Health Privacy: The New Federal Framework

Aimee N. Wall

Patients usually expect that health information shared and generated when they are receiving medical care will be kept confidential by their health care provider and, if they have insurance, by their health insurance plan. A recent Gallup survey found that almost 78 percent of adults believe it is "very important" that their health information be kept confidential.[1] Most providers and insurers strive to meet these expectations. However, other people and organizations often need access to health information to carry out their responsibilities. For example, public health officials want health care providers to report communicable diseases, law enforcement officials expect emergency care providers to report gunshot wounds, and social services agencies rely on health care providers to report evidence of abuse or neglect.

For many years, federal, state, and local lawmakers have struggled to find the appropriate balance between protecting the privacy of health information and ensuring that health information is available when necessary for other important purposes. A patchwork of federal and state laws, rules, common law, and professional ethical obligations and guidelines has resulted, providing a hazy outline at best for when providers and insurers may share health information with other entities. This past year, however, the first and only *comprehensive* federal rule on health privacy went into effect.[2] This article provides a brief history of the new rule, summarizes many of the rule's complex requirements, and offers a few suggestions for entities and local governments, particularly counties, to consider as they begin to comply.

Why Is the New Rule Necessary?

Until recently the federal government approached the issue of privacy in a piecemeal fashion. Several laws dealt with health information privacy but did not regulate it comprehensively. For example, most information held by the federal government that identifies individuals is subject to the Privacy Act of 1974;[3] health information held by substance abuse programs receiving federal assistance is subject to a substance abuse confidentiality rule;[4] and information held by providers treating Medicare and Medicaid patients is subject to an array of confidentiality statutes and rules.[5]

Similarly every state has health privacy laws, but only a handful are comprehensive.[6] The vast majority of states, including North Carolina, have limited laws governing only particular types of entities, such as HMOs,[7] or specific conditions, such as communicable diseases.[8]

The result of this piecemeal approach has been that under most circumstances, people could not be assured that health care providers, insurers, or others were legally required to keep health information confidential.[9] Many argued that the legal framework was fractured and wholly inadequate to protect information.[10]

As health care delivery entered the electronic age, concerns about privacy increased. The health care industry began to integrate technological tools into the practice of medicine—for example, electronic medical records,

The author, an Institute of Government faculty member who specializes in public health law, frequently advises local health departments about health information privacy. Contact her at wall@iogmail.iog.unc.edu.

"telemedicine" (the use of telecommunications to support long-distance clinical care), and electronically filed insurance claims. The industry appealed to Congress for legislation to facilitate electronic sharing of information between providers and insurers. Congress passed such legislation as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). One part of this legislation, entitled Administrative Simplification, directed the U.S. Department of Health and Human Services (DHHS) to develop a series of rules that would standardize the electronic sharing of health information and dramatically reduce administrative expenses.

Congress recognized, however, that because Administrative Simplification would encourage health information to flow more freely, preserving the confidentiality of that information had to become a high priority at the federal level. Therefore, as part of Administrative Simplification, Congress also directed DHHS to develop rules governing both the privacy and the security of health information. Privacy and security are closely connected but distinct concepts. Privacy is "the patient's right over the use and disclosure of his or her own personal health information," whereas security is the "specific measures a health care entity must take to *protect* personal health information from unauthorized breaches of privacy."[11]

In recognition of this difference, DHHS is developing separate rules for privacy and security. The security rule was proposed in 1998 but has not yet been finalized. The privacy rule, which is the focus of this article, was finalized during the Clinton Administration, and the compliance date is currently April 14, 2003, for most health care providers and insurers.[12] In March 2002 the Bush Administration proposed several significant revisions to the privacy rule.[13] After the public has had an opportunity to comment on the proposed revisions, DHHS will consider whether to adopt any changes recommended by the public, and then it will publish another final privacy rule. DHHS has indicated that compliance with the rule is still expected by April 2003, although Congress could delay the compliance date.

A doctor's laptop was stolen at a medical conference. The computer contained the names and medical histories of his patients in North Carolina.

From A. Santana, *Thieves Take More than Laptops*, WASHINGTON POST, Nov. 5, 2000, at A1

What Do Local Governments Need to Do?

The privacy rule requires "covered entities"—public and private health plans, health care clearinghouses, and most health care providers (those that transmit health information electronically)—to make significant administrative and organizational changes in the way that they handle health information. Many different components of local government will be affected by this new rule either directly or indirectly. For example, local health departments, area mental health authorities, and emergency medical service agencies are directly regulated because they are health care providers. Jail health programs and social services agencies also may be regulated entities. Law enforcement officials, courts, and medical examiners may not be covered entities, but because they often need health information from covered entities, such as health departments, social services agencies, and private health care providers, the new restrictions on disclosure will affect their ability to carry out their duties.

Given that the compliance date is fast approaching, state and local governments must immediately begin making some changes. In North Carolina, efforts are well under way at the state level to bring state agencies into compliance with the privacy rule. Last October, the General Assembly directed the Office of State Budget and Management to develop a strategic plan for implementing HIPAA.[14]

By contrast, local governments are in many different stages of readiness to comply. Some counties have only a basic awareness of the new law, whereas others have developed a strategic plan, hired a privacy officer, and are working toward compliance. Local governments should be taking a careful look at their operations and developing a compliance plan.

If it has not already done so, a county should immediately appoint a compliance officer, preferably an attorney, to become familiar with the privacy rule and oversee its implementation throughout the county. Once the officer understands the rule, he or she should determine which components of local government are covered entities, such as local health departments and jail health programs (see the later

HELPFUL HIPAA WEB SITES

U.S. Department of Health and Human Services, Office of Civil Rights
www.hhs.gov/ocr/hipaa/

North Carolina HIPAA Program Management Office
dirm.state.nc.us/hipaa/

UNC–Chapel Hill, Institute of Government and School of Public Health Medical Privacy Training
www.medicalprivacy.unc.edu

North Carolina Healthcare Information and Communications Alliance, Inc.
www.nchica.org

New Individual Rights

Arguably the most revolutionary aspect of the HIPAA privacy regulations is the establishment of several new individual rights. The basic principle underlying these new rights is that people should be able to understand how their health information is used and disclosed and have some opportunity to control it. The privacy rule establishes several rights intended to ensure that individuals are able to control their health information, including the right to a notice of privacy practices, the right to inspect and amend health information, the right to receive a disclosure history, and the right to request certain restrictions on disclosure. Covered entities, including all local health departments and area mental health authorities, will need to develop and implement policies and procedures to accommodate these new rights.

Right to Notice

The key to gaining control over one's health information is having a clear and accurate understanding of how that information is used and shared with others. As DHHS explained, "One of the goals of this rule is to create an environment of open communication and transparency with respect to the use and disclosure of . . . health information."[1] Therefore the privacy rule creates an individual right to a notice of privacy practices that covered entities must develop and disseminate to patients and enrollees.[2]

This notice is not a simple statement saying, "We will keep your personal health information confidential." Rather, the notice is intended to be a fairly comprehensive inventory of how the entity may use and disclose health information and an explanation of the individual's rights and the entity's legal duties with respect to that information. The rule outlines the types of information that must be included in the notice and requires that it be drafted in "plain language." It is extremely important that these notices be drafted carefully and updated regularly because covered entities are bound by their notices. In other words, if they use or disclose health information in a way that is not specified in their notice, they could be subject to civil or criminal penalties.

Right of Access and Amendment

In addition to understanding how health information is used and shared, a patient must have access to that information in order to know exactly what information is being used and shared. The privacy rule therefore establishes a right to inspect and obtain a copy of most health information held by covered entities. The rule sets out several circumstances in which a patient's request for access may be denied, such as when the information requested is psychotherapy notes or has been compiled for legal or administrative proceedings. A request for access also may be denied if a health care professional determines that access is "reasonably likely to endanger the life or physical safety of the individual or another person."[3] If a covered entity denies a request, in some situations an individual may request that the decision be reviewed. The entity must act on such a request within sixty days, and it may charge a reasonable, cost-based fee for a copy of the information.

Now that patients have the right of access, it is only logical that they also be provided with the right to have the covered entity amend information that patients find to be inaccurate or incomplete.[4] The entity may deny an amendment request for a variety of reasons. Most important, it may deny a request if it determines that the information is in fact accurate or complete. If the entity does deny a request, the patient has the right to submit a "statement of disagreement," which must be kept with the record and

Continued on page 47

section headed "Who Is Regulated?"). It is possible that the entire county will be considered a covered entity. In such a case, the county's compliance officer still will need to identify the components of the county that must comply with the rule.

In addition to identifying covered entities, the county should identify other components of local government that use and share health information, and evaluate whether and how those components can continue obtaining health information from covered entities after the compliance date. For example, the privacy rule places new restrictions on when law enforcement officials may obtain health information without a court order. The compliance officer must evaluate the current practices of law enforcement officials and determine if any changes need to be made in order to ensure that the officials can obtain health information when necessary.

Once a county has identified all the local entities that will be directly and indirectly affected by the rule, it should develop a countywide compliance plan. Just as the state has designated a HIPAA Program Management Office to oversee the state's implementation, counties would be prudent to consider centralizing compliance activities at the county level. In addition, a regional approach may be appropriate in the case of area mental health authorities or public health districts. Although each county component will encounter unique challenges to implementation, having a coordinated and comprehensive countywide plan for ensuring that the April 2003 deadline is met will be worthwhile. (For a list of steps that an entity should take to move toward compliance within the necessary timeframe, see the sidebar on page 48. For Web resources, see the sidebar on page 45.)

Who Is Regulated?

When Congress passed HIPAA, it specifically limited the scope of the law to three types of entities: health care providers, health plans, and health care clearinghouses (defined later).[15] Many other groups—for example, employers, courts, researchers, and marketers—regularly handle personal health

Continued from page 46

disclosed with the record any time that the entity shares the disputed information with another entity.

If the entity accepts a request for an amendment, it need not alter the actual record but must identify the affected information and either append the amendment or provide a link in some way to the amendment. After accepting the amendment, the entity is required to make reasonable efforts to notify certain other entities that received the inaccurate or incomplete information. The entity must act on an individual's request for amendment within ninety days.

Right to an Accounting of Disclosures

To keep track of where his or her health information is going, a patient now is able to request a disclosure history from a covered entity—basically an accounting of each time that the entity has disclosed identifiable health information to other entities in the previous six years.[5] The history will provide the patient with important information about disclosures made without his or her permission, such as certain disclosures to researchers or government officials.

The history does not have to include any of the standard disclosures that an entity makes for purposes of treatment, payment, or health care operations (business practices like quality assurance that require the use of health information)—most likely the vast majority of disclosures. The history also may exclude certain other types of disclosures, such as those from a hospital's patient-information line.

Right to Request Additional Protections

The privacy rule also provides individuals with two new tools to help them gain control over how their information is disclosed.[6] First, they have the right to request that health care providers and health plans make special arrangements for communicating directly with them. For example, a patient may request that her provider or health plan send all communications (bills, test results, and so forth) to a work address rather than a home address. The provider must accommodate such a request. The health plan, meanwhile, must accommodate such a request only if the patient "clearly states that the disclosure of all or part of [the] information could endanger the individual."

Second, patients have the right to request certain restrictions on the use or the disclosure of their health information. For example, a patient may request that a provider not disclose his information for research purposes. This second right is not particularly strong because it is only the right to *request*—the entity is not required to accept the request. However, if the entity does accept the request, it is bound by the request (except in emergency circumstances), so a disclosure in violation of the request would be considered a violation of the privacy rule.

Notes

1. Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,549, 82,820 (Dec. 28, 2000).
2. 45 C.F.R. § 164.520.
3. 45 C.F.R. § 164.524. Before the privacy rule, about half of the states, including North Carolina, provided some statutory rights of access. *See, e.g.*, N.C. GEN. STAT. § 58-39-45 (hereinafter G.S.) (requiring certain insurance institutions to provide individuals with access to certain information); G.S. 122C-53(c) (requiring facilities providing treatment to people who are mentally ill, developmentally disabled, or substance abusers to provide access under certain circumstances).
4. 45 C.F.R. § 164.526.
5. 45 C.F.R. § 164.528.
6. 45 C.F.R. § 164.522.

information, but they are not covered by the privacy rule because DHHS does not have the legal authority to include them. If an entity is covered, it must comply with the privacy rule and will be subject to significant criminal and civil monetary penalties for violations.[16]

The privacy rule broadly defines "health care provider" to include any "person or organization who furnishes, bills, or is paid for health care in the normal course of business."[17] The rule applies only to providers that transmit health information electronically in connection with one of several types of health care transactions (for example, health insurance claims). Once a provider conducts such a transaction, all the individually identifiable health information held by that provider is covered by the rule. Almost all providers, including *all* local health departments and area mental health authorities, conduct some form of electronic transaction, either through their own business office or through a contract with a third-party billing company. As a result, only a handful of providers are likely to be exempt from the privacy rule. For example, a small jail health program or private free clinic might not submit any insurance claims electronically and therefore would not be covered.

By contrast, all health plans and health care clearinghouses are required to comply. "Health plan" is defined to include not only traditional private health insurance plans like Aetna and Blue Cross/Blue Shield but also public insurance programs, including Medicare, Medicaid, and the State Children's Health Insurance Program (known as Health Choice in North Carolina).[18] If a county self-insures to provide employee health insurance, it will most likely be covered by the privacy rule as a health plan. A "health care clearinghouse" is, in general, an entity (public or private) that translates health information from one data format to another.[19] It is unlikely that a county operates a health care clearinghouse, although it may contract with one.

Even though the privacy rule technically covers only these three types of entities, DHHS indirectly extended the reach of the rule to some noncovered

entities by requiring covered entities to have contracts with their business associates. A "business associate" is a third party that uses identifiable health information to provide services to or for the covered entity or otherwise assist the entity with its activities—for example, a billing company, an accountant, an attorney, or a consultant.[20] The rationale for expanding the scope of the rule is that if it were restricted to the three types of entities, individuals could not be assured that their health information would be protected. In other words, once the information traveled from a covered entity to a noncovered one, the privacy rule would become meaningless because it could no longer protect the information, and in many instances, no other law would be available to protect the information.[21] For example, if a health department contracted with a vendor to file insurance claims and bill individuals for health services, the vendor would most likely not be a covered entity, and theoretically it could choose to use, disclose, or even sell a list of patients treated by the health department.[22] Under the privacy rule, the health department must enter into a contract with the vendor that requires protection of the information.

The biggest problem with this contractual requirement is that only the covered entity, not the business associate, is subject to DHHS enforcement. Therefore, DHHS can hold only the covered entity responsible if the business associate breaches the contract and discloses health information inappropriately.[23] In response to public comments, DHHS stated that the regulatory authority provided by the underlying statute, HIPAA, was too limited and admitted that such indirect regulation of business associates was not the ideal approach but was necessary to ensure that the information was protected. DHHS has therefore encouraged Congress to pass new legislation that would allow these entities to be regulated directly.[24]

What Information Is Regulated?

The rule applies to health information that identifies individuals, in any form or medium, including electronic, paper,

What Should a Covered Entity Do Now?

To comply with the new privacy rule by April 2003, covered entities should be taking action now. Suggested steps follow.

Designate a privacy officer. He or she should understand all the requirements of the privacy rule, as well as any other applicable federal and state privacy laws. The officer should be responsible for overseeing implementation of the privacy rule within the entity, providing training or organizing training for other members of the entity's workforce, and monitoring compliance.

Conduct a "gap analysis." Review current information-sharing practices in order to compile a comprehensive inventory of how health information is used within the entity and disclosed to outside people or entities. Identify business associates—that is, third parties that use identifiable health information in providing services to a covered entity. Focus on situations or relationships in which information is currently used or disclosed in a way that violates the privacy rule.

Develop a compliance plan. This plan should begin with the gap analysis, include all the steps necessary to come into compliance, and end with an ongoing plan for monitoring compliance. Entities should work with experienced attorneys or compliance officers in developing and implementing the plan.

Develop and maintain privacy policies and procedures. Each entity's policies and procedures must be comprehensive, and they must be reviewed regularly to ensure that they reflect the entity's current practices as well as changes in state or federal law. Entities must maintain a written or electronic copy of their policies and procedures.

Review current forms and notices. Review current consent and authorization forms (for example, release of information, or ROI, forms) and any notices that are provided to patients. Consult with an attorney to prepare new forms and a notice of privacy practices that are consistent with the privacy rule. As with the entity's policies and procedures, these forms and notices must be kept up-to-date and accurate.

Develop training. The rule requires each entity to train its workforce on its policies and procedures before the compliance date (April 2003); to train new employees within a reasonable period after they join the workforce; and periodically to retrain any employee affected by a material change in law, policy, or procedure. The training should not only outline the requirements of the rule but also reflect all applicable federal and state laws and the agency's *own* policies and procedures.

Consider developing a coalition. Hundreds of entities throughout the state will be working at the same time on compliance. Although each entity will have to address particular needs and practices, creating a coalition of similar entities (such as local health departments in a region) that can work together toward compliance may be worthwhile. For example, the coalition might serve as an advisory group, develop a core set of policies and procedures, prepare draft forms and notices, and offer common training to the workforces of coalition members.

and even oral information. Critics of the rule argued that it is far too expansive and that Congress intended DHHS to regulate only electronically transmitted information. In reponse, DHHS asserted that Congress authorized the regulation of all health information and that this approach was the most reasonable and practical means available. Specifically, DHHS explained that limiting the application of the rule to electronically transmitted information would have created an "artificial boundary" because information is constantly moving from one format to another.[25] For example, a health care provider may submit a claim to Medicaid electronically, print out a copy of the claim, and discuss it with a co-worker. In this example, only the format of the information, not the content, has changed. The privacy rule would not adequately protect the *content* of the information if the rule was limited to electronically transmitted information.[26]

A banker who also served on his county's health board cross-referenced customer accounts with patient information. He called due the mortgages of anyone suffering from cancer.

From M. Lavelle, *Health Plan Debate Turning to Privacy: Some Call for Safeguards on Medical Disclosure. Is a Federal Law Necessary?* NATIONAL LAW JOURNAL, May 30, 1994, at A1

What Does the Rule Require?

The requirements outlined in the privacy rule are based on many of the practices that already are employed by health care providers and insurers across the country. The rule compiles many of these practices into a single, comprehensive law. Although numerous terms and concepts, such as "patient consent" and "patient authorization," will be familiar throughout the health care industry, the privacy rule redefines many terms and concepts and inserts them into a new framework.

The privacy rule has four basic parts:

1. *Use and disclosure:* An entity may use or disclose identifiable health information only when the rule either requires or allows the use or the disclosure.

2. *Minimum necessary:* When an entity uses or discloses health information (as required or allowed by the rule), it must "make reasonable efforts to limit the . . . information to the minimum necessary to accomplish the intended purpose of the use or disclosure. . . ."[27]

3. *Individual rights:* An entity must respond to and accommodate some new individual rights (see the sidebar on page 46).

4. *Administrative requirements:* An entity must institute certain business practices, such as documenting privacy policies and procedures, designating a privacy officer, providing training for employees, and establishing a system of sanctions for employees who violate privacy policies and procedures.[28]

The first part of the framework, which outlines the required and allowed uses and disclosures, is perhaps the most complicated part of the rule, so it is discussed here in detail. The rule *requires* disclosure in only two instances: first, when DHHS needs information to evaluate an entity's compliance with the rule, and second, when a patient requests a copy of his or her own information (for a discussion of the patient's right to request access to his or her health information, see the sidebar on page 46). The rule *allows* use and disclosure in several instances, which fall into three general categories: (1) use or disclosure for purposes of treatment, payment, and health care operations, (2) use or disclosure with the patient's permission, and (3) use or disclosure without the patient's permission.

Use or Disclosure for Treatment, Payment, and Health Care Operations

The original version of the privacy rule published by the Clinton Administration requires most health care providers to obtain the patient's express permission to use health information for treatment, payment, and health care operations.[29] This type of patient permission is termed "consent" under the rule.[30] For example, a local health department's prenatal clinic would be required to seek a woman's consent before providing her with prenatal care or billing her insurer for that care. The consent also would allow the health department to use the woman's health information for its "health care operations"—a term that is defined broadly to include many of the business practices that require the use of health information, such as quality assurance, credentialing of providers, and other management activities.

This consent requirement may ultimately be eliminated from the final privacy rule. In the suggested revisions published this March, the Bush Administration proposed changes that would allow all covered entities, including health care providers, to use and disclose health information for treatment, payment, and health care operations without obtaining the patient's consent. In proposing the change, DHHS explained that the consent process in the current version of the privacy rule could "potentially interfere with the efficient delivery of health care."[31] In lieu of the consent requirement, DHHS proposes to require covered entities to attempt to obtain a patient's written acknowledgment that he or she received a copy of the entity's notice of privacy practices (for a description of the requirement for a notice of privacy practices, see the sidebar on page 46). For example, under the Bush Administration's proposal, the health department's prenatal clinic would not be required to obtain the woman's consent to use her information for treatment or billing purposes, but it would need to give her a copy of the department's notice of privacy practices and attempt to have her acknowledge receiving the notice by signing a form or a log.

Therefore, regardless of whether the final rule requires a consent or simply an acknowledgment of the notice, covered entities will need to have systems in place for obtaining signatures whenever necessary and maintaining appropriate documentation.

Use or Disclosure with the Patient's Permission

In addition to consent, the privacy rule recognizes three other types of patient permission: authorization, opportunity to opt out, and opportunity to agree or object. Each type applies in different circumstances and comes with its own set of requirements.

Patient *authorization* is required when an entity wants to use or disclose health information in a way that is not otherwise permitted by the privacy rule. A patient may authorize any type of use or disclosure as long as the authorization form is consistent with the detailed format and content requirements contained in the rule. For example, if a school requires students to have physical examinations before participating in school sports, a provider (such as a local health department) would have to obtain an authorization (most likely from the parent or guardian) before sending a copy of the physical examination results to the school.

The last two types of individual permission apply in narrow circumstances and are more informal than authorization. First, a person must be given an *opportunity to opt out* of certain uses or disclosures, such as the entity's use of health information for fund-raising purposes. For example, if a hospital wants to use a list of all its cardiology patients in a mailing to raise money for an expansion of the cardiac care unit, it must include a statement in its materials explaining how a patient may opt out of receiving such fund-raising communications.[32] Second, a person must have an *opportunity to agree or object* when an entity is going to use health information in a facility directory (for example, if a hospital discloses information about a patient's condition to the general public through a patient-information line), disclose information to someone involved in the person's care (for example, a friend or a family member), or disclose information to people or organizations involved in certain disaster relief efforts.[33] The entity may orally inform the person that he or she has the right to object, and the person may orally agree or object to the use or the disclosure.

Use or Disclosure without the Patient's Permission

One aspect of the privacy rule that surprises many members of the public is that it allows entities to disclose health information in a wide variety of circumstances without the patient's permission. In drafting the rule, DHHS recognized that "health information is needed to support certain national priority activities" and that "[i]n many cases, the need to obtain authorization for use of health information would create significant obstacles in efforts to fight crime, understand disease, and protect public health."[34] These national priority activities relate to the following:

- Public health
- Victims of abuse, neglect, or domestic violence
- Law enforcement
- Judicial and administrative proceedings
- Health oversight (for example, fraud and abuse investigations, civil rights investigations, and licensure or disciplinary activities)
- Correctional institutions
- Workers' compensation
- Duties of a coroner or a medical examiner
- Organ, eye, or tissue donation
- Research

Many of these activities are the responsibility, in whole or in part, of state and local governments. Although the privacy rule allows entities to share health information with state or local officials for many of these activities, each type of disclosure may have new strings attached.[35] For example, if a health care provider has reasonable cause to believe that an adult with disabilities needs protective services, the provider is currently required by state law to report this information to the county director of social services.[36] The privacy rule allows this reporting but also requires the provider to notify the adult that the report has been or will be made (subject to limited exceptions).[37]

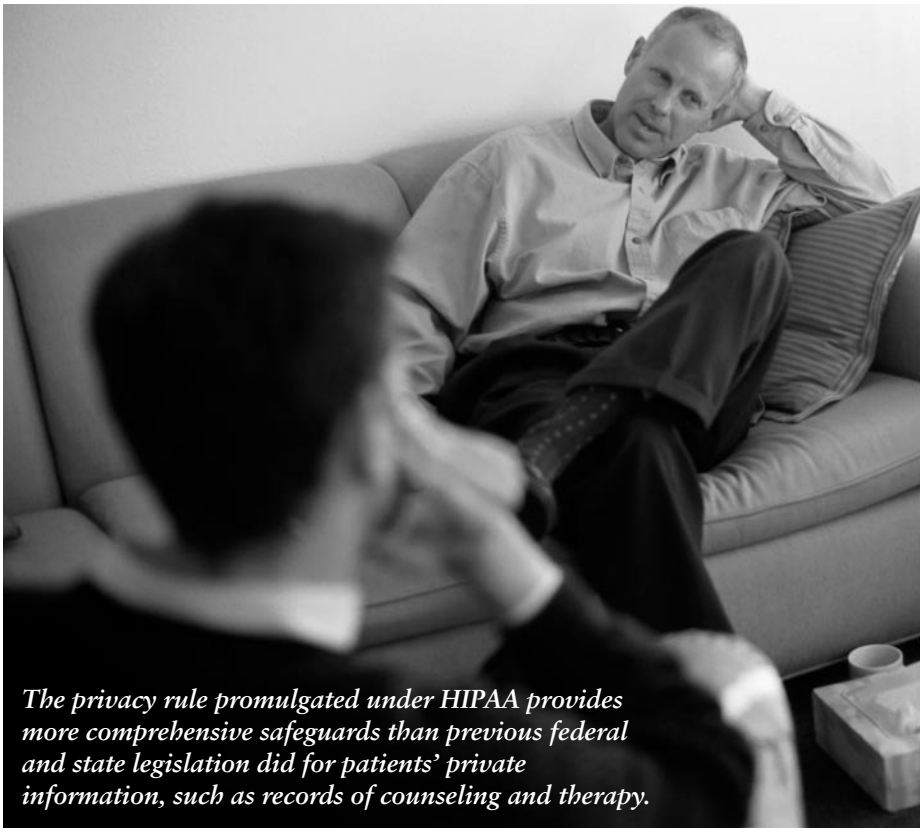
In addition to these listed categories of permissible disclosures, the rule provides broad authority for disclosures that are "necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public."[38] These disclosures must be consistent with applicable law and ethical standards, be made in good faith, and be made to a person reasonably able to prevent or lessen the threat. A mental health provider, for example, might rely on this authority to disclose health information about a dangerous patient to law enforcement authorities or a potential victim.

In Tampa, a public health worker walked away with a computer disk containing the names of 4,000 people who tested positive for HIV. The disks were sent to two newspapers.

From J. Bacon, *AIDS Confidentiality,* USA Today, Oct. 10, 1996, at A1

How Does the Rule Affect Current Laws?

North Carolina has more than one hundred state statutory provisions, plus many more rules, court decisions, and policies, that intersect with the privacy rule in some way. Many covered entities argued that expecting them to comply with a comprehensive federal law *in addition to* all the state laws was unreasonable; therefore the federal privacy rule should preempt (or override) all other privacy laws. Despite this argument, Congress did not provide DHHS with the authority to preempt all other privacy laws.[39] Rather, it established an extraordinarily complicated relationship between the privacy rule and other laws.



The privacy rule promulgated under HIPAA provides more comprehensive safeguards than previous federal and state legislation did for patients' private information, such as records of counseling and therapy.

People often say as a rule of thumb that HIPAA establishes a "federal floor" of privacy protections. In other words, all federal, state, and local privacy laws that are "more stringent" (more protective) than the privacy rule will remain in place.[40] This rule of thumb is accurate to some extent, but many state laws will remain in place whether or not they are more stringent than the privacy rule.

First, the privacy rule "carves out" several categories of laws from preemption—for example, laws that provide for the reporting of disease or injury, child abuse, birth, or death. North Carolina has many laws that fall into one or more of these carve-outs. For example, one statute directs hospitals to keep birth and death records and to make those records available to the state registrar.[41] This statutory provision falls within the carve-out and therefore is not affected by the privacy rule.

Second, the secretary of DHHS may make individualized determinations that a particular law is not preempted because it is necessary for certain stated purposes, such as preventing fraud and abuse.[42]

Third, the most confusing exception to the federal-floor rule of thumb is that the privacy rule specifically leaves in place any law that "requires" a disclosure. A disclosure is "required by law" if it is mandated by a statute, regulation, court-ordered warrant, grand jury subpoena, civil investigative demand, or similar authority.[43] For example, a North Carolina statute requires substance abuse facilities to furnish health information to the commissioner of motor vehicles regarding people who are involuntarily committed for the treatment of alcoholism or drug addiction.[44] This law will likely stay in effect because the disclosure is required by law, even though the general philosophy underlying the privacy rule would require the patient's authorization for such a disclosure.

Given this complex relationship between state and federal law, it is crucial that covered entities and others who need health information to do their work (such as law enforcement officials and health oversight agencies) seek sound legal advice as they work toward an understanding of their rights and obligations.

Conclusion

The requirements of the privacy rule add a new layer to the already complex landscape of health privacy law. The process of understanding the new law and coming into compliance with it will most certainly be resource-intensive and time-consuming. Therefore, if they have not already done so, local governments and covered entities should begin this process as soon as possible. Once the necessary changes have been implemented and staff have been appropriately trained, all the new requirements that are perhaps intimidating at first glance will become second nature.

Notes

The three highlighted quotations in this article are taken from *Medical Privacy Stories*, Health Privacy Project, Inst. for Health Care Research and Policy, Georgetown Univ. (last updated July 12, 2001), available at www.healthprivacy.org/usr_doc/privacystories%2Epdf.

1. *See* Gallup Organization, Public Attitudes Towards Medical Privacy (Sept. 2000) (submitted to the Inst. for Health Freedom), available at www.forhealthfreedom.org/Gallupsurvey/IHF-Gallup.html.

2. 42 U.S.C. §§ 1320d–1320d(8) (Administrative Simplification); 45 C.F.R. pts. 160, 164 (2001).

3. 5 U.S.C. § 552a.

4. *See* 42 U.S.C. § 290dd-2; 42 C.F.R. pt. 2 (implementing regulations).

5. *See, e.g.*, 42 U.S.C. § 1396a(a)(7) (requiring each state's medical assistance plan to provide for safeguarding of information of Medicaid applicants and recipients); 42 C.F.R. pt. 431 [implementing 42 U.S.C. § 1396a(a)(7)]; 42 C.F.R. § 422.118 (requiring managed care organizations participating in Medicare to ensure the confidentiality and the accuracy of enrollee records); 42 C.F.R. § 484.10 (establishing as a condition of participation in Medicare a patient's right to confidentiality with respect to medical records maintained by a home health agency).

6. Joy Pritts et al., The State of Health Privacy: An Uneven Terrain: A Comprehensive Survey of State Health Privacy Statutes, Health Privacy Project, Inst. for Health Care Research and Policy, Georgetown Univ. (Aug. 8, 1999), available at www.healthprivacy.org/resources.

7. *See* N.C. Gen. Stat. § 58-67-180 (hereinafter G.S.).

8. *See* G.S. 130A-143.

9. *See*, *e.g.*, American Medical Association, *Fundamental Elements of the Patient-Physician Relationship*, Ethical Opinion E-10.01, Report

of the Council on Ethical and Judicial Affairs of the American Medical Ass'n (Aug. 2001) ("The patient has the right to confidentiality. The physician should not reveal confidential communications or information without the consent of the patient, unless provided for by law or by the need to protect the welfare of the individual or the public interest"), available at www.ama-assn.org/ama/pub/category/2510.html.

10. *See, e.g.*, *Medical Records Confidentiality Act of 1995: Hearing on S. 1360 before the Senate Comm. on Labor and Human Resources*, 104th Cong. (Nov. 14, 1995) (testimony of Janlori Goldman, Deputy Director of the Center for Democracy and Technology), available at www.cdt.org/ testimony/951114 goldman.shtml; Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL LAW REVIEW 451, 516 (1995) (explaining why a uniform federal law is necessary to develop a coherent and viable health information infrastructure).

11. David C. Kibbe, *A Problem-Oriented Approach to the HIPAA Security Standards*, FAMILY PRACTICE MANAGEMENT, July–Aug. 2001, at 37, 38, available at www.aafp.org/fpm.

12. Small health plans have until April 2004 to comply. 45 C.F.R. § 164.534.

13. Modifications to the Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 67 Fed. Reg. 14,776 (Mar. 27, 2002) (hereinafter Modifications); *see also* A. Goldstein, *Medical Privacy Changes Proposed*, WASHINGTON POST, Mar. 22, 2002, at A1.

14. SL 2001-424 (signed Sept. 26, 2001).

15. The privacy rule subdivides covered entities into a few additional categories, including hybrid entities, affiliated covered entities, covered entities with multiple covered functions, and organized health care arrangements. *See* 45 C.F.R. §§ 164.504(b) (discussion of "health care component of a hybrid entity"), 164.504(d) (discussion of "affiliated covered entities"), 164.504(g) (discussion of "covered entities with multiple covered functions"), 164.501 (definition of "organized health care arrangement"); Standards for Privacy of Individually Identifiable Health Information; Final Rule, 65 Fed. Reg. 82,462, 82,502–09 (Dec. 28, 2000) (hereinafter Privacy Rule Preamble) (preamble discussion and regulation text relating to organizational requirements for different types of covered entities). There are benefits and drawbacks to each category. Compliance officers should review the rule carefully to determine if an entity falls within a special category.

16. HIPAA provides for civil monetary penalties of $100 for each violation (up to $25,000 per year). 42 U.S.C. § 1320d-5(a)(1). Criminal penalties range from a fine of $50,000 and/or up to one year in prison, to a fine of $250,000 and/or up to ten years in prison. 42 U.S.C. § 1320d-6.

17. 45 C.F.R. § 160.203.

18. A social services agency's determining eligibility for Medicaid or Health Choice does not automatically mean that it is a covered entity (i.e., a health plan) or a business associate. The agency also would have to perform other functions that would qualify it, such as providing home health services. Privacy Rule Preamble, 65 Fed. Reg. at 82,479.

19. *Id.* (definition of "health plan," "health care clearinghouse").

20. *Id.* (definition of "business associate").

21. "If covered entities were able to circumvent the requirements of these rules by the simple expedient of contracting out the performance of various functions, these rules would afford no protection to individually identifiable health information and be rendered meaningless." Privacy Rule Preamble, 65 Fed. Reg. at 82,640.

22. This would be true only if no other privacy laws applied to the third party.

23. A covered entity will be held responsible under HIPAA for the misdeeds of a business associate only "if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the [contract] unless the covered entity took reasonable steps to cure the breach or end the violation" and, if such steps were unsuccessful, the entity either terminated the contract or reported the problem to DHHS. 45 C.F.R. § 164.504 (e)(1)(ii).

24. *See* Privacy Rule Preamble, 65 Fed. Reg. at 82,567 ("We agree . . . that comprehensive legislation is necessary to provide full privacy protection and have called for members of Congress to pass such legislation. . . ."); *id.* at 82,641 ("[W]e agree that there are advantages to legislation that directly regulates most entities that use or disclose protected health information. However, we reiterate that our jurisdiction under the statute limits us to regulate only those covered entities listed in § 160.102").

25. *See* Privacy Rule Preamble, 65 Fed. Reg. at 82,618–19.

26. Recognizing that tight restrictions on oral communications could present some implementation challenges, the Bush Administration's proposed revisions include several changes that, if adopted, would provide more flexibility with respect to oral disclosures occurring "incidentally" while the entity is making a disclosure that is otherwise permitted by the privacy rule. *See* Modifications, 67 Fed. Reg. at 14,785–86.

27. 45 C.F.R. § 164.502(b). There are several exceptions to the "minimum necessary" requirement. For example, an entity does not need to limit the information disclosed to health care providers for treatment purposes. *Id.*

28. *Id.* § 164.530.

29. *See* 45 C.F.R. § 164.501 (definitions of "treatment," "payment," and "health care operations").

30. Consent as required by the privacy rule is not the same as the commonly used informed consent. "Informed consent," as it has been interpreted and applied in most instances, refers to a patient agreeing to certain treatment (after adequate discussion and/or disclosure), whereas "consent" required by the privacy rule refers to a patient providing permission to use and disclose information. *See* G.S. 90-21.13 (informed consent to a health care treatment or procedure); *see generally* FAY A. ROZOVSKY, CONSENT TO TREATMENT: A PRACTICAL GUIDE § 1.0 (2d ed., Boston: Little, Brown, 1990, and 2d ed. Supp., Gaithersburg, Md.: Aspen Publishers, 1999). The consent required by the privacy rule is not intended to be uninformed, however. The rule requires that the patient be provided with a "notice of privacy practices," which will provide detailed information on how information will be used and disclosed by the covered entity (see the sidebar on page 46).

31. *Fact Sheet: Standards for Privacy of Individually Identifiable Health Information —Proposed Rule Modification,* DHHS (Mar. 21, 2002), available at www.hhs.gov/news/press/2002pres/20020321.html.

32. 45 C.F.R. § 164.514(e)–(f).

33. 45 C.F.R. § 164.510. Each category of disclosure is subject to certain limited exceptions.

34. Standards for Privacy of Individually Identifiable Health Information; Proposed Rule, 64 Fed. Reg. 59,918, 59,925 (proposed Nov. 3, 1999) (to be codified at 42 C.F.R. pts. 160, 164) (preamble to the proposed privacy rule).

35. *See* 45 C.F.R. § 164.512 (specifying the rules that apply to disclosures for each type of "national priority activity").

36. G.S. 108A-102 (requiring "any person having reasonable cause to believe that a disabled adult is in need of protective services" to report such information to the director of social services).

37. 45 C.F.R. § 164.512(c).

38. *Id.* § 164.512(k).

39. 42 U.S.C. § 1320d-7.

40. 45 C.F.R. §§ 160.202 (definition of "more stringent"), 160.203 (outlining the general rule of preemption and the exceptions, including the "more stringent" exception).

41. G.S. 130A-117.

42. 45 C.F.R. § 160.203(a). If an exception is granted under this section, it stays in effect until either the secretary revokes it or the state law or the privacy rule changes such that the ground for the exception no longer exists.
45 C.F.R. § 160.205.

43. 45 C.F.R. §§ 164.501 (definition of "required by law"), 164.512(a) (required-by-law exception).

44. G.S. 20-17.1(e).