the Health Insurance Portability and Accountability Act of 1996[2] (HIPAA), the United States Department of Health and Human Services (HHS) issued new standards for the privacy of individually identifiable health information (Privacy Rule).[3] These new standards will have widespread application throughout the health care industry.

The Privacy Rule establishes a compliance deadline for most covered entities of Feb. 26, 2003.[4] "Covered entities" include, among many others, physicians, hospitals, pharmacies,

See **Rule** *page 8*

Inside This Issue ...

PROGNOSIS

Vol. 17, No. 2
March 2001

Published by the NCBA's Health Law Section & the North Carolina Society of Health Care Attorneys

Co-Editors
Dean M. McCord
Patricia A. Markus

Editorial Address
PO Box 3688
Cary, NC 27519

Section Features Key Issues in Spring Events

The Chair's Comments ...

By Robert L. Wilson Jr.

The Health Law Section has a busy spring calendar of events that should offer outstanding educational opportunities to all members of the section with a wide variety of interests. First, please make plans now to attend the Annual Meeting on April 27 at the Sheraton Imperial Hotel in Research Triangle Park. Program Planners Carol Bowen and Cindy Turco have done an outstanding job in preparing a timely program, titled *New Developments in Health Law*.

Among a number of current topics of interest, the Annual Meeting will address the new health care-related regulations promulgated in the last weeks of the Clinton administration, including HIPAA and the Stark II final regulations. The meeting also will address current North Carolina certificate of need issues and, for the first time, provide a bankruptcy primer for health care attorneys. Please look for the program brochure in the mail and register early for this excellent continuing legal education opportunity.

The section's other educational opportunity this spring is our *Rural Health Symposium*, sponsored by the section for its membership, other members of the North Carolina Bar Association, and for members of the health care industry and the public who have an interest in rural health issues. The *Symposium* will be held at Monroe Auditorium at FirstHealth Moore Regional Hospital in Pinehurst on May 16 from 10 a.m. until 3 p.m. While not intended as a traditional continuing legal education program, the *Symposium* seeks to bring together experts on rural health from the areas of government, community care, hospitals and mental health to discuss critical issues involved in the delivery of health care to rural areas in North Carolina.

Panelists from each of these sectors not only will identify the issues involved, but will talk about the challenges that have been overcome already and the hurdles of the future. Please make your plans now to attend this unique offering by the Health Law Section as a part of its service to the public this year. Section Vice Chair Curtis Venable has put together an excellent, thought-provoking assortment of panelists for the *Symposium*, and the section needs your support of this first-time educational opportunity.

The Health Law Section Council has enjoyed planning the Annual Meeting and the *Rural Health Symposium* for you this year. Your participation in these key section activities will make them a true success. If any section members would like more information on these activities, please contact any council member, or e-mail me at *bob_wilson@shmm.com*. □

N.C. Society of Health Care Attorneys

President	Sandra van der Vaart
Vice President	James A. Wilson
Secretary-Treasurer	Forrest Campbell
Immediate Past President	Gary S. Qualls
Directors	Barry Bloch, Mike Hubbard, Nancy Mason, Ed Meyer, Patricia Markus and Bill Shenton

Always wanted to be a writer?

Great! Your section needs you. Getting information to fellow members is the key role of NCBA section newsletters and what you have to say is important. Your contribution of articles, ideas and timely case updates is welcomed by newsletter editors. If you have something to add, please contact the editor.

Regulations

from page 1

of people and entities that are affected. This "who," however, is first answered by addressing a definition: "protected health information."

Scope: Who Should Care?

Protected health information (PHI) is defined as "individually identifiable health information," which includes health information received or created by a "covered entity" that 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 … and identifies the individual or with respect to which there is a *reasonable basis* to believe the information can be used to identify the individual." (Emphasis added) 45 C.F.R. § 164.501.[1]

Significantly, in the proposed regulations, PHI was relevant only if it was at any time transmitted or stored in *electronic form* (*e.g.*, typed into a computer or transmitted via facsimile). Under the final regulations, however, PHI exists when "transmitted or maintained in any … form or medium." *Id.* Thus, PHI may be created under circumstances in which no information is converted to electronic format or even written down. Conversations between a doctor and nurse, a billing company representative and a hospital administrator, or a patient and a hospital janitor regarding a person's health, health care provided to that person or billing for such health care all may include the transfer of PHI.

Covered Entities

The regulations require compliance by "covered entities," which include health plans, health care clearinghouses and health care providers. 45 C.F.R. §§ 160.102, 103. We might assume, based upon this cursory review, that the regulations are the concern solely of providers, insurers, and those handling billing, but we shall soon see otherwise.

A "health care provider" includes "any … person or organization who furnishes, bills or is paid for health care in the normal course of business." § 160.103. "Health care clearinghouses" include entities that take health information received from another entity in a nonstandard format and convert it into standard data elements and those who do the opposite — take standard data and turn it into nonstandard (but user-friendly) content. § 160.103.

In short, a prototypical clearinghouse might receive health information (generally from providers), revise the data and send it out to payors of health care costs. "Health plans" include "an individual or group plan that provides, or pays the cost of, medical care," including group health plans, health insurance issuers, HMOs, the Medicare and Medicaid programs, issuers of Medicare supplemental policies, issuers of long-term care policies, employee welfare benefit plans, a variety of other federal and state programs for the payment of health costs, and "any other individual or group plan … that provides or pays for the cost of medical care." § 160.103.

Business Associates

"Business Associates" include persons who: (i) assist a covered entity in the performance of a function or activity involving the use or disclosure of individually identifiable health information; or (ii) provide legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to or for a covered entity if the service involves the disclosure of individually identifiable health information.

The definition does not, however, include members of the covered entity's "workforce," who are addressed as part of the covered entity. A covered entity's workforce includes employees, volunteers, trainees and others whose conduct is under the direct control of the entity. In some instances, independent contractors may be part of the workforce. While a member of a covered entity's workforce is not a "business associate," the categories of "covered entity" and "business associate" are not mutually exclusive. A covered entity may also be a business associate of another covered entity.

Although non-covered entities are outside the scope of HIPAA, the final regulations require covered entities to enter into written agreements with business associates *ensuring confidentiality* of PHI. Accordingly, lawyers, accountants, consultants, management companies and others who traffic regularly in PHI must comply with the regulations to stay in business. Many attorneys will be called on to comprehend HIPAA not only in advising clients but also in ordering their own affairs.

The Net of HIPAA

Many statutes may be thought of as similar to a sword. The point of the sword — its prohibition — is singular and supported by definitions, exceptions and refinements that serve to sharpen and make useful the prohibition itself. HIPAA, by contrast, can be compared to a net: the regulations contain no single prohibition, but, like a net, a number of knots, each knot a separate prohibition bound to other knots by the common strings of definitions and concepts.

The most significant knots include requirements relating to notice, the need to inform, consents, authorizations, business associate contracts, organizational reform and policies, disclosure of PHI and amendment of PHI. The strings tying each of these knots together include concepts such as "minimum necessary," affiliations, the safety of persons and special protections for psychotherapy notes and the conduct of research. Due to space constraints, this article highlights only in the roughest terms the general knots and strings of the regulations.

Knot 1: Notice

An individual has a right to notice regarding: (i) the uses and disclosures of PHI that may be made by a covered entity; (ii) the individual's rights; and (iii) the entity's legal duties. 45 C.F.R. § 164.520. This notice must be in plain language. The introduction to the regulations suggests that a covered entity may need to provide the notice in a variety of languages. The notice must include its effective date, which

See **Regulations** *page 4*

from page 3

may not be earlier than the date it is published. In addition, the notice must be generally available, provided on request, and posted prominently in the offices of healthcare providers. Where a provider treats an individual electronically (*e.g.*, via e-mail), the notice must be provided electronically at the commencement of care.

Health plans must provide notice to individuals covered by the plan no later than the plan's compliance date, thereafter at the time of enrollment of an individual, and upon any revision to the notice. In addition, once every three years a health plan must notify individuals covered by the plan of the availability of the notice.

Most covered entities within a given area and providing a common service may adopt the same or similar notice. Thus, numerous organizations such as trade organizations and those addressing privacy and healthcare technology concerns likely will draft model notices for use by a number of covered entities (in fact, the American Hospital Association already has drafted a model notice policy for hospitals).

Knot 2: The Need to Inform

All individuals within the sphere of a covered entity must have access to a notice. Other disclosures may not be equally mandated. Certain relatively public information may be revealed by health care providers operating a health facility in order to maintain a directory for those hoping to locate friends and family within the facility. Similarly, clergy may wish to locate those patients within the cleric's faith who require compassionate visitation. Under such circumstances, a general assent by an individual to be included in a directory sufficiently protects the individual's need for privacy.

The final regulations allow a provider to include patient information in the facility's directory if it informs incoming patients of its policies regarding a directory, permits the patient to opt out of the directory, and the patient does not object to inclusion. 45 C.F.R. § 164.510. Information that may be disclosed includes the individual's location within the facility and general condition. In addition, the facility may disclose to clergy the individual's name, general condition, location in the facility and religious affiliation. Unlike a member of the general public, a clergy member need not request an individual by name. *Id.*

Similarly, providers may release certain PHI under very particular circumstances where the individual requesting the information has an obvious need to know the information and consent may be inferred or is otherwise not deemed necessary. For example, an individual wishing to pick up prescription medications on behalf of a friend or relation may do so, and that person's possession of the prescription implies a relationship of trust and the patient's intent that the information included with the prescription be disclosed. A second example is a friend who assists an individual in traveling home from the hospital. If there are particular medical concerns in transporting the patient, a member of the facility's workforce may inform the friend of such concerns. The very presence of the friend again implies consent to reveal such information. Such implied consent only applies to one event, however. Should the same friend return to the facility alone the next day requesting further information regarding the patient's condition, the regulations would appear to preclude the disclosure of such information. 65 FR 82523.

Knot 3: The Need for Consent

The vast majority of individuals will gladly consent to disclosure of PHI for common purposes relating to the care of the individual or payment by third parties. Unlike the proposed regulations, however, the final regulations require that a patient execute a consent for the use or disclosure of such information. Once an individual executes a consent, the covered entity receiving such consent may then use or disclose the PHI to the extent permitted by the consent. At most, a consent may grant the covered entity the right to use or disclose the individual's PHI for treatment, payment, or health care operations. 45 C.F.R. §164.501.
In the absence of a proper consent, any use or disclosure of PHI by the covered entity violates the statute.

Knot 4: Authorizations

Authorizations represent the most specific level of acquiescence the regulations require. Any use or disclosure of PHI not permitted by the previously discussed knots will require an authorization. An authorization is intended to apply where a covered entity wishes to use PHI for a purpose that would not otherwise be allowed by a consent or by merely informing the individual of the use. As such, an authorization may permit almost any legal disclosure, so long as the authorization otherwise meets the requirements of the regulations. 65 FR 82517. Thus, for example, although a consent will allow a covered entity to use or disclose PHI in attempting to secure payment, one wishing to send marketing materials to the individual must first obtain an authorization from the individual.

Knot 5: Business Associates

A covered entity may "disclose" PHI under a number of circumstances. Even though a covered entity properly has and may disclose PHI, it may not do so to a "business associate" unless the covered entity and business associate have a contract containing particular provisions. The definition of business associate is quite broad and delineated at the beginning of this article. We simply reiterate that a covered entity may also be a business associate, and so a business associate agreement may be required in the disclosure of PHI between covered entities. The business associate contract must set forth several matters which are addressed in another article in this issue.

Where disclosure is permitted under an authorization to an entity not performing such functions, the business associate requirements become irrelevant. For example, an individual executes a consent for a provider to use PHI in order to collect payment. The provider hires a lawyer to assist it in collecting amounts from a third party payor in litigation. The lawyer is a business associate, and the cov-

ered entity may not disclose PHI except pursuant to a business associate contract. The lawyer then discloses the PHI to an expert witness, who will not be serving the functions of the lawyer, i.e., "on behalf of the covered entity." The expert witness serves the business associate, not the provider, and therefore is not within the definition of a business associate. Nonetheless, the regulations require that the lawyer make assurances that any agents agree to the same restrictions applicable to the business associate. 45 C.F.R. §164.504(e)(2)(ii)(D). While one might resolve such conflict by asserting that the expert witness is not an agent of the lawyer, such resolution strikes one as less than satisfying. Where a covered entity knows that the business associate is violating the contract, the covered entity no longer complies with the regulations if it continues to disclose PHI to the business associate. This standard constitutes a loosening of the proposed regulations, which placed affirmative duties on the covered entity regarding potential violations of the contract.

Knot 6: Organizational Requirements

The sixth knot sets forth the manner by which the organization must conform to the other knots of the regulations.

Personnel Matters

Under the regulations, a covered entity must designate two individuals: a privacy official and a person or office to receive complaints. The duties of the former are to ensure compliance with the regulations, and the duties of the latter are to act appropriately when individuals complain that the organization has not complied with privacy requirements. In addition, a covered entity must train all members of its workforce regarding policies and procedures relating to PHI prior to the compliance date of the entity. Thereafter, each new member of the workforce must be trained within a reasonable time after hire, and all workforce members must be retrained within a reasonable time after a change in the regulations or a change in the entity's policies. Training must be documented.

Safeguards

Perhaps one of the greatest costs of the regulations will be in the requirement that the covered entity have appropriate administrative, technical and physical safeguards protecting the privacy of PHI. If the covered entity fails to protect against any intentional *or unintentional* use or disclosure, a violation occurs. The impact of this requirement will vary from eliminating sign-in sheets to placing locks and security systems in rooms where records are stored. The level of security required will vary depending on the entity and its risks.

Complaints

The covered entity must create a process whereby people may complain regarding activities of the entity. All such complaints must be documented and acted upon as appropriate. Any failure to comply must be met with sanctions. For example, should a physician group discover that one of its physicians improperly disclosed to his wife that he treated a local celebrity, the group must sanction the physician using meaningful penalties and then mitigate any harm to the "extent practicable." The manner of determining what mitigation is practicable is not set forth in the regulations. The regulations provide that a covered entity may not retaliate against a person who complains or reports the entity's violations.

Policies

Finally, the regulations require that each covered entity cre ate its own additional policies regarding PHI. The policies must be amended as the regulations change. For example, a policy will likely need to set forth in sufficient detail how each type of PHI in each location within a covered entity will be protected.

Knot 7: When Disclosure Is Required or Otherwise Approved

The regulations assume that PHI, under certain circumstances, not only *may* be disclosed, but *should* be disclosed. The regulations, to this end, set forth circumstances where disclosure is tolera ted, promoted, or even required.

De-identified Information

De-identified information may be disclosed, insofar as it is not PHI. De-identified information is defined as "health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual…" A covered entity may either contract with a person with "appropriate knowledge and experience" to opine that the risk is "very small" that the information could be used to identify an individual who is the subject of the PHI. Alternatively, if certain identified information is removed from a record or if appropriate encryption methods are used, then one may assume that the risk of identifying the subject individual is very small.

Whistleblowers and Crimes

The regulations further permit disclosure of information when: (i) a crime takes place at the location of a provider; (ii) a victim of a crime is unable to consent to disclosure; and (iii) whistleblowers notify appropriate agencies of fraud and abuse by a covered entity. Each of these exceptions includes a number of requirements too lengthy to address here.

Public Good

The regulations approve a third set of disclosures to benefit the public good, including disclosures to disaster relief agencies in the case of a natural disaster and disclosures permitted in order to report abuse or neglect of individuals. An important exception applies to family members and friends of an individual where the individual may not consent to the disclosure.

Disclosures Mandated by Law

A number of appropriate disclosures are actually mandated. These include, among others, disclosures to the Secretary pursuant to an investigation, disclosures mandated by State law and disclosures pursuant to a court order. Particular provisions also apply to responses to subpoenas.

Disclosure to an Individual.

Also mandated are disclosures to an individual upon

See **Regulations** *page 6*

Regulations

from page 5

his request. Should the individual request a copy of his medical record or other PHI, the covered entity must disclose the same with certain exceptions and limitations. The regulations specify what information must be provided, where and when such information is to be provided, as well as appeal rights in case of denial.

Where, What and When

PHI may be provided at a mutually convenient time and place, which may be negotiated between the covered entity and individual. In the alternative, the covered entity may mail the PHI to the individual. If the covered entity does not maintain the PHI requested, but knows where the PHI is maintained, the covered entity must inform the individual of where to direct the request for access.

The covered entity must provide the record of the entity containing the PHI requested. Obviously, if more than one copy is retained, only one copy need be provided. In addition, if agreed upon by the individual, the covered entity may provide a summary of the record rather than the entire record. The covered entity may charge the individual for the reasonable costs of preparing such summary, as well as any copying or postage costs.

Within 30 days of receiving a request for PHI, a covered entity must grant the access, provide a written denial of the access or send a written extension of no more than 30 days explaining the reasons for the delay and the date by which it will complete one of the above actions.

The Exceptions

Inmates of a correctional institution may be denied a copy of records containing PHI if granting a copy of the records could jeopardize the health, safety, security, custody or rehabilitation of the individual or of other inmates. In addition, a covered entity may deny any and all *access* to PHI in the case of: (i) psychotherapy notes; (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action; (iii) PHI maintained by a covered entity that is subject to CLIA or in situations in which disclosure could make the entity subject to CLIA; and (iv) PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access would reveal the source of the information. Access may be limited temporarily if the PHI was created in the course of research including treatment and the individual agreed to a limit on access (*e.g.*, a double-blind study in which access to information would perhaps reduce the value of results of the study).

Access may be denied, but the individual requesting access may seek an independent review of such denial, where: (i) a licensed health care professional has determined that the access is reasonably likely to endanger the *life or physical safety* of the individual or another person; (ii) the PHI refers to another individual, and a professional has determined that the access would be reasonably likely to cause substantial harm (of any variety) to such other person; or (iii) a personal representative has made the request, and a health care professional determines that the provision of access is reasonably likely to cause substantial harm to the individual or another person.

Denial

If a covered entity denies an individual's request for access, and such denial is reviewable, the individual may request that an independent licensed health care provider, who did not participate in the original determination, review the determination.

Knot 8: Amendment of PHI

The final regulations grant an individual the right to request an amendment to her PHI. 45 C.F.R. § 164.526. The covered entity may deny the request only if: (i) the PHI was not created by the covered entity unless the originator is no longer available to act; (ii) the PHI to be amended is not part of the individual's records held by the covered entity; (iii) the individual would not have a right to access to the records; or (iv) the PHI, prior to amendment, is accurate and complete.

A covered entity must respond within 60 days by amending the record, denying the amendment in writing or extending the deadline no more than 30 days. In the event that an amendment is denied, the individual has a right to either submit a written statement disagreeing with the denial (which will be attached to the record) or have a copy of the request for amendment and denial included with any future disclosures of the PHI. In any event, the individual may file a complaint with the covered entity and / or the secretary. If the individual files a statement of disagreement, the covered entity may include with the statement a rebuttal statement, both of which are to be included with the record.

Strings

The very substance of our HIPAA net — the strings — are summarized briefly.

String A: Minimum Necessary

When providing or requesting PHI, a covered entity must make "reasonable efforts" to limit PHI to the "minimum necessary to accomplish the intended purpose of the use, disclosure or request." 45 C.F.R. § 164.502. "Minimum necessary" will apply to a disclosure pursuant to a consent or an authorization. Likewise, a disclosure to a business associate may well be limited by the concept of minimum necessary. A few exceptions exist: disclosures to or requests by a health care provider for treatment; disclosures to an individual under the individual's right to access; required disclosures to the secretary; certain other disclosures required by law; and disclosures required for compliance with the regulations themselves.

The final regulations significantly modify the proposed rules to require a covered entity to create policies regarding the minimum necessary standard including appropriate members of the workforce with access to particular types of PHI. Covered entities will no longer be permitted to simply release the entirety of a medical record for any purpose. Instead, the entity must determine the minimum necessary amount of information needed to meet the needs of the entity requesting PHI (or the minimum necessary to meet its own needs).

String B: Affiliations

Affiliated entities under a number of circumstances

may publish a single notice form. For example, a physician providing services at a hospital as a member of its staff may rely upon a notice form of the hospital. Of course, the physician will need to comply with, and agree to, the provisions contained in the notice. The notice would not, however, apply to the same physician's office practice.

Similarly, the regulations address entities that are more formally integrated. One variety of such entities is termed a "hybrid" entity. A hybrid entity is "a single legal entity that is a covered entity and whose covered functions are not its primary functions." The regulations find that application of HIPAA to the entirety of a large entity simply because a relatively insignificant portion of its business is related to health care would be unfair. Instead, merely that portion of the business relating to PHI will be subject to the regulations. A second variety of an integrated entity is described at 45 § C.F.R. 164.504(d), which permits legally distinct covered entities that share common ownership or control to designate themselves, or their health care components, together as a single covered entity.

Finally, entities that provide more than one service (*e.g.*, clearinghouse services, provider services and insurance services) will need to keep various functions separate. As noted above, plan sponsors may not allow the use of PHI for employment decisions. Likewise, as an example, an insurer offering a staff model HMO service could not use PHI derived by its staff physicians in order to make decisions regarding continuation of HMO benefits to a particular individual.

String C: Safety of Persons

The regulations make several exceptions for situations in which a person may be endangered. Similarly, a number of exceptions and rules are created addressing the needs of law enforcement — both under enforcement of the regulations and the enforcement of other laws. For example, the regulations address, among others, the following matters: disclosure of PHI to enforcement agencies for enforcement of HIPAA; disclosure of criminal conduct at the location of a provider; withholding of required disclosures to protect the health and safety of individuals; and disclosure of PHI regarding an individual who is the victim of a crime. Counsel therefore should be familiar with situations in which HIPAA will apply, or no longer apply, because the safety of individuals may be compromised.

String D: Special Protections for Psychotherapy Notes

The final regulations define psychotherapy notes as notes recorded by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session. 45 C.F.R. § 164.501. Deemed to be of high sensitivity, psychotherapy notes may not ordinarily be disclosed for purposes otherwise permitted by a consent. For most purposes, psychotherapy notes may be released only pursuant to an authorization by an individual or his personal representative, even if such use is for treatment, payment or health care operations (ordinarily permitted with a consent).

Only a consent is required in the following circumstances, however: (i) for the person who created the psychotherapy notes to use them to carry out treatment; (ii) for the covered entity to use or disclose psychotherapy notes for conducting training programs; or (iii) for a covered entity to defend a legal action or other proceeding brought by the individual. Additionally, an authorization is not required for use or disclosure of psychotherapy notes when required for enforcement purposes, when mandated by law, when needed for oversight of the health care provider who created the psychotherapy notes, when needed by a coroner or medical examiner or when needed to avert a serious and imminent threat to health or safety.

String E: Research Concerns

Although the regulations, as discussed above, contain broad prohibitions, the regulations also include numerous refinements intended to make the prohibitions more palatable in a number of contexts. One such special context is research studies. Where a research study does not involve treatment of a patient, a separate authorization to use PHI likely will be required. It appears that a typical consent form used by institutional review boards (IRBs) and researchers will not be sufficient, and that a separate authorization will be required.

In the event that a covered entity alters an authorization form, however, the entity nonetheless may use or disclose PHI for research purposes if an IRB or privacy board approves either the alteration or a waiver of the authorization. 45 C.F.R. § 164.512. Where a research study also involves medical care of individuals, the covered entity still must obtain an authorization, but such authorization may be *combined* with a consent. For example, a single document: (i) may grant the entity the right to disclose PHI as required for the treatment of the patient, as would normally be stated in a consent; and (ii) also may contain an authorization for use of the same PHI for research purposes. 45 C.F.R. § 164.508.

String F: Interaction with State Laws

In most situations, HIPAA preempts state law unless the state law is "more stringent" than HIPAA. A few clear-cut examples exist where HIPAA allows state and local laws to continue without interference from the regulations, *e.g.*, worker's compensation. The number of laws implicated by HIPAA is enormous. The definition of "more stringent" is extremely vague. The time and effort that will be devoted to studying preemption by the regulations will be vast, but no more of either shall be exerted in this article.

Conclusion

HIPAA privacy regulations present a vast landscape to be explored. The present article has attempted merely to point toward the larger outcroppings of HIPAA's topography. Given the importance and intricacies of HIPAA, for most covered entities and business associates, now is the time to begin preparations lest one be caught in HIPAA's net.

[1] References to sections of the Code of Federal Regulations relate to sections as set forth in the regulations contained at 65 FR 82461 *et seq.* except as otherwise noted.

WYMAN IS A HEALTH CARE ATTORNEY IN THE RTP OFFICE OF MAUPIN TAYLOR & ELLIS, PA.

Rule

from page 1

nursing homes, medical equipment suppliers, dentists and health plans. The Privacy Rule also regulates covered entities' relationships with their "business associates" — including lawyers — involving the disclosure of individuals' health information.

The Privacy Rule comprehensively regulates uses and disclosures of "protected health information" by "covered entities." "Protected health information" (PHI) is health information that is identifiable to a specific individual. [5] There are three categories of "covered entities:" (1) health plans; (2) health care clearinghouses; and (3) health care providers.[6] A health plan is an individual or group plan that provides or pays the cost of medical care.

Health plans include employee welfare benefit plans as defined under the Employee Retirement Income Security Act of 1974 (ERISA), including insured and self-insured plans, to the extent the plan provides medical care directly or through insurance reimbursement or otherwise, unless it has fewer than 50 participants and is self-administered by the employer.[7]

Health care clearinghouses are companies that "translate" electronic transactions related to health insurance claims and health insurance coverage between "standard" formats and code sets required under HIPAA and non-standard formats and code sets. Health care providers are broadly defined to include any person or organization who furnishes, bills, or is paid for health care in the normal course of business.[8]

The Privacy Rule prohibits covered entities from using or disclosing PHI except as permitted or required under the Privacy Rule.[9] "Use" and "disclosure" are defined very broadly.[10] In over-simplified terms, a covered entity cannot look at or "touch" PHI within its own organization, or divulge or provide access to the information to any outsiders, except as the Privacy Rule permits or requires.

A covered entity's failure to comply with the Privacy Rule can result in severe civil and criminal penalties. A person who knowingly discloses PHI to another person in violation of the regulatory scheme is subject to potential criminal penalties of up to a $50,000 fine and imprisonment for up to one year. If the offense is committed with the intent to sell, transfer or use PHI for commercial advantage or personal gain, a person faces potential fines up to $250,000 and a sentence up to 10 years.[11] In the Jones hypothetical, the assistant United States attorney was exploring whether Jones' disclosing PHI to a lawyer in seeking collection of an account constituted acting with the intent to "transfer" PHI for "personal gain."

Lawyers as "Business Associates"

In the Jones hypothetical, Smith was a "business associate" of Jones in providing legal services to her. The Privacy Rule contains specific requirements for the disclosure of PHI to a covered entity's "business associate." A business associate is a person who performs a function or activity on behalf of a covered entity involving the use or disclosure of PHI. The Privacy Rule specifically states that a business associate includes a person who provides legal services to or for a covered entity involving the disclosure of PHI.[12] The covered entity's disclosure of PHI to a lawyer as a business associate may implicate, among other provisions, the Privacy Rule's provisions regarding patient consents, business associate agreements and "minimum necessary" uses and disclosures of PHI.

Patient Consent to Disclosure

In the hypothetical, the assistant United States attorney was considering prosecution of Jones for failure to obtain patient consents prior to the disclosures of PHI to Smith. The Privacy Rule requires a broad category of covered entities, "direct treatment" health care providers, to obtain an individual's written consent prior to the covered entity's use or disclosure of that individual's PHI for "treatment," "payment" or "health care operations."[13] "Health care operations" are defined to include arranging for legal services.[14]

Law Firm Business Associate Agreements

The Assistant United States Attorney also was considering prosecution of Jones for failure to have a written business associate agreement with Smith. The Privacy Rule permits a covered entity to disclose PHI to a business associate if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.[15] As a covered entity, a client must document the "satisfactory assurances" through a written agreement with the lawyer/business associate that meets very specific requirements.[16]

The business associate agreement between lawyer and client cannot authorize the lawyer to use or further disclose the PHI in a manner that would violate the Privacy Rule if done by the client.[17] The agreement must establish the permitted and required uses and disclosures of PHI by the lawyer. The agreement must specifically provide that the lawyer will:

> Not use or further disclose PHI other than as permitted or required by the agreement or as required by law.
>
> Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for by the agreement.
>
> Report to the client any use or disclosure of PHI not provided for by the agreement of which the lawyer becomes aware.
>
> Ensure that the lawyer's agents and subcontractors who receive PHI from the lawyer agree to the same restrictions that apply to the lawyer.
>
> Make available PHI in accordance with an individual's right of access to information and right to amend information under the Privacy Rule, and incorporate any such amendments in the PHI maintained by the lawyer in accordance with the Privacy Rule.
>
> Make available information required to provide an accounting to the patient of disclosures that were made of the PHI in accordance with the Privacy Rule.

Make available to the secretary of HHS the lawyer's internal practices, books and records relating to the use and disclosure of PHI received by the lawyer from the client or created on behalf of the client, for purposes of the secretary's determining the client's compliance with the Privacy Rule.[18]

If the client knows of a pattern of activity or practice of the lawyer that constitutes a material breach or violation of the lawyer's obligations under the business associate agreement, the client must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the client must terminate the agreement or, if termination is not feasible, report the problem to the secretary of HHS.[19]

Upon termination of the agreement, if feasible, the lawyer must return or destroy all PHI the lawyer received or created on behalf of the covered entity that the lawyer still maintains in any form, and the lawyer cannot retain any copies of such information. If such return or destruction is not feasible, the lawyer must extend the protections of the agreement to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.[20] If the client determines that the lawyer has violated a material term of the agreement, the agreement must authorize the client to terminate the agreement.[21]

"Minimum Necessary" Use and Disclosure

The "minimum necessary" provisions of the Privacy Rule present significant implementation challenges to covered entities. For any use or disclosure of PHI or request for PHI from another covered entity, a covered entity must limit the PHI to the "minimum necessary" for the particular purpose.[22] For example, a provider's own billing staff and a health plan may not need to see a patient's complete medical history to submit and process a claim. These provisions apply to a covered entity's disclosure of PHI to the covered entity's lawyer.

In the Jones hypothetical, Smith may not need to see a patient's entire medical history to collect an account for a single procedure. The "minimum necessary" provisions may also be asserted as applicable to the *lawyer's* further uses and disclosures of PHI. As discussed above, a business associate agreement between the lawyer and the covered entity / client cannot authorize the lawyer to use or further disclose the PHI in a manner that would violate the Privacy Rule if done by the client.[23]

Business Associates' Potential Liability

An analysis of whether a business associate can be held directly liable by the federal government for a violation of the Privacy Rule is beyond the scope of this article. The better argument would seem to be that a lawyer acting as a business associate cannot be held directly liable under the Privacy Rule because the HIPAA statute and the Privacy Rule expressly state that they apply to "covered entities," and a lawyer acting as a business associate in providing legal services to a client is not a covered entity.

The relative merits, if any, of various other theories of liability that potentially could be asserted against a business associate relating to uses and disclosures of PHI would have to be evaluated in the context of the specific facts. Depending on the facts, under federal law, liability theories that could potentially be asserted include, *inter alia*, theories of criminal conspiracy, aiding and abetting or misprision of felony relating to a covered entity's violation of the Privacy Rule.[24] Depending on the facts, under various states' laws, claims against lawyers / business associates potentially could include, *inter alia*, breach of a lawyer's alleged duty to counsel the client regarding the Privacy Rule's regulation of communications between the lawyer and client, breach of duty of care to protect confidential information, civil conspiracy, inducement of wrongful disclosure of nonpublic patient information, or invasion of privacy.

For an example of how common law developments can affect this analysis, *see* **Biddle v. Warren Gen. Hosp.**, 86 Ohio St.3d 395, 715 N.E.2d 518 (1999). In that case, the Ohio Supreme Court ruled that class action plaintiffs stated a cause of action against a law firm recipient of patient information. The Court recognized a new tort: "We hold that in Ohio, an independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship." The Court extended potential liability to third parties: "We hold that a third party can be held liable for inducing the unauthorized, unprivileged disclosure of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship."

State legislative developments should also be monitored. For example, on Jan. 11, a "mini-HIPAA" bill was introduced in the Texas Legislature that would make it a state law felony to "induce another to use or disclose . . . protected health information " for "commercial advantage" in violation of the proposed law.[25]

Security NPRM

HHS is also required to issue new federal standards for the security of PHI. HHS issued proposed security standards in a notice of proposed rule-making on Aug. 12, 1998 (Security NPRM).[26] A discussion of the Security NPRM is beyond the scope of this article. If the final security rule reflects the extensive degree of information security measures proposed under the Security NPRM, a law firm may want to ratchet up its own security measures. The "triggers" for enhancing law firm security could be based on requirements of the final security rule itself, client-imposed specific requirements, or a law firm's own risk management concerns.

Federally mandated information security measures for covered entities may be asserted (rightly or wrongly) as a point of reference for comparison purposes in asserting or determining the scope of a law firm's duty of care to covered entity clients with respect to information security and the scope of the contractual duty to use "appropriate safeguards " under the lawyer's business associate agreement.

Issues to Consider

The HIPAA Privacy Rule presents significant challenges to lawyers who will receive PHI as business associ-

See **Rule** *page 10*

Rule

from page 9

ates of covered entities. There are many issues to resolve. For example:

• What degree of "appropriate safeguards" are needed to satisfy the required business associate agreement provision regarding preventing the use or disclosure of PHI other than as provided for by the agreement?

• What systems or technologies will be necessary for lawyers to track all places where PHI appears in lawyers' records for purposes of making the PHI available for a patient's right of access to information and right to amend under the Privacy Rule? How do these business associate agreement requirements comport with the lawyer's interests under the work product doctrine?

• If a lawyer makes available PHI to an individual or the Secretary of HHS, does that have any effect on the attorney-client privilege?

• Would it be "feasible" for a lawyer to return or destroy all PHI received *or created* by the lawyer that the lawyer maintains in any form upon termination of the business associate agreement, and for the lawyer to retain no copies of such information?

• If the Privacy Rule's "minimum necessary" requirements apply to lawyers through the "bootstrap" of the business associate agreement, how will lawyers implement these requirements? Will this necessitate that law firms adopt formal written policies and procedures, including "role-based" access limitations in information technology systems?

• How will the lawyer respond to the client's questions and requests for legal advice as to the various required provisions in the business associate agreement with the lawyer?

Will lawyers, through business associate agreements or otherwise, be required to meet some of the information security standards that will be established in the final security rule, and even if not, will lawyers have to explain their own relative levels of information security against the "backdrop" of the Security Rule?

Things To Do

Where and when should a lawyer start to prepare for addressing the many impacts of the HIPAA Privacy Rule on the lawyer-client relationship? Some may wait to see if the Privacy Rule is relaxed or the compliance deadline is extended by Congress or President Bush. That approach has its risks if the Privacy Rule and the compliance deadline remain intact and precious time elapses. Lawyers may want to consider now the benefits of performing the following tasks:

• Become HIPAA-educated. Understand the Privacy Rule and how it affects your clients and your relationship with your clients.

• Do the same when the final HIPAA security rule is issued. Even before then, read the Security NPRM to grasp the magnitude and extent of what some have compared to military intelligence levels of security that HHS has proposed.

• Designate internal "point" responsibility within your firm for management of HIPAA privacy and security compliance.

• Perform a "gap" assessment of where your firm is now and what will need to be done to achieve information privacy and security compliance. Obtain outside assistance as needed. Be mindful of the substantial differences in potential consequences from a potentially unprivileged, "self-critical assessment" by your firm, and an assessment that is structured to maximize the protections of the attorney-client privilege.

• Assess what will need to be included in your firm's engagement letters and when your engagement letters should include the provisions required by the Privacy Rule, including engagements that begin prior to Feb. 26, 2003 but that are expected to extend beyond that date. The North Carolina Society of Health Care Attorneys is creating a task force to develop model forms for lawyer business associate agreements under the HIPAA Privacy Rule.

• Develop forms of agreements that your firm will use with its agents or contractors to whom your firm will disclose PHI, including expert witnesses, litigation support services, demonstrative evidence vendors and information technology companies who will have access to PHI on your IT system. Recall that under the business associate agreement, the client must require the lawyer to require its agents and subcontractors to abide by the same contractual restrictions and conditions that apply to the lawyer/business associate with respect to "downstream" uses and disclosures of PHI.

Address what risk management is warranted as to clients who may fail to obtain necessary consents for disclosure of PHI to your firm, including for disclosures of PHI that are made prior to the Privacy Rule's compliance date for engagements that will extend beyond the compliance date.[27]

Conclusion

Large segments of the health care industry face many implementation challenges for HIPAA privacy and security compliance. The legal profession has many points of contact with "protected health information," and law firms will need to manage their own responsibilities with respect to such information. □

HUBBARD IS A PARTNER WITH SMITH, ANDERSON, BLOUNT, DORSETT, MITCHELL & JERNIGAN, L.L.P.
MHUBBARD@SMITHLAW.COM

Endnotes

1 This article is intended to provide in a brief format a high-level, initial awareness of some of the HIPAA Privacy Rules' implications for the lawyer-client relationship. This article should not be construed as providing legal advice to any person. Counsel should resort to the Privacy Rule itself and other authority and seek interpretations as appropriate to assure compliance with the Privacy Rule. Exceptions, qualifications, and further clarifications to various statements in this article are not provided due to space constraints (*e.g.*, a six paragraph definition in the Rule may be condensed here to one sentence).

2 Title II, Subtitle F of the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

3 65 Fed. Reg. 82798 (Dec. 28, 2000) and 65 Fed. Reg. 82944 (Dec. 29, 2000); 45 C.F.R. Parts 160 and 164 (as of Dec. 2000).

4 The Privacy Rule's "effective date" is Feb. 26, 2001, unless Congress or President Bush acts otherwise, or unless questions concerning "delivery" of the Rule to Congress result in a delayed effective date of april 14, 2001. The compliances deadline is two years from the effective date. While two years may seem to be a comfortable period to prepare for compliance, a thorough understanding of the many HIPAA implementation challenges causes many observers to believe that two years is a tight schedule. Various health care industry stakeholders will lobby Congress and President Bush for an extension of the compliance deadline and a relaxation of the Privacy Rule's requirements.

A Note from the Editors of *Prognosis*

First, ***Prognosis*** extends a special thanks to contributors Greg Hassler, Mike Hubbard, Ed Meyer, and Roy Wyman, each of whom tackled the voluminous final HIPAA privacy regulations (or a significant portion thereof) in order to prepare the informative articles in this issue.

Additionally, it has been clarified that the final privacy regulations will become effective April 14, and that the new compliance deadline will be April 14, 2003 (or a year later for small health plans). The revised effective and compliance dates for the regulations, issued on Feb. 21, were necessitated by the fact that under the Congressional Review Act, the Department of Health and Human Services (HHS) was required to submit this regulation for consideration by Congress for a 60-day period. Due to an oversight at the end of the Clinton Administration, however, this requirement was not met, so the 60-day period began to run on Feb. 13. HHS Secretary Tommy Thompson announced on Feb. 23 that HHS will reopen the HIPAA privacy regulations for a new 30-day comment period, to end on March 30.

The final issue of *Prognosis* for the 2000-2001 year will be devoted to issues affecting rural health. Please contact the editors at *trish_markus@shmm.com* and *dmccord@wyrick.com* if you have ideas for articles in this area or know of a practitioner who might be willing to contribute. □

Endnotes, cont.

5 *See* 45 C.F.R. § 164.501 and 45 C.F.R. § 160.103 ("Protected health information" derives from the definitions of "individually identifiable health information" and "health information;" there are limited differences between protected health information and individually identifiable health information, but for simplicity of reference, protected health information is used in this article to refer to either term).

6 *See* 45 C.F.R. § 164.103 (health care providers are covered entities if they transmit health information in electronic form in connection with transactions related to health claims and health coverage that are regulated under HIPAA).

7 Note that many law firms sponsor "health plans" under this definition.

8 *See* 45 C.F.R. § 160.103.

9 *See* 45 C.F.R. § 164.502(a).

10 *See* 45 C.F.R. § 164.501. "Use" includes an "examination" of PHI; "disclosure" includes divulging or providing access to PHI.

11 *See* § 1177 of the Social Security Act. HHS is planning to issue an enforcement rule that will address violations of the Privacy Rule. The Dr. Jones hypothetical in this article is for illustrative purposes to provoke thought and discussion only, and is not a statement of whether this statute would be violated by the hypothetical facts presented.

12 *See* 45 C.F.R. § 160.103. "Business Associate" also includes a person who performs "any other function or activity regulated by this subchapter" with respect to a covered entity. The "business associate" definition excludes services performed as a member of the covered entity's "workforce" (*e.g.*, in-house counsel in most cases).

13 *See* 45 C.F.R. § 164.506. Provision of health care to an inmate is excepted.

14 *See* 45 C.F.R. § 164.501.

15 *See* 45 C.F.R. § 164.502(e)(1).

16 *See* 45 C.F.R. § 164.502(e)(2). In referencing the Privacy Rule's business associate requirements as applicable to lawyer-client relationships, this article occasionally substitutes "client" for "covered entity" and "lawyer" for "business associate" to simplify references to the Rule's provisions. Note also that there are special rules if the client/covered entity and lawyer/business associate are both governmental agencies.

17 *See* 45 C.F.R. § 164.504(e)(2)(i). There are two exceptions to this requirement that permit the business associate to use and disclose PHI for proper management and administration of the business associate and for data aggregation services relating to the health care operations of the covered entity.

18 *See* 45 C.F.R. § 164.504(e)(2)(ii).

19 *See* 45 C.F.R. § 164.504(e)(1)(ii). The statute also requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards "*to ensure*" the integrity and confidentiality of information needed to protect against "*any reasonably anticipated*" threats or hazards to the security and integrity of the information and unauthorized uses or disclosures of the information and otherwise to ensure compliance. *See* § 1173(d)(2) of the Social Security Act. The Privacy Rule also requires covered entities to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The covered entity "must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications, or other requirements" of the Privacy Rule. *Id.* (emphasis added). These provisions could also be asserted to have an impact on the client's duties with respect to the lawyer's handling of PHI.

20 *See* 45 C.F.R. § 164.504(e)(2)(ii)(I).

21 *See* 45 C.F.R. § 164.504(e)(2)(iii).

22 *See* 45 C.F.R. § 164.502(b); 45 C.F.R. § 164.514(d). There are certain exceptions to the "minimum necessary" provisions, including disclosures of PHI to a health care provider for treatment.

23 The minimum necessary disclosure provisions do provide that the covered entity may reasonably rely on a professional's requested disclosure as being the minimum necessary for the stated purpose when the professional represents that the information requested is the minimum necessary for the stated purpose. *See* 45 C.F.R. § 164.514(d)(3)(iii)(C). Note, however, that the minimum necessary provisions also state that a covered entity may not disclose an entire medical record except when the entire medical record is specifically justified as the amount that is reasonably necessary. *See* 45 C.F.R. § 164.514(d)(5).

24 *See generally*, Imperato, Gabriel L., "Criminal and Civil Liability for Health Care Consultants, 13 *The Health Lawyer*, No. 2, Page 1 (December 2000).

25 Texas Senate Bill No. 11 (Prefiled November 13, 2000; Introduced January 9, 2001).

26 *See* 63 Fed. Reg. 43263 (August 12, 1998).

27 The transition provisions of the Privacy Rule, 45 C.F.R. § 164.532, address permitted uses and disclosures of PHI occurring after the compliance date where the PHI was created or received by a covered entity prior to the compliance date.

Consents and Authorizations Under Final HIPAA Privacy Regulations

By Edward A. Meyer

General Rule

The final Health Insurance Portability and Accountability Act (HIPAA) privacy regulations generally prohibit "covered entities"[1] from either using or disclosing "protected health information"[2] (PHI), unless that use or disclosure falls within specified exceptions.[3] This article addresses the HIPAA exceptions which permit use and disclosure of PHI when a covered entity has obtained either a consent or an authorization in accordance with the regulations. This article does not, however, address those circumstances under HIPAA in which no consent or authorization is required. These latter exceptions, found generally at 45 C.F.R. 164.510[4] and 164.512,[5] should be reviewed by any practitioner advising clients on HIPAA obligations.

Given the complexity of the final regulations, covered entities such as health care providers, health plans and health care clearinghouses will need to implement strict policies and procedures to ensure that they obtain the necessary and valid consents, authorizations or notices to permit them to use or disclose PHI without violating the regulations.

Consent Requirement

Overview

The HIPAA privacy rules generally require that a covered health care provider,[6] prior to using or disclosing the PHI of an individual to carry out treatment, payment or health care operations, obtain the individual's valid consent.[7] The individual must not have revoked the consent in writing (although the consent will be valid for actions taken in reliance on the unrevoked consent).[8] Significantly, the regulations do permit a covered health care provider to condition treatment on the provision by the individual of a valid consent.[9] In addition, a health plan may condition enrollment in the health plan on the provision by the individual of a valid consent, provided that the consent is sought in conjunction with such enrollment.[10]

Exceptions

The regulations include some broad, and some limited, exceptions to the consent requirement. The broadest of the exceptions permits a covered health care provider who has only an indirect treatment relationship with the individual (such as a consulting physician or a pathologist or radiologist who does not directly treat the individual) to use or disclose the PHI to carry out treatment, payment or health care operations.[11] In addition, PHI may be used or disclosed in emergency treatment situations, provided that consent is attempted as soon as practicable after the delivery of such treatment.[12]

Limited exceptions to the consent requirement apply (i) if the health care provider is required by law to treat the individual;[13] (ii) where consent can not be obtained due to substantial barriers to communicating with the individual and the covered health care provider determines, in the exercise of professional judgment, that the individual's consent to receive treatment is "clearly inferred from the circumstances;"[14] or (iii) in limited cases involving inmates.[15] Under the first two limited exceptions, the covered health care provider must attempt to obtain the required consent but must be unable to obtain it.[16] The attempt to obtain consent, and the reason why the consent was not obtained, must be documented.[17] This latter documentation requirement also applies in the emergency treatment situation.[18]

Consent Content Requirements

The final regulations do not include a form consent. Instead, the regulations describe the required contents of a consent, each element of which must be included in the consent form in order for the consent to be valid under the regulations.[19] In order to be valid, the consent must be written in plain language, must be signed and dated by the individual, and must inform the individual that PHI may be used and disclosed to carry out treatment, payment or health care operations.[20] The consent also must refer the individual to the notice required by the regulations for a more complete description of such uses and disclosures.[21]

If the covered entity has reserved the right to change its privacy practices as described in the notice, the consent must state that the terms of the entity's notice may change, and it must describe how the individual may obtain a revised notice.[22] The consent also must state: (i) that the individual has the right to require the covered entity to restrict how PHI is used and disclosed to carry out treatment, payment or health care operations;[23] (ii) that the covered entity is not required to agree to the requested restrictions;[24] and (iii) that if the covered entity agrees to a requested restriction, the restriction is binding on the covered entity.[25] In addition, the consent must 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 the consent).[26]

The consent may be combined with an informed consent for treatment, a consent to assignment of benefits or other types of written legal permissions given by the individual. When so combined, the HIPAA consent must be visually and organizationally separate from the other written legal permission and must be separately signed by the individual and dated.[27] The consent also can be combined with a research authorization (described below). However,

when combined with a research authorization, the regulations do not require the consent to be visually or organizationally separate or separately signed and dated.[28]

Covered entities must document and retain any signed consent they receive, in accordance with the administrative requirements of the regulations.[29]

Authorization Requirement

Overview

The HIPAA requirements for obtaining an individual's prior authorization to use or disclose PHI are distinguishable from the consent requirements. The regulations require covered entities to obtain valid authorizations before they use or disclose PHI for any purpose, except as otherwise permitted or required in the regulations.[30] When an authorization is used to permit use and disclosure of PHI, the use and disclosure of the PHI must be consistent with the valid authorization. *Id.* The regulations also include special use and disclosure restrictions with regard to authorizations applicable to psychotherapy notes.[31]

Like the consent requirements, an individual may revoke an authorization at any time.[32] However, the revocation will not be valid for actions taken by the covered entity in reliance on the authorization and for certain contested insurance claims.[33]

Unlike the consent requirements, however, a covered entity generally 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.[34] A few limited exceptions apply. A covered entity *may* condition the provision of research related treatment on the provision of the special authorization applicable to research.[35] In addition, in certain instances health plans may condition enrollment in the health plan, eligibility for benefits, or payment on the provision of an authorization.[36]

Authorization Content Requirements

The final regulations do not include a form authorization. Instead, the regulations describe the required elements for a valid authorization. In order to be valid, an

See **Consents** *page 14*

Consents

from page 13

authorization document must use plain language and must include eight core elements.[37] These core elements include "a description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion," and "the name or other specific identification of the person(s), or class of persons" authorized to make the requested use or disclosure, as well as a listing / description of such persons / classes of persons to whom the covered entity may make the requested use or disclosure.[38]

An expiration date or event of expiration must be specified, and the authorization must include statements regarding the individual's right to revoke the authorization, and that the information may be subject to redisclosure by the recipient and no longer protected by the rule.[39] Specific requirements also are included for the signature and dating by the individual or his or her authorized representative of the authorization.[40]

Additional core elements are required for the following types of special authorizations: (i) authorizations requested by a covered entity for its own uses and disclosures;[41] (ii) authorizations requested by a covered entity for disclosures by others;[42] and (iii) authorizations for uses and disclosures of PHI created for research that includes treatment of individuals.[43]

If the authorization lacks any of the required core elements, or if the authorization has not been filled out completely with regard to any of the required elements, the authorization is not valid.[44] The authorization also is not valid if either: (i) the expiration date has passed;[45] (ii) the expiration event is known by the covered entity to have occurred;[46] or (iii) if the authorization is known by the covered entity to have been revoked.[47] An authorization is defective, and thus not valid, if any material information in the authorization is known by the covered entity to be false. The regulations do not, however, describe whether actual or constructive knowledge is required in determining the invalidity of the authorization.

While the consent requirements permit combined consents where the consent is physically separate and separately signed within the document, the authorization provisions generally prohibit an authorization for use or disclosure of PHI from being combined with any other document to create a compounded authorization.[48] Certain exceptions do apply, however.[49] Like the consent requirements, the regulations require covered entities to document and retain any signed authorizations they receive.[50]

Conclusion

As the legal advisors to the health care community, we need to raise the HIPAA awareness of our clients. We need to inform our clients that the HIPAA consent and authorization requirements are complex and include numerous required elements, the absence of any one of which will invalidate the consent or authorization under HIPAA. HIPAA applies broadly to protect the use or disclosure of individually identifiable health information and extends to the most common uses and disclosures by covered entities. These aspects of HIPAA emphasize the importance of HIPAA compliance as an institutional priority.

Our clients must begin now to review their policies and procedures and formulate their consent and authorization documents. The Feb. 26, 2003 (or Feb. 26, 2004, for certain small health plans) compliance dates should not cause our clients to place HIPAA preparation on the back burner. The required consents and authorizations must be in place or a suitable exception must be found by those dates in order for covered entities to lawfully use or disclosure PHI. Meeting this deadline will be a challenge, as it will take significant time and effort to create these documents and implement the policies and procedures governing consents and authorizations. □

MEYER IS A PARTNER IN THE GREENSBORO LAW FIRM OF MCDONALD & MEYER, PLLC.

Endnotes

1 The term "covered entities" is defined in the HIPAA regulations to mean "(1) a health plan [a defined term], (2) a health care clearinghouse [a defined term], and (3) a health care provider [a defined term] who transmits any health information [a defined term] in electronic form in connection with a transaction [a defined term] covered by this subchapter." 45 C.F.R. 160.103. It is beyond the scope of this article to describe in detail the definitions and subdefinitions of this term.

2 "Protected health information" includes individually identifiable health information which is transmitted or maintained in any form or medium, but excludes certain education records. *See* 45 C.F.R. 165.501.

3 45 C.F.R. 164.502.

4 Certain limited uses and disclosures of PHI by covered entities are permitted when the individual is informed in advance of the use and disclosure and has the opportunity to agree or prohibit or restrict the disclosure. *See* 45 C.F.R.164.510. These include certain use of basic identification information in a facility directory and disclosure of that information to clergy and persons asking for the individual by name and the disclosure to family / friends / caregivers who involved the individual's care or payment for the individual's health care. *Id.* Each has specific requirements to fit within the exception.

5 The HIPAA privacy regulations also permit and require a number of uses and disclosures of an individual's PHI without a prior consent, authorization, or a notice and opportunity to object. *See* 45 C.F.R. 164.512.

6 A "covered health care provider" means "a health care provider [a defined term] who transmits any health information [a defined term] in electronic form in connection with a transaction [a defined term] covered by this subchapter." 45 C.F.R. 160.103.

7 45 C.F.R. 164.506(a).

8 45 C.F.R. 164.506(c).

9 45 C.F.R. 164.506(b)(1).

10 45 C.F.R. 164.506(b)(2).

11 *See* 45 C.F.R. 164.506(a)(2)(i).

12 *See* 45 C.F.R. 164.506 (a)(3)(i).

13 45 C.F.R. 164.506(a)(3)(i) (B).

14 45 C.F.R.164.506(a)(3)(i) (C).

15 45 C.F.R. 164.506(a)(2)(iii).

16 45 C.F.R. 164.506(a)(3)(i)(B) and (C).

17 45 C.F.R. 164.506(a)(3)(ii).

18 *Id.*

19 *See* 45 C.F.R. 164.506(c) and 45 C.F.R. 164.506(d).

20 45 C.F.R. 164.506(c)(1) and (6).

21 45 C.F.R. 164.506(c)(2).

22 45 C.F.R. 164.506(c)(3).

23 45 C.F.R. 164.506(c)(4)(i).

24 45 C.F.R. 164.506(c)(4)(ii).

25 45 C.F.R. 164.506(c)(4)(iii).

26 45 C.F.R. 164.506(c)(5).

27 45 C.F.R. 165.506(b)(4)(i).

28 45 C.F.R. 164.506(b)(4)(ii).

29 45 C.F.R. 164.506(b)(6); *cf.* 45 C.F.R. 164.530(j).

30 45 C.F.R. 164.508(a)(1).

31 *See* 45 C.F.R. 164.508(a)(2).

32 45 C.F.R. 164.508(b)(5).

33 *Id.*

34 45 C.F.R. 164.508 (b)(4).

35 45 C.F.R. 164.508 (b)(4)(i); *see* 45 C.F.R. 164.508(f).

36 *See* 45 C.F.R. 164.508 (b)(4)(ii) and (iii).

37 *See* 45 C.F.R. 164.508(c).

38 45 C.F.R. 164.508(c)(ii) and (iii).

39 45 C.F.R. 164.508(c)(iv) – (vii).

40 45 C.F.R. 164.508(c)(viii).

41 *See* 45 C.F.R. 164.508(d).

42 *See* 45 C.F.R. 164.508(e).

43 *See* 45 C.F.R. 164.508(f).

44 45 C.F.R. 164.508(b)(2)(iv) and (ii).

45 45 C.F.R. 164.508(b)(2)(i).

46 45 C.F.R. 164.508(b)(2)(ii).

47 45 C.F.R. 164.508(b)(2)(iii).

48 45 C.F.R. 164.508(b)(3).

49 *See* 45 C.F.R. 164.508(b)(3) (i) – (iii).

50 45 C.F.R. 164.508(c); cf. 45 C.F.R. 164.530(j).

What's HOT in Health Law?

Health Law Section • 2001 Annual Meeting

April 27
Sheraton Imperial Hotel
Research Triangle Park

CLE Credit: 6.0 Hours Including 1.0 Ethics/Professionalism Hour

PROGRAM PLANNERS:

Carole E. Bowen, Moore & Van Allen PLLC, Charlotte
Cynthia L. Turco, Craven Regional Medical Center, New Bern

SPEAKERS:

Edward G. Connette, III, Lesesne & Connette, Charlotte
Trisha Crone, CIGNA Medicare, Nashville, Tenn.
Brett J. Denton, Charlotte-Mecklenburg Hospital Authority, Charlotte
Deborah L. Fletcher, Holcomb & Fletcher, PLLC, Charlotte
Susan McNear Fradenburg, Smith Helms Mulliss & Moore, L.L.P., Greensboro
Patricia T. Meador, Womble Carlyle Sandridge & Rice, PLLC, Research Triangle Park
Jon Neiditz, PricewaterhouseCoopers, Atlanta, Ga.
Lanek K. Stell, Davidson College, Davidson
Thomas W. Waldrep Jr., Bell Davis & Pitt, PA, Winston-Salem

PROGRAM TOPICS:

- **Federal Law Fraud and Abuse Update: A Review of These Last Twelve Months**
  Presented by Meador
- **Preparing to Comply with the Final HIPAA Regulations**
  Presented by Neiditz
- **Update on North Carolina CON Issues**
  Presented by Fradenburg
- **Bankruptcy Primer for Healthcare Providers**
  Presented by Fletcher and Waldrep
- **Ethics in Healthcare: Implications of The Cartrette Case**
  Presented by Connette, Denton and Stell
- **Medicare Part A and B Audits**
  Presented by Crone

HOTEL INFORMATION:

A block of sleeping rooms has been reserved for you at the **Sheraton Imperial Hotel and Convention Center in Research Triangle Park.** Take Exit 282 (Page Road) off of I-40. You must make your reservations directly with the hotel. Rates are $114 for single or double occupancy. Call (919) 941-5050 **by March 21,** to make your reservations.

TO REGISTER:

By Phone: Please call (919) 677-8745 or 1-800-228-3402 from 8:30 a.m. — 5:00 p.m. Visa, Mastercard and American Express.

Online: Visit our Web site at *www.ncbar.org/CLE* available 24 hours a day. Visa, Mastercard and American Express.

Society Plans Mini-Seminars to Address HIPAA

The President's Report ...

BY SANDRA D. VAN DER VAART

This year promises to be an interesting and busy one for health care attorneys. On Jan. 4, HCFA published the long-awaited final Stark II regulations. These regulations followed on the heels of the voluminous HIPAA privacy regulations, issued late last year by President Clinton. The privacy regulations, which are more than 1,500 pages long, were the second set of HIPAA regulations issued in the latter part of last year; the final regulations governing standards for electronic transactions had been issued on Aug. 17, 2000.

As health care attorneys were scrambling to evaluate and interpret these significant new regulations, President Bush, on his first day in office, issued a memorandum extending the effective date of pending published regulations and withdrawing all unpublished regulations. President Bush's memorandum directed the heads of executive departments and agencies to withdraw regulations that had been sent to the Federal Register but had not yet been published, and to extend the effective date of regulations that had been published but had not yet taken effect.

While the outcome of the Bush administration review of these regulations is uncertain, there is little doubt that health care attorneys will need to engage in significant compliance counseling with their clients on these issues. In order to assist our members in providing timely and practical advice, the North Carolina Society of Health Care Attorneys is planning two mini-seminars over the next several months. The first mini-seminar is targeted for this spring and will address HIPAA. This will be followed by a mini-seminar on the Stark II regulations toward the beginning of summer.

In addition to these upcoming educational opportunities, the society also has launched a project to develop a form Business Associate Agreement between an attorney and a HIPAA "covered entity" client which meets HIPAA's requirements. Mike Hubbard and Bill Shenton, society board members, are spearheading this project and are currently seeking interested (and enthusiastic) volunteers to work with them. Our goal is to present a form Agreement to the society's membership at the Annual Meeting this fall. If you would be interested in participating in this project, or in helping to organize a mini-seminar, please contact Elizabeth Stark, the society's executive director, at (919) 787-5181 or *estark@olsonmgmt.com*. □

SECTION/DIVISION PRO BONO PARTICIPATION

■ Create a Pro Bono Committee. The committee leads and coordinates the section's pro bono efforts. Consider appointing members active in pro bono as well as section leadership.

■ Build Discussion of Pro Bono Into Section Meetings. Include substantive law discussion where appropriate. The Public Service Advisory Committee will provide a member to make a presentation at section meetings throughout the year.

■ Publish Articles on Pro Bono in Section Newsletter. The chair of the section's Pro Bono Committee, or other members of the committee or section, may write articles on pro bono issues within the respective substantive area. Also, articles by members who have performed pro bono service can help demonstrate how pro bono service is possible within a given section.

■ Where Appropriate, Develop Special Projects. The particular substantive area of a section may lead it to develop a special program to recruit, train, or develop a panel of mentors, experts or willing volunteers.

■ Consider Legislative Action to Address Legal Needs of the Poor. The North Carolina Bar Association's efforts to address the legal needs of the state's poor go beyond promoting pro bono service and seeking adequate funding for legal services programs. Thus, sections and divisions are encouraged to consider legislation which will help to improve access to justice for the poor and seek funding for legal services programs.

Sections and divisions should be aware of both the potential consequence of their own proposed legislation on access to justice for the poor and consider what reforms within their substantive area may be possible. The Governmental Affairs Office would be happy to assist this effort.

For more information on how your section or division can become involved in pro bono activities, please contact the North Carolina Bar Association, Pro Bono Project, PO Box 3688, Cary, NC 27519-3688.

Document, Document, Document: HIPAA Standards Applicable to Institutional Review Boards and Researchers

By Gregory L. Hassler

The U.S. Department of Health and Human Services' final rule implementing the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA requires an Academic Medical Center (AMC)[1] to comply with certain documentation standards before it permits the use or disclosure of personal health information for research purposes. These standards aspire to strengthen and extend existing privacy safeguards for personal health information that is used or disclosed for research, while not creating unnecessary disincentives to an AMC that chooses to use or disclose personal health information for such purposes (65 Fed. Reg. 82694).

This article does not present an exhaustive analysis of ambiguities and implications inherent in the HIPAA regulations and instead attempts to provide an introductory orientation to pertinent regulatory standards and their applicability to the research context within an AMC, particularly to Institutional Review Boards (IRBs) and researchers.

The HIPAA privacy standards contain several critical words and definitions germane to an AMC's understanding of its responsibilities within the research enterprise. For purposes of t his article, there are four definitions that necessitate particular attention: "Protected health information" (PHI) means — with some exclusions — individually identifiable health information that is transmitted by electronic media; or maintained in any electronic media; or transmitted or maintained in any other forms or medium (45 C.F.R. 164.501 at Protected Health Information). The word "use" means the sharing, employment, application, utilization, examination or analysis of identifiable health information within an entity that maintains such information (45 C.F.R. 164.501 at Use).

"Disclosure" means the release, transfer, provision of access to or divulgence in any other manner of information outside the entity holding the information (45 C.F.R. 164.501 at Disclosure). Most importantly for IRB purposes, the word "research" means a systematic investigation, including research, development, testing and evaluation, designed to develop or contribute to generalizable knowledge (45 C.F.R. 164.501 at Research). A firm grasp of these and similar applicable definitions enable an AMC and its IRB to fulfill their regulatory responsibilities with respect to protecting human research subjects.

As a general rule, HIPAA requires an AMC to obtain a written authorization from a research subject before it uses or discloses PHI if such use or disclosure is not otherwise permitted without appropriate authorization (45 C.F.R. 164.508). HIPAA standards anticipate that most researchers will secure a research subject's written informed consent in the customary and traditional manner, and that an IRB will rigorously review the consent as required by applicable IRB regulations (see, e.g., 45 C.F.R. 46.108(b), which is also known as the "Common Rule"). In those situations in which a researcher wishes to have access to a subject's PHI for research purposes, and in which informed consent is not secured from the subject, the final rule allows for the AMC to disclose such PHI as long as the necessary waiver of authorization is obtained (45 C.F.R. 164.512(i)(1) and such waiver is properly documented (45 C.F.R. 164.512 (i)(2).

Meeting the waiver requirements is fairly straightforward: An AMC, prior to any disclosure or use of a research subject's PHI, must verify the identity and authority of persons requesting PHI, and obtain documentation from the researcher that is required as a condition of disclosure (45 C.F.R.64.514(d)(3)(iii)(D)). A researcher must provide the AMC, prior to its disclosure, with three written representations. The first representation entails an assurance from the researcher that the use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research (45 C.F.R. 164.512(i)(1)(ii)(A)).

The second representation provides assurances that no PHI is to be removed from the AMC by the researcher in the course of the review (45 C.F.R. 164.512(I)(1)(ii)(B)). Finally, the researcher must represent that the PHI is necessary for the research purposes for which use or access is sought (45 C.F.R. 164.512(i)(1)(ii)(C)). The standards suggest that a researcher may provide the foregoing representations to the IRB (see 65 Fed. Reg. 82697).

Once the IRB approves the waiver of authorization, it must also provide sufficient documentation that demonstrates it approved a research subject's waiver under 45 C.F.R. 164.512(i)(1)(i) before an AMC may permit the use or disclosure of PHI for research purposes. This documentation includes five elements, addressed below.

First, an IRB must provide a statement that identifies itself and the date upon which it approved the alteration or waiver of authorization (45 C.F.R. 164.512(i)(2)(i)). Second, an IRB must provide a statement that, in its determination, the alteration or waiver, in whole or in part, satisfies eight criteria (45 C.F.R. 164.512(i)(2). These criteria include determinations that:

> The use or disclosure of PHI involves no more than minimal risk to the subject;
>
> The alteration or waiver will not adversely affect the privacy rights and the welfare of the individuals;
>
> The research could not practicably be conducted without access to and use of the PHI;
>
> The privacy risks to individuals whose PHI is to be used or disclosed are reasonable in relation to the anticipated benefits if any to the individuals, and to the impor-

See **Document** *page 18*

Document

from page 17

> tance of the knowledge that may reasonably be expected to result from the research;
>
> There is an adequate plan to protect the identifiers from improper use and disclosure;
>
> There is an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
>
> There are adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for some other research for which the use or disclosure of PHI would be permitted by the rule.
>
> — (45 C.F.R. 164.512(i)(2)(ii)(A) through (H)).

"In addressing these criteria, an AMC may expect its IRB to consider the immediate privacy interests of the individual that would arise from the proposed research study and the possible implications from a loss of privacy" (65 Fed. Reg. 82696). Moreover, the standard requires the IRB to comply with applicable IRB regulations and final HIPAA rules in this context (65 Fed. Reg. 82697). One foresees that an IRB will likely require a researcher to provide assurances in the internal processing form that the researcher meets the foregoing criteria.

The third documentation element that the IRB must provide to its AMC entails describing the PHI for which use or access has been determined to be necessary by the IRB (45 C.F.R. 164.512(i)(2)(iii)). The IRB satisfies the fourth element of documentation by providing a statement that the subject's alteration or waiver of authorization has undergone either IRB normal review under 45 C.F.R. 46.108(b) or expedited review under 45 C.F.R. 46.110. The final required element of documentation is the IRB chair's — or its designee's — signature upon the documentation of the alteration or waiver of authorization.

Subsequent to the use or disclosure, an AMC has additional regulatory responsibilities towards the subjects. The standards require an AMC to include research disclosures in their notice of information practices to subjects enrolled in research protocols (45 C.F.R. 164.520). Moreover, where individual subjects enrolled in a research protocol request, an AMC must provide them with an accounting of disclosures made about their individual PHI (45 C.F.R. 164.528).

This article intends to provide an introductory orientation to those regulatory standards contained in HIPAA's final rule applicable to the research context within an AMC. Readers may want to consult additional resources for a more in-depth examination of the standards.

For example, the U.S. Department of Health and Human Services' Office for Human Research Protection maintains a Web site, *http://ohrp.osophs.dhhs.gov*, that may ultimately provide guidance regarding the implementation of the standards relevant to researchers and IRB. The IRB Discussion Forum, *www.mcwirb.org*, furthermore, is an excellent resource for further information. The Forum includes 2,100 members who promote the discussion (via a listserv) of regulatory and policy concerns surrounding human subjects research. □

HASSLER SERVES AS THE CHIEF LEGAL COUNSEL OF EAST CAROLINA UNIVERSITY'S BRODY SCHOOL OF MEDICINE AND AS THE ASSOCIATE UNIVERSITY ATTORNEY FOR THE DIVISION OF ALLIED HEALTH SCIENCES.

Endnote

[1] This article uses the term "Academic Medical Center" to mean a "covered entity" under the HIPAA regulations, as an AMC constitutes a health care provider that transmits any health information in electronic form in connection with the use and disclosure of such information for research purposes. 45 C.F.R. 160.103 under "Covered Entity."

26 Good Reasons

to join the North Carolina Bar Association

- **Annual Meeting**

Join us in June for section programs, informative speakers, athletic and family events and much more.

- **Association Group Insurance**

Health, Life and Disability Programs at group rates. Contact Lawyers Insurance Agency at (919)677-8900 or 1-800-662-8843.

- **Bank Card**

Platinum Plus Credit Card offered by MBNA with expanded benefits, lower interest rates and the NCBA logo.

- **Committees**

More than 40 standing committees examine issues affecting the practice of law.

- **Computer Training Center**

With high-tech workshops for members and their staff.

- **Continuing Legal Education**

Live and video programs statewide to keep your practice current. Video, book sales, newsletters.

- **CLE Passport Program**

One year of unlimited Continuing Legal Education at an incredible low price. Contact the CLE Department at 1-800-228-3402.

- **Endowment**

Offers the opportunity to support service projects of the N.C. Bar Association and Foundation and to honor and memorialize family members and friends.

- **Lawyer Referral Service**

Refers more than 50,000 clients annually. An excellent way to serve the public and develop your practice.

- **Legal Information Pamphlets**

Pamphlets on common legal problems are distributed free to the public. Available for display in your office.

- **Legislative Program**

Up-to-date information on any legislative matter. Copies of pending legislation and ratified bills. Lobbying to promote legislation affecting lawyers and the administration of justice.

- **Local Bar Services**

Provide active support to local bars with assistance for local projects and programs.

- **Long Distance Discount with BTI**

Get substantial savings on long distance telephone and internet service through BTI.

- **NC Casemaker©**

Members can search NC statutes, opinions, codes and much more. Starting June 1, 2001 you can go to *www.ncbar.org* for your research needs.

- **Overnight Delivery Service**

Discounts on overnight shipping in the U.S. and world-wide through Airborne Express.

- **Practical Skills Course**

Held annually to help new attorneys grasp the nuts and bolts of practice and to provide a review for practicing lawyers.

- **Pro Bono Office**

Activates and supports Pro Bono programs throughout the state.

- **Professional Liability Insurance**

Contact Lawyers Mutual Liability Insurance Company at 1-800-662-8843.

- **Publications**

North Carolina Lawyer, sent bimonthly to all members; Section, Legislative, SLD and YLD newsletters; CLE publications and more.

- **Relocation Service**

Confidential relocation assistance for attorneys, legal administrators and paralegals.

- **Section Activities**

26 specialized sections offer informative programs, committee activities and regular newsletters.

- **Senior Lawyers Division**

Any member 55 or older can belong to the SLD which provides seminars, committees and programs directed to the needs of senior lawyers.

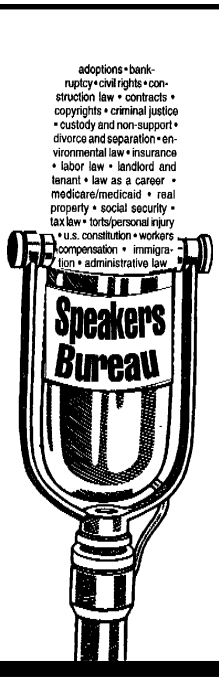
- **Technology Assistance**

Discounts on law office technology consulting services. Call Bob Stearn, ELM Consulting, 1-800-508-8989.

- **Young Lawyers Division**

Includes all members under age 36 or within three years of licensing. Committee activities, public service programs, regular newsletter.

For more information on any of these programs, call 1-800-662-7407.



NCBA Seeking Speakers

The Communications Committee of the N.C. Bar Association maintains a Speakers Bureau with more than 800 lawyers who have agreed to make themselves available to community and business groups who want to learn more about various aspects of North Carolina law.

The majority of the NCBA's speakers live and work in the state's more densely populated regions. The Communications Committee applauds their efforts and welcomes additional speakers from those areas. At the same time, much of the remainder of the state is underserved.

If you live or work in any of these areas, such as **Camden, Cherokee, Clay, Dare, Hyde, Madison** and **Tyrrell** counties, please contact the NCBA at 1-800-662-7407 (677-0561 within Wake County) and say you want to join the NCBA Speakers Bureau. The names of those attorneys volunteering to serve as panel members will be added to a list at the Bar Center which rotates members' names as they agree to speaking engagements.

NORTH CAROLINA BAR ASSOCIATION
North Carolina Bar Center
PO Box 3688
Cary, NC 27519-3688

Nonprofit Organization
U.S. POSTAGE
PAID
Raleigh, NC
Permit Number 297

Rural Health Symposium

THE CRITICAL ISSUES CANNOT BE IGNORED

The Health Law Section of the North Carolina Bar Association is pleased to present to the members of the North Carolina Bar Association a Rural Health Symposium. The Symposium will allow key panelists the opportunity to explore the difficulties faced by practitioners in the delivery of health care to rural areas, to identify challenges that have been overcome and to explore remaining hurdles.

- **Date:** Wednesday, May 16, 2001
- **Time:** 10:00 am to 3:00 pm
- **Location:** Monroe Auditorium at FirstHealth Moore Regional Hospital

Please mark your calendars now to attend this important and informative seminar. Registration information will be provided at a later date.

Topic and Speakers: Speakers involved with many areas of rural health delivery including representatives of government, community care, hospitals and mental health will share their thoughts and experiences. The goal of this symposium is to encourage a free exchange of concerns in an effort to promote thought, support and change.