CE Home Study Course

HIPAA—The Health Insurance Portability and Accountability Act
What RNs Need to Know About Privacy Rules and Protected Electronic Health Information

This home study CE is part one of a two-part series. Look for the second installment and the CE quiz to appear in the next issue of National Nurse.

Description

This home study course provides a review of pertinent HIPAA definitions, and the legislative history and intent of relevant privacy rules and regulations as they relate to the collection, use, and disclosure of protected, individually identifiable electronic health information. It describes the appropriate safeguards that RNs must follow to protect the privacy of patients’ health information and discusses the rationale and strategies for protecting RN professional practice and credibility with the public. In addition, a selected review of publicly reported HIPAA violations and penalties are included to increase awareness and help RNs avoid the risk of discipline by the employer, their professional licensing board, or the imposition of penalties and fines imposed by civil or criminal courts.

Objectives: Upon completion of this home study course RNs will be able to:

Describe the intent of HIPAA regulation
List identifying information that is protected under HIPAA
Describe how HIPAA affects provider communications and electronic medical records
Describe how HIPAA impacts patients’ right to privacy and confidentiality
Identify strategies to prevent privacy and data breaches from occurring and reduce risk of personal, professional, and organizational liability

Introduction

Protecting patient confidentiality has always been an important responsibility of the nursing profession, and few government regulations have generated as much anxiety among healthcare providers as the federal medical privacy rules. Nurses are in a unique position; they are often the first contact patients have within healthcare systems. Patients share personal and intimate details and may have to reveal embarrassing information about their lifestyle, living conditions, past medical history, and personal habits during the assessment process so an accurate diagnosis and care plan can be formulated. The assumption is that nurses won’t disclose the information in a less-than-professional and respectful manner to anyone who isn’t involved in their care.

The HIPAA regulations were instituted to protect the privacy of individuals by safeguarding individually identifiable healthcare records, including those housed in electronic media. Protection of individual medical records extends not only to clinical healthcare sites but also to all ancillary healthcare providers, such as pharmacies, laboratories, and third-party payers. Each healthcare provider dealing with client healthcare data must provide for secure and limited access to the information. The intent of HIPAA regulation includes four main components: 1) Establishes limits for appropriate use and release of healthcare information; 2) Provides individuals with more control over their health information; 3) Requires the majority of healthcare providers and their agents to comply with safeguards to protect individual privacy related to healthcare information; 4) Delineates a set of civil and criminal penalties holding HIPAA regulation violators accountable if the patient’s confidential healthcare privacy is compromised.

Getting HIPAA with IT (Information Technology). When physicians profess the Hippocratic Oath, they make a solemn pledge: “What I may see or hear in the course of the treatment..., which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.” Lo, Dornbrand, and Dubler (2005) asserted that Hippocrates could never have envisioned the world today, with telephones, faxes, and e-mail communications, or the number of other healthcare providers and administrators involved in the care of a patient.

Historically speaking, confidentiality isn’t just a legal issue; it’s also a matter of ethics. Ethically, overriding confidentiality to prevent harms to third parties is warranted when several criteria are met: the potential harm to identifiable third parties is serious and likely (necessity); the breach of confidentiality allows effective steps to prevent harm (effectiveness); there is no less restrictive alternative for protecting those at risk; disclosure is limited to what is essential to avert harm and harms to the patient are minimal and acceptable (proportionality), and policies are justified publicly (transparency).

Submitted by the Joint Nursing Practice Commission, DeAnn McEwen, RN, and Hedy Dumpel, RN, JD
Provider Approved by the California Board of Registered Nursing, Provider #00754 for 4.0 contact hours (cehs).
Recognized by all states with the exception of Arkansas, Delaware, Massachusetts, Minnesota, Montana, North Carolina, and South Carolina.

20 NATIONAL NURSE WWW.NATIONALNURSESUNITED.ORG JULY / AUGUST 2011
patients also have other rights to privacy which predated HIPAA that cover a broader area than just their medical information. In general, a patient's right to privacy falls within one of four domains:

(1) Use of the patient’s likeness or name without his or her consent for the commercial benefit of the defendant. This refers to use of photographs or names that may be included in advertising for the healthcare agency or provider without the patient’s permission;

(2) Unreasonable intrusion into the patient’s private affairs and seclusions. This involves observation of patient care (such as by medical device vendors, nursing, medical, and technical students) or taking of photographs for any purpose without the patient’s consent.

(3) Public disclosure of private facts about the patient. Private information provided to others who have no legitimate need or right to know that information.

(4) Placing the patient in a false light in the public eye. This type of invasion involves publishing information that is normally considered offensive and is untrue.

HIPAA standards for the privacy and confidentiality of individually identifiable protected health information is congruent with our ethical obligations as professionals; the regulations reinforce behaviors that should already be second nature for most RNs. Nurses are legally and ethically obligated to keep information about their patients confidential. Confidentiality is crucial to the provision of nursing care and is an important part of the basis for a trusting patient/family and professional nurse relationship. If confidentiality is broken, patients may experience great harm and may not seek needed medical care. They may not provide a truthful medical history if they believe that others will know about their medical condition. Patient confidentiality is an important value to the nursing profession.

Nurses should not discuss a patient’s examination, observation, conversation, or treatment with other clients or staff not assisting in a specific patient’s care. Only the staff directly involved in a specific patient’s care has legitimate access to the patient’s records. Patients and/or their designated representatives frequently request copies of their medical records and they have the right to read those records. Each institution has policies for controlling the manner in which records are shared. In most situations, patients are required to give written permission for release of medical information.

Nurses are responsible for protecting records from all unauthorized readers. When nurses and other healthcare professionals have a legitimate reason to use records for data gathering, research or continuing education, appropriate authorization must be obtained according to agency policy. Student nurses and faculty may be required to present identification indicating access to the record is authorized. The nurse assigned to the patient should know the location of the record at all times. The healthcare facility or agency has the responsibility for securely storing the patient’s record after treatment ends.

HIPAA: History and Legislative Overview. HIPAA’s roots began in the United States Senate in 1995 as an insurance reform bill introduced by Sen. Edward Kennedy (D-Massachusetts) and Sen. Nancy Kassebaum (R-Kansas). The bill became known as the Kennedy-Kassebaum bill, and it was remarkable for garnering unique bipartisan support, considering the fact that its main goal was to curb market indiscretions and abuses in the health insurance industry. Cosponsors included liberals such as Paul Wellstone (D-Minnesota) and conservatives such as Richard Lugar (R-Indiana). The final version passed the Senate by unanimous consent. The Senate bill was an extension of the insurance reforms passed in the Consolidated Omnibus Budget Reconciliation Act (COBRA) a decade earlier. COBRA enabled workers to continue to purchase the same health insurance coverage they had under their employer-based plan upon leaving their job. The Kennedy-Kassebaum bill constrained payers from limiting or excluding employees from coverage for preexisting medical conditions.

The House bill, introduced in 1996, contained what would become the “administrative simplification” provisions of HIPAA. The House version reflected recommendations made by a special committee assembled by the first Bush administration, known as the Work Group for Electronic Data Interchange. Their charge was to find ways to reduce healthcare administrative costs. HIPAA passed the House of Representatives by a vote of 421 to 2 and President Clinton signed HIPAA into law on Aug. 21, 1996.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) limited the extent to which health plans may impose preexisting condition limitations and prohibits discrimination of health plans against individual participants and beneficiaries based on health status. One of the ways that insurance companies protect their profits is by not insuring certain preexisting conditions that patients have when they obtain group health insurance coverage. For example, if a patient has heart disease, an insurer may agree to provide health insurance for the client for all medical problems except heart disease. HIPAA requires insurers to only limit coverage for a preexisting condition for 12 months in most cases. This means that if an employee has group health insurance coverage with his job for at least 12 months and then changes jobs, the second employer cannot impose preexisting condition exclusion on the individual. The advantages of HIPAA are that employees can change jobs without losing coverage as a result of preexisting coverage exclusion as long as they have had 12 months of continuous group health insurance coverage.

HIPAA (Public Law 104-191) provided the first comprehensive federal protection for the privacy of individually identifiable health information (IIIH). Until Congress passed HIPAA, personal health information (PHI) was protected by a patchwork of state and federal laws. In many circumstances, patients’ health information could be distributed without their consent for reasons having nothing to do with their medical treatment or healthcare reimbursement. Sections 261 through 264 of HIPAA required the Secretary of Health and Human Services (HHS) to publicize standards for the electronic exchange, privacy, and security of health information. Collectively these are known as the “Administrative Simplification” provisions.

HIPAA required the secretary to issue privacy regulations governing individually identifiable health information. HHS developed a proposed rule and released it for public comment on Nov. 3, 1999. The department received more than 52,000 public comments, and on Dec. 28, 2000, the Privacy Rule was published. Legislation to protect patient privacy for health information (HIPAA) became a final rule in April 2001 and took effect in April 2003. This legislation governs all areas of information management, including reimbursement, coding, security, and client records. Healthcare providers (e.g. hospitals, clinics, physicians’ offices, clinical laboratories, and pharmacies) are required to provide their clients with greater control over personal healthcare information. Under newer regulations, in order to eliminate barriers that could delay access to care, providers are required only to notify clients of their privacy policy and make a reasonable effort to get written acknowledgment of this notification.
**HIPAA Violations: Consequences, Terms, Conditions, and Enforcement.** Failure to comply with HIPAA can result in civil and criminal penalties (42 USC § 1320d-5).

**Civil Penalties.** The “American Recovery and Reinvestment Act of 2009” (ARRA) that was signed into law on Feb. 17, 2009, established a tiered civil penalty structure for HIPAA violations (see sidebar). The Secretary of the Department of Health and Human Services (HHS) still has discretion in determining the amount of the penalty based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation. The Secretary is still prohibited from imposing civil penalties (except in cases of willful neglect) if the violation is corrected within 30 days (this time period may be extended).

**Criminal Penalties.** In June 2005, the U.S. Department of Justice (DOJ) clarified who can be held criminally liable under HIPAA. Covered entities and specified individuals, as explained below, who “knowingly” obtain or disclose individually identifiable health information in violation of the Administrative Simplification regulations face a fine of up to $50,000, as well as imprisonment up to one year. Offenses committed under false pretenses allow penalties to be increased to a $100,000 fine, with up to five years in prison. Finally, offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm permit fines of $250,000, and imprisonment for up to 10 years.

**Covered Entity and Specified Individuals.** The DOJ concluded that the criminal penalties for a violation of HIPAA are directly applicable to covered entities—including health plans, healthcare clearinghouses, healthcare providers who transmit claims in electronic form, and Medicare prescription drug card sponsors. Individuals such as directors, employees, or officers of the covered entity, where the covered entity is not an individual, may also be directly criminally liable under HIPAA in accordance with principles of “corporate criminal liability.” Where an individual of a covered entity is not directly liable under HIPAA, they can still be charged with conspiracy or aiding and abetting.

**Knowingly.** The DOJ interpreted the “knowingly” element of the HIPAA statute for criminal liability as requiring only knowledge of the actions that constitute an offense. Specific knowledge of an action being in violation of the HIPAA statute is not required.

**Exclusion.** The Department of Health and Human Services (DHHS) has the authority to exclude from participation in Medicare any covered entity that was not compliant with the transaction and code set standards by Oct. 16, 2003 (where an extension was obtained and the covered entity is not small) (68 FR 48805).

**Enforcing Agencies.** The DHHS Office of Civil Rights (OCR) enforces the privacy standards, while the Centers for Medicare & Medicaid (CMS) enforces both the transaction and code set standards and the security standards (65 FR 18895).

**Practice Points.** It is important for RNs to be aware of identifying information that is protected by HIPAA which may not be initially perceived as health information. The Privacy Rule allows a covered entity to de-identify data by removing all 18 elements that could be used to identify an individual. Examples include name, address, phone number, account numbers, medical record numbers, fax numbers, website address, Social Security number, all geographic subdivisions smaller than a state, all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death, and biometric identifiers including voiceprints and fingerprints. Age also becomes an identifier in seniors older than age 89! The Privacy Rule protects all individually identifiable health information (PHI) held or transmitted by a covered entity or its business associates, in any form or media, whether electronic, paper, or oral. There are no restrictions on the use or disclosure of de-identified health information.

De-identified health information neither identifies nor provides a reasonable basis to identify and individual. There are two ways to de-identify information according to the United States Department of Health and Human Services: either (1) a formal determination by a qualified statistician; or (2) the removal of specified identifiers of the individual and of the individual’s relatives, household members, and employers is required, and is adequate only if the covered entity

### HIPAA Violation

<table>
<thead>
<tr>
<th>Minimum Penalty</th>
<th>Maximum Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA</strong></td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by state attorneys general regardless of the type of violation)</td>
</tr>
<tr>
<td><strong>$50,000 per violation, with an annual maximum of $1.5 million</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HIPAA violation due to reasonable cause and not due to willful neglect</strong></td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
</tr>
<tr>
<td><strong>$50,000 per violation, with an annual maximum of $1.5 million</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HIPAA violation due to willful neglect but violation is corrected within the required time period</strong></td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
</tr>
<tr>
<td><strong>$50,000 per violation, with an annual maximum of $1.5 million</strong></td>
<td></td>
</tr>
<tr>
<td><strong>HIPAA violation is due to willful neglect and is not corrected</strong></td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td><strong>$50,000 per violation, with an annual maximum of $1.5 million</strong></td>
<td></td>
</tr>
</tbody>
</table>
has no actual knowledge that the remaining information could be used to identify the individual.

Public Health and Safety Reporting Provisions. Most state and federal jurisdictions have a variety of statutes that impose a duty to report selected confidential patient and/or client information, which falls into one of four major categories: (a) vital statistics, such as births and deaths; (b) infections and communicable diseases, such as diphtheria, tetanus, syphilis, and active tuberculosis; (c) child or elder abuse and neglect; and, (d) violent incidents such as gunshot and knife wounds. The HIPAA Privacy Rule recognizes the legitimate need for public health authorities and others responsible for ensuring public health and safety to have access to protected health information to carry out their public health mission. The rule also recognizes that public health reports made by covered entities are an important means of identifying threats to the health and safety of the public at large, as well as individuals. Accordingly, the rule permits covered entities to disclose protected health information without authorization for specified public health purposes.

Generally, covered entities are required to reasonably limit the protected health information disclosed for public health purposes to the minimum amount necessary to accomplish the public health purpose. A “public health authority” is an agency or authority of the United States government, a state, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with a public health agency. Examples of a public health authority include state and local health departments, the Food and Drug Administration (FDA), the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration (OSHA).

Yes, they can! Workplace Medical Surveillance. A covered healthcare provider who provides a healthcare service to an individual at the request of the individual’s employer, or provides the service in the capacity of a member of the employer’s workforce, may...
such as a diagnosis of AIDS. The worksite if that is where the service is provided). 
provide the individual with written notice that the information will be disclosed to his or her employer (or the notice may be posted at the workplace if that is where the service is provided).

**Ensuring Confidentiality of Electronically Stored PHI on Computers.** A data security breach can have devastating consequences for healthcare organizations as well as patients and clients. To reduce the risk of such an occurrence, healthcare agencies have developed policies and procedures to ensure compliance with the HIPAA Security Rule, which has been mandatory since 2005. This rule governs the security of protected health information. Suggested guidelines and policies for covered entities and professional providers include:

- **A personal password is required** to enter and sign off computer entries, orders, files, along with policies against sharing this password with anyone, including other health team members.
- **Never leave a computer terminal unattended** after logging in.
- **Do not leave patient information displayed** on a monitor where others may see it.
- **Shred all computer-generated work sheets.**
- **Know the facility’s policy and procedure for correcting an entry error.**
- **Follow agency procedures** for documenting sensitive material such as a diagnosis of AIDS.
- **Information technology (IT) personnel must install a firewall** to protect the server from unauthorized access.

Covered entities and healthcare employers are required to keep all policies and procedures regarding HIPAA compliance in written format. All changes to policies and procedures must be distributed to affected employees. An any violation or employee sanction and the issue resolution must be documented. For example, except when treating or caring for the patient, any access of friends, relatives, or your own personal records will generally be reportable.

**The Patient Safety and Quality Improvement Act of 2005.** (PSQIA) establishes a voluntary reporting system designed to enhance the data available to assess and resolve patient safety and healthcare quality issues. To encourage the reporting and analysis of medical errors, PSQIA provides federal privilege and confidentiality protections for patient safety information, called patient safety work product. PSQIA authorizes HHS to impose civil money penalties for violations of patient confidentiality. PSQIA also authorizes the Agency for Healthcare Research and Quality (AHRQ) to list patient safety organizations (PSOs). PSOs are the external experts that collect and review patient safety information.

The Patient Safety Rule was published in the Federal Register on Nov. 21, 2008, and went into effect on Jan. 19, 2009. The Patient Safety Rule implements select provisions of PSQIA. In summary, the secretary of Health and Human Services adopted rules to implement certain aspects of the Patient Safety and Quality Improvement Act of 2005, Pub. L. 109–41 (Patient Safety Act). The final rule establishes a framework by which hospitals, doctors, and other healthcare providers may voluntarily report information to patient safety organizations (PSOs), on a privileged and confidential basis, for the aggregation and analysis of patient safety events. The final rule outlines the requirements that entities must meet to become PSOs and the processes by which the secretary will review and accept certifications and list PSOs. It also describes the privilege and confidentiality protections for the information that is assembled and developed by providers and PSOs, the exceptions to these privileges and confidentiality protections, and the procedures for the imposition of civil monetary penalties for the knowing or reckless impermissible disclosure of patient PHI.

The Patient Safety Act focuses on creating a voluntary program through which healthcare providers can share information relating to patient safety events with PSOs, with the aim of improving patient safety and the quality of care nationwide. The statute attaches privilege and confidentiality protections to this information, termed “patient safety work product,” to encourage providers to share this information without fear of liability and creates PSOs to receive this protected information and analyze patient safety events. These protections will enable all healthcare providers, including multi-facility healthcare systems, to share data within a protected legal environment, both within and across states, without the threat that the information will be used against the subject providers’ safety work product.

The Patient Safety Act is clear that it is not intended to interfere with the implementation of any provision of the HIPAA Privacy Rule. The statute also provides that civil monetary penalties cannot be imposed under both the Patient Safety Act and the HIPAA Privacy Rule for a single violation. In addition, the statute states that PSOs shall be treated as business associates, and patient safety activities are deemed to be healthcare operations under the HIPAA Privacy Rule.

When the Health Information Technology for Economic and Clinical Health (HITECH) Act was signed into law by President Obama on Feb. 17, 2009, it included a new definition of “breach” and requires business associates of covered entities to comply fully with the HIPAA Administrative Simplification Security Rule beginning Feb. 17, 2010. The new definition of breach follows and the Security Rule is available on the HIPAA.com website.

**Breach Notification Rule.** Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA-covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.

**HITECH Act definition of “breach.”**

(A) In General. The term “breach” means the unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

(B) Exceptions. The term “breach” does not include:

(i) Any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if -
(I) Such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate; and

(II) Such information is not further acquired, accessed, used, or disclosed by any person; or

(ii) Any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and

(iii) Any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.

Red Flag Rules. In response to these new privacy laws effective on Jan. 1, 2009, as well as other recent developments including Centers for Medicare and Medicaid Services (CMS) performing proactive auditing and enforcement of the HIPAA Security Rule, and the issuance of the Federal Trade Commission (FTC) Red Flag Rules, which requires organizations to implement an identity theft detection and prevention program, many employers are re-evaluating their privacy/security policies, computer access strategies and procedures.

It’s been well established that many healthcare entities are subject to compliance with the rule because of their billing and collection practices. Failure to comply can mean civil monetary penalties, but not criminal penalties, for violations.

According to the FTC, a red flag is “a pattern, practice, or specific account activity that indicates the possibility of identity theft.” Red flags include:

Alerts or warnings from a consumer reporting agency;

Suspicious documents and/or personal identifying information e.g., an inconsistent address or nonexistent Social Security number);

Unusual use of or suspicious activity concerning a patient account; and,

Notices of possible identity theft from patients, identity-theft victims, or law enforcement agencies.

However, there’s a twist that complicates compliance. The Joint Commission requires healthcare organizations to meet National Patient Safety Goals (NPSGs) to improve patient safety. Among other things, healthcare organizations, including acute-care and post-acute care facilities, must “reliably identify” the individual as the person for whom the service or treatment is intended. The Joint Commission requires healthcare organizations and providers to obtain two patient identifiers in order to reliably match the service or treatment to a specific individual.

Because of the economic downturn and the growing population of uninsured, identity theft, or co-opting someone’s financial identity in order to receive medical care will continue to be a growing concern. Nurses must also remain vigilant in order to protect patients from unscrupulous practitioners who perform procedures that aren’t medically indicated for financial gain.

HIPAA’s Effect on Research. For purposes of research and education, most agencies allow staff nurses, students, quality liaisons, and graduate health professionals access to patient records. The records are used in client conferences, clinics, rounds, studies, and written papers. The students and researchers are bound by strict legal and ethical obligation to hold all information in confidence. This holds true for RNs, NPs, and MDs who may plan to participate in morbidity and mortality conference for identification and mitigation of risk factors and evaluation of standards of care for compliance, or for debriefing and analysis after a sentinel event. RNs should not assume they have the authority as an individual to review and evaluate a patient’s plan of care once they are no longer caring for a patient who has expired, transferred off the unit, or has been discharged.

However, many researchers have reported that HIPAA restrictions have affected their ability to perform retrospective, chart-based research as well as their ability to prospectively evaluate patients by contacting them for follow-up. A study from the University of Michigan demonstrated that implementation of the HIPAA Privacy Rule resulted in a drop from 96 percent to 34 percent in the proportion of follow-up surveys completed by study patients being followed after a heart attack. Another study, detailing the effects of HIPAA on recruitment for a study on cancer prevention, demonstrated that HIPAA-mandated changes led to a 73 percent decrease in patient accrual, a tripling of time spent recruiting patients, and a tripling of mean recruitment costs.

In addition, informed consent forms for research studies now are required to include extensive detail on how the participant’s protected health information will be kept private. While such information is important, the addition of a lengthy, legalistic section on privacy may make these already complex documents even less user friendly for patients who are asked to read and sign them.

These data suggest that the HIPAA privacy rule, as currently implemented, may be having negative impacts on the cost and quality of medical research. Dr. Kim Eagle, professor of internal medicine at the University of Michigan was quoted as saying, “Privacy is important, but research is also important for improving care. We hope that we will figure this out and do it right.”

The complexity of HIPAA, combined with potentially stiff penalties for violators, can lead physicians and medical centers to withhold information from those who may have a right to it. A review of the implementation of the HIPAA Privacy Rule by the U.S. Government Accountability Office found that healthcare providers were “uncertain about their [legal] privacy responsibilities and often responded with an overly guarded approach to disclosing information than necessary to ensure compliance with the Privacy Rule.”

Reports of this uncertainty continue.

In addition, it should be noted that HIPAA provided a floor under the States regarding privacy, but it did not impose a privacy ceiling. It specifically empowered states to keep or pass their own privacy laws under certain circumstances. For example, many states single out certain classes of medical information for special handling. The most common include records of patient care involving mental health treatment, drug and alcohol abuse or addictions, and certain diseases such as HIV/AIDS. Although HIPAA usually preempts contrary state law, there are four situations in which state law preempts HIPAA. The exceptions are for: 1) state reporting laws; 2) health plan reporting and information; 3) specific exemptions determined by the HHS secretary; and 4) when state health privacy provisions are more stringent.

HIPAA versus Hype: The Role of Professional Judgment. Although abuse of electronic databases and communication created the need for explicit standards, as we now know, HIPAA standards are not limited to electronic information transfer. They apply to all personal health information—electronic, written, oral, and visual. In part, because of hefty fines associated with violations, many healthcare organizations have invested substantial resources to educate providers and employees.
about HIPAA. It’s become apparent that many of these “education” programs have been more focused on communicating threats of discipline and warnings to staff about the law rather than the proper place of privacy and confidentiality in patient care.

As nurses and other providers consider the restrictions on information transfer, whether based on HIPAA or on the precepts of professional ethics, one basic rule should be remembered: Patient care and patient safety come first! It should be noted that HIPAA contains explicit exceptions for payment, healthcare operations, and treatment. PHI that is required for these three purposes is exempt from HIPAA’s restrictions. When HIPAA appears to compromise good patient care or safety it most likely indicates a misunderstanding of HIPAA. Apparent conflicts between HIPAA and patient safety often reveal underlying unsafe practices that can disrupt workflow and put patients at risk. One often cited area of confusion and conflict that poses a conundrum for staff is between privacy and safety.

Our obligation to respect patient privacy is an ethical imperative, but we must also act in our patients’ best interests. The ethical precepts of beneficence and nonmalefence require that we ensure our patients’ safety in the things that we, as clinicians, do for them. We also have a duty to identify and change system problems that increase the risk of medical errors and harm. For instance, because recovery rooms and intensive care units are examples of patient care settings that should enhance our ability to observe and monitor immediate post-operative and critically ill patients for subtle signs and symptoms of deterioration and complications, one must judiciously question the use of privacy drapes in these settings, unless staffing permits continuous direct observation.

Incidental Uses and Disclosures. Many customary healthcare communications and practices play an important or even essential role in ensuring that individuals receive prompt and effective healthcare. Due to the nature of these communications and practices, as well as the various environments in which individuals receive healthcare or other services from covered entities, the potential exists for an individual’s health information to be disclosed incidentally. For example, a hospital visitor may overhear a provider’s confidential conversation with another provider or a patient, or may glimpse a patient’s information on a sign-in sheet or nursing station whiteboard.

The HIPAA Privacy Rule is not intended to impede these customary and essential communications and practices and, thus, does not require that all risk of incidental use or disclosure be eliminated to satisfy its standards. Rather, the Privacy Rule permits certain incidental uses and disclosures of protected health information to occur when the covered entity has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual’s privacy.

**How the Privacy Rule Works.** The Privacy Rule permits certain incidental uses and disclosures that occur as a by-product of another permissible or required use or disclosure, as long as the covered entity has applied reasonable safeguards and implemented the minimum necessary standard, where applicable, with respect to the primary use or disclosure. An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a result of another use or disclosure that is permitted by the rule. However, an incidental use or disclosure is not permitted if it is a by-product of an underlying use or disclosure which violates the Privacy Rule.

**Reasonable Safeguards.** A covered entity must have in place appropriate administrative, technical, and physical safeguards that protect against uses and disclosures not permitted by the Privacy Rule, as well as that limit incidental uses or disclosures. It is not expected that a covered entity’s safeguards guarantee the privacy of protected health information from any and all potential risks. Reasonable safeguards will vary from covered entity to covered entity depending on factors, such as the size of the covered entity and the nature of its business. In implementing reasonable safeguards, covered entities should analyze their own needs and circumstances, such as the nature of the protected health information it holds, and assess the potential risks to patients’ privacy. Covered entities should also take into account the potential effects on patient care and may consider other issues, such as the financial and administrative burden of implementing particular safeguards.

**Minimum Necessary Standard.** Covered entities must implement reasonable minimum necessary policies and procedures that limit how much protected health information is used, disclosed, and requested for certain purposes. These minimum necessary policies and procedures also reasonably must limit who within the entity has access to protected health information, and under what conditions, based on job responsibilities and the nature of the business. The minimum necessary standard does not apply to disclosures, including oral disclosures, among healthcare providers for treatment purposes.

---

**LIVE TO TELL**

*(Continued from page 9)*

suffering that those on Wall Street and inside the Beltway prefer not to see or hear. But we are not going to let them suffer in silence any longer. Send us your stories. Please go into your community. Ask your friends and neighbors to come out of the shadows and send us their stories as well. Go online at www.mainstreetcontract.org to tell your story and view others.

“My close friend has been out of work since a layoff in 2006. He has a graduate degree and is in his ‘60s and in spite of hundreds of applications no one wants to hire him. He receives roughly $1,000 a month in Social Security benefits, and occasionally receives extra income from freelance research projects. These are his only income except for $18 a month in food stamps. He has avoided homelessness only because he is staying in an abandoned house.”

—Washington State RN

“I never thought it would happen to me, but it did. Through a series of mismanagement and overtime being cut out, I find myself losing my home to foreclosure. The cost of living is so great I am considering moving to another state. At this point in life to have to start over is so difficult. While I would never ever harm myself, I do have to admit that to go to sleep and not wake up would be a relief, no struggling to pay the bills, no worries about working it out and finding my way.”

—Rhode Island RN

We are reminding people that it is not your fault. America is not broke. Don’t believe the lies from those who want to blame working people for a crisis you did not make and do not deserve, and join us in this campaign to make Wall Street pay, heal America, and rebuild our nation.

RoseAnn DeMoro is executive director of National Nurses United.