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 two of a two-part series. The first installment appeared in the July-August 2011 issue of National Nurse and is required reading for successful completion of this home study course.

Description

This home study course provides a review of pertinent HIPAA definitions, 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 analyze their own uses of health information and to otherwise obtaining full reimbursement down the road (i.e. as provided for in the HITECH Act).

Objectives: Upon completion of this home study 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

EHRs and Compliance Incentives. Ongoing implementation of electronic health records (EHRs) has raised many professional practice concerns with respect to surveillance, privacy, and security issues. Historically, it is safe to say that if a healthcare provider indicated they were HIPAA compliant, what they likely meant was that they were attempting to comply with the HIPAA Privacy Rule (especially true for small providers). With the recent enactment of The American Recovery and Reinvestment Act of 2009 (ARRA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act 2009) contained within it, things have become even more interesting.

The HITECH Act focuses on the establishment of a national health infrastructure and on providing incentives for the adoption of electronic health records (EHRs). It also provides for “enhanced” privacy protections. This act now places both the HIPAA Privacy Rule and the HIPAA Security Rule as front and center issues for healthcare providers. Now, not only are you or your employer subject to civil and criminal penalties for HIPAA violations and non-compliance, such non-compliance may actually prevent your employer from receiving financial incentives for EHR adoption and from otherwise obtaining full reimbursement down the road (i.e. as provided for in the HITECH Act).

HIPAA & HITECH Act—Words to the Wise. The HITECH Act substantially expanded the HIPAA Privacy and Security Rules and increased the penalties for HIPAA violations. Like the Privacy Rule, the Security Rule gives covered entities significant discretion to analyze their own uses of health information and, according to HHS standards, each covered entity has a perpetual duty to renew and modify its security provisions to ensure reasonable protection of EPHI. If a covered entity discovers that an employee has violated the privacy policies and procedures and/or EPHI security rules, it must discipline the employee and attempt to mitigate any potential harm that may result.

According to the Privacy Rights Clearinghouse, there have been more than 87 separate data breaches made public from Jan. 1 through June 10, 2011, which affected an aggregate of more than 5,000,000 individuals’ records. Unfortunately, being compliant is not synonymous with being secure. Although the majority of the reported data losses were not because of social media, privacy standards can easily be violated “when Facebook goes to the hospital” according to an August 2010 story in the Los Angeles Times. In the article, National Nurses United’s (NNU) Communications Director Chuck Idelson warns, “People may think they’re protected so that what they post can only be seen by a friend or family member, but life has proved otherwise.”

As hospitals and provider settings have grown more “wired” by the day, they have dramatically increased their reliance on the electronic creation, transmission, and storage of data. Add to this the human factors of curiosity and fascination with new technology. Many people using computers in their work settings are not techies or legal experts. They may have little intuition toward good security
practices, such as logging off or locking their work stations, and using strong passwords. They may be naïve and lack understanding of the inherent danger and liability that comes with sharing passwords. Less technically savvy staff may be unaware that global positioning technology and digital tagging of time and date of access and location of transmission from a portable or mobile device is discoverable and can be used as evidence for auditing purposes and investigation of alleged wrongdoing by the user.

In the legal arena, an appellate court has implied that a violation of the Privacy Rule may constitute a negligent breach of the fiduciary duty of confidentiality and a violation of professional standards. Therefore, a violation of the Privacy Rule can be used to establish the standard of care. HIPAA provides standards of conduct, and as such, when a nurse fails to comply with HIPAA, he or she may very well be judged to be negligent.

However, given HIPAA’s complexity and the discretion that it affords covered entities, HHS has recognized the difficulty in abiding by the Privacy and Security Rules. Therefore, rather than first issuing a fine for a violation, it works with covered entities to write and file a plan of correction and assists them in achieving compliance. Healthcare employers and risk-averse administrators may be less forgiving and many of them have adopted zero-tolerance policies for their employees. Many professionals are becoming concerned that a covered entities’ overly broad interpretation of HIPAA, and confusion as to what constitutes a reportable breach, will lead to selective retaliation, suspension, and firing of workers, rather than HHS-style education and mitigation. Nurses as a profession support patient confidentiality, as well as the right to due process and a fair hearing.

Unfortunately, recent newspaper and network media reports have been replete with stories regarding unauthorized social media postings and access to patients’ protected health information and the consequences imposed on violators. Egregious breaches of patient privacy are rare but they need to be dealt with swiftly. Therefore, NNU strongly urges nurses never to post patient-related information online and avoid unauthorized use of PHI. Nurses must always honor the trust patients and the public have placed in them.

Professionalism and Social Media: First, Do No Harm.

Scholar and educator William Arthur Ward once said, “Curiosity is the wick in the candle of learning.” And in her book, Notes on Nursing, Florence Nightingale wrote, “The most important practical lesson that can be given to nurses is to teach them what to observe—how to observe.” Thus, curiosity in nurses is informed by the scientific method. When patients begin to exhibit subtle signs and symptoms of deterioration in their condition, their very lives often hang in the balance. Education and experience leads to skilled inquiry, synthesis, and analysis of the patient’s condition, which may lead to treatment decisions and effective life interventions.

Contrast that with the old adage that says, “Curiosity killed the cat!” More relevant to this discussion are the words of the ancient Greek philosopher Plato. He said, “To be curious about that which is not one’s concern, while still ignorant of one’s self is ridiculous.” The inference to be drawn from this is that critical thinking and reflective practice will help nurses maintain appropriate professional boundaries and standards of conduct. Idle curiosity and ignorance of the risks inherent in the use of social networking sites such as Facebook, Twitter, and weblogs has the potential to kill your reputation and your career.

We’ve known that the World Wide Web is not only a medium to facilitate entertainment and acquisition of new knowledge; it also provides unparalleled opportunities for exhibitionism, voyeurism, and unwitting indiscretions. We are just beginning to understand the social costs in a digital age when so much of what we say and do, or what others say about us becomes permanently and publicly stored online in cyberspace. “The permanent memory bank of the Web increasingly means there are no second chances—no opportunities to escape a scarlet letter in your digital past. Now, the worst thing you’ve done is often the first thing everyone knows about you,” wrote New York Times columnist Jeffry Rosen in a July 21, 2010 article titled “The Web Means the End of Forgetting.”

A recent survey by Microsoft revealed that 75 percent of human resource professionals and recruiters do online research about job applicants. Many use a range of sites, including photo and video-sharing sites, personal blogs, Web pages, search engines, Twitter, and online gaming sites in addition to Facebook. In the same survey, 70 percent of recruiters reported they rejected applicants because of the information found online, such as membership in or contributions to “controversial” groups. According to company spokespersons, all information published on these sites should be presumed available to the general public. Legal experts agree that these public information sources can be legally used in criminal or other types of investigations.
Although invasion of privacy can result from a seemingly harmless curiosity over the medical records of an “A-List” movie star, or concern about coworkers, their children, or friends and family, it may not cause any actual damage. However, one can imagine situations in which the divulgence of private health information can result in extraordinary psychological hardship. The fact remains that HIPAA privacy and security violations constitute an unconscionable breach of professional ethical and moral principles.

Headline News: HIPAA Hall of Shame, Violators Meet the Press.

All over the world, celebrities, scholars, political leaders, and everyday people are challenged for ways to preserve control of their identities in a digital media world that never forgets or forgives. The solutions for protecting our privacy may be technological, legisliative, political, or judicial. Yet in an era of demands for full disclosure and calls for accountability and transparency, the French data-protection commissioner has reportedly called for a “constitutional right to oblivion” to allow citizens to enjoy a greater degree of anonymity online and in public. Until such time as our social mores and ethics lead us toward better control of ourselves, we should rightly expect more from each other as professionals than we do from technology.

JULY 2009: Actor George Clooney and his girlfriend were injured in a motorcycle accident and taken for treatment to a hospital in New Jersey. During Clooney’s hospital stay, several curious staff members and nurses who were not directly participating in his care pried into his medical records. The hospital conducted an investigation and suspended 27 staff members for one month without pay. Mr. Clooney was quoted as saying, “While I very much cared pried into his medical records. The hospital conducted an investigation and suspended 27 staff members for one month without pay. Mr. Clooney was quoted as saying, “While I very much

DECEMBER 2008: An LPN employed at an Arkansas clinic accessed the medical records of the plaintiff involved in a lawsuit against her husband, who had been in an auto accident. The patient had also suffered injuries in the accident and had joined in a lawsuit with other passengers seeking compensation for their injuries from the LPN’s husband. Her husband had been complaining about the upcoming legal proceedings and they were both suffering financial hardships with the loss of income. She gave her notes from the patient’s chart to her husband, who then called the former clinic patient, saying he intended to use the information against him. The patient called the clinic where the LPN worked and complained to the Arkansas district attorney. She was fired from her job, and her employer reported her to the nursing board, who sought revocation of her license. She was charged with violating HIPAA and with “conspiracy to wrongfully disclose PHI for personal gain with maliciously harmful intent in a personal dispute.” In a plea agreement with the federal prosecutor, she pleaded guilty to one count of wrongful disclosure of PHI. She also faced up to 10 years in prison and a fine of up to $250,000. In exchange for her plea to the lesser charge, charges against her husband were dropped.

MAY 2009: California health regulators fined a hospital $250,000 for privacy breach in a multiple birth (“Octomom”) case. The fine was the first monetary penalty imposed and largest allowed under a new state law enacted in 2008 after widely publicized privacy violations occurred at UCLA Medical Center involving Farah Fawcett, Britney Spears, California’s former First Lady Maria Shriver, and other celebrities. The state Department of Public Health found that breaches of the so-called Octomom’s records extended beyond the hospital.

Workers at other hospitals and the chain’s regional office were among those implicated. A total of 23 employees, including two doctors, were identified as having accessed the patient’s records without authorization. Of the 23 employees, 15 were either terminated or forced to resign under pressure, and eight faced other disciplinary actions. The doctors were not among those who were fired. The secretary of California’s Health and Human Services issued a statement that said, “It’s the hospital’s job to prevent these breaches from occurring, not just crack down after the fact.”

JULY 2009: Two employees, including an emergency room unit clerk, and the account services coordinator at a hospital in Arkansas became curious about the status of a patient they processed on admission for whom they’d been ordered to set up an alias by the charge nurse. After the patient had been moved to ICU, hospital records showed the clerk accessed the patient records three times, and the account representative accessed the record twelve times subsequent to the transfer, even though they had no legitimate job-related reason to do so. Records also showed they had received hospital training on HIPAA privacy laws. They were subsequently fired from their jobs.

The medical director of the hospital was reportedly home watching the TV news reports regarding the same patient, a local TV personality, who was beaten by an intruder at her home in October of 2008. He accessed patient records from his computer at home to determine if the news reports about the severity of her injuries were accurate. He admitted he accessed the files because he was curious, and stated that he then logged off the computer admitting that he knew it was inappropriate for him to be looking at the patient’s file. He had received HIPAA training. His medical privileges were
suspended for two weeks and he was required to complete an online HIPAA training module.

Pursuant to plea agreements with the United States, all three employees pleaded guilty to a misdemeanor violation of the health information privacy provisions of HIPAA. Each additionally faced a maximum penalty of one year of imprisonment and a fine of not more than $50,000, or both. In determining the actual sentences, federal judges can consult advisory U.S. sentencing guidelines, but they are not bound by them.

**JANUARY 2011:** A male nurse working at a hospital in Florida was fired for allegedly looking at Tiger Woods’ medical records. The nurse was accused of peeking at Woods’ medical records three times during a 10-minute period, when the golfer was admitted after crashing his car into a fire hydrant. The nurse in turn claimed someone else used his code to access the records and subsequently filed a lawsuit seeking reinstatement and $400,000 damages. He claimed he was wrongfully terminated as the case against him was based solely on circumstantial evidence.

**JANUARY 2011:** A group of female nursing students posted a picture of themselves posing with a placenta from a recently delivered mother during their lab course at a hospital in Missouri and posting it on Facebook. One student claimed she asked her nursing instructor for permission to post the photo to share their learning experience, but later that day the instructor called her back and asked her to remove the post. The student promptly complied. The students were expelled from the community college in suburban St. Louis. The students’ dismissal was overturned by a federal judge who ordered the school to reinstate them. He focused on the fact that the mother was not identifiable and argued that there was implied consent on the part of the instructor, and that the school’s response was overkill that violated the students’ due process rights.

According to a press release issued by the college, “The entire college community is disappointed that the students have decided to abandon the academic appeals process and take their grievances to the court for resolution. We regret that the students used such poor judgment to take such a unique educational opportunity that was presented in a private clinical setting and broadcast it on the Web. We teach our students to respect the confidentiality of patient care, which extends beyond the hospital room and includes situations when the nurse is not in the presence of the patient. The actions of the students showed not only poor judgment, but also a lack of respect and a complete disregard for the ethical standards of the nursing profession.

“We will do whatever we need to do to reassure the community that this behavior is not what we teach at the community college. Because we cannot tolerate such unprofessional behavior in our students, we took what we believed to be appropriate action. The behaviors of the students were insensitive and disrespectful toward

---

**References**


Ornstein, C., Kaiser Hospital Fined $250,000 for Privacy Breach
the mother and the human tissue involved. The fact that this story has so quickly gone viral is evidence itself of how damaging social media can be if not used appropriately.”

**APRIL 2011:** A Massachusetts hospital agreed to pay the U.S. government $1 million to settle potential violations involving the loss of protected health information (PHI) of 192 patients. Evidently a hospital employee, while commuting to work, accidently left documents behind on a subway train. The documents contained protected health information such as billing encounter forms containing the name, date of birth, medical record number, health insurer and policy number, diagnosis, and name of providers. An employee mistake resulted in costly violations.

**MAY 2011:** A laptop containing more than 1,500 patient names and their personal information was stolen from a medical billing company employee’s car. A medical billing and management company located in Goodlettsville, Tenn., reported the laptop stolen from the trunk of the worker’s vehicle at a mall on May 7, 2011. Since the incident, the company operates a toll-free call center to address questions and provide ID theft service at no cost to those affected. The company has now encrypted and password-protected all the laptops, reinforcing proper safety protocols with the staff.

**JULY 2011:** A Southern California university agreed to an $865,000 settlement with the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) resolving allegations it violated the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules. The complaints alleged that university employees repeatedly and without permissible reason looked at the electronic protected health information of two celebrity patients between 2005 and 2008.

The corrective action plan requires the university to implement Privacy and Security policies and procedures approved by OCR, to conduct regular and robust trainings for all employees who use protected health information, to sanction offending employees, and to designate an independent monitor who will assess compliance with the plan over three years. (The agreement specifies that it is neither an admission of liability on the part of the university nor a concession on the part of HHS that the university is in violation of HIPAA.)

A review of these recent incidents should prompt you to consider making an inquiry to locate and become familiar with your employer’s health information privacy and security policies. Also, it’s instructive to review the primary purpose of patient records.

A record is a valuable source of data that is used by all members of the healthcare team. Its purposes include communication, legal documentation, financial billing, education, research, and auditing-monitoring. The patient record is a means by which healthcare team members communicate patient needs and progress, individual therapy and treatment, content of conferences, patient education, and discharge planning. The plan of care needs to be clear to anyone

---


Nursing standards and honest, ethical fact-finding should not be compromised in the care planning and investigatory process, especially when the evaluation of a poor outcome may be the result of a system problem. Critical thinking attitudes, reflective practice, and applications in practice start with curiosity. Always ask why! Be prepared to question assumptions and confront bias and self-serving attitudes from peers and administrators. Recognize when your opinions may conflict with those of the patient, your peers, or management/supervisory personnel; review your position and decide how best to proceed to maintain professional standards and achieve professional goals and outcomes.

Recognize when more information is needed to make a decision and reach a conclusion. A clinical symptom or unexpected clinical outcome can indicate a variety of problems that require a systematic approach to problem-solving. Be wary of the easy or expedient answer. Use known scientific and practice-based criteria when making assessments and evaluations. Be thorough and identify the risks for problems of the same type to help prevent reoccurrence. Bring colleagues together for a patient care conference during a staff meeting. Look for patterns and identify solutions. Do not compromise nursing standards, patient privacy and confidentiality, or intellectual integrity when providing care or evaluating nursing care.

Avoiding Breaches in Confidentiality and the Pitfalls of Technology.

In 2006, the CNA/NNOC Joint Nursing Practice Commission, together with National Director of Nursing Practice and Patient Advocacy Hedy Dumpel, RN, JD reviewed their organizational “Position Statement on Telemursing,” Subsection IX, “Privacy and Protection of Individually Identifiable Health Information,” includes the following relevant problem statement:

“Electronic records make it easier to snoop or engage in chart browsing, which creates some concerns since hospital mergers have made it more likely that employees will receive medical care from their own institution. The most likely targets are certain patients, hospital employees, celebrities, and patients with a sensitive diagnosis.”

Indeed there are a growing number of news reports of citations, arrests, criminal penalties, and fines for violations of patient confidentiality and security breaches that have occurred in healthcare settings. CNA/NNOC’s position statement concludes with relevant recommendations, congruent with HIPAA guidelines, for prudent and proactive RN practice and patient protection:

- **No disclosures of health information** or genetic information without informed consent of patient and affected parties. Healthcare and genetic information about consumers should be disclosed for health purposes and/or research only. Under no circumstances can health information be used for hiring, firing, promotion, or to deny affordable health insurance or in any other way infringe on one’s civil rights.

- **Individuals or entities** who legally receive health information must be required to safeguard the information or be subjected to legal or disciplinary sanctions when trading such information for economic gains or undue advantage.

- **There will be no sanctions against registered nurses** or other healthcare workers for disclosing health information or records to authorized public officials for the purpose of patient advocacy and protecting the public interest.

- **Encourage the use of technical security safeguards** like audit trails, security codes, scrambling devices, passwords, or electronic blocks. Encryption of confidential information transmitted via Internet or other online means. Support legislation to classify Medical Expert Systems (MES) as products, not services, giving injured patients the right to litigate any injuries resulting from the use of such systems in the courts, pursuant to product liability principles.

- **Sponsor or support regulations** or legislation to assure the strictest regulation of Medical Expert Systems (Class III) medical devices, where such systems are to be marketed to the consumer for use without the supervision and intervention of a registered nurse or physician.

Conclusion

When it comes to information technologies, whether high tech or low tech, taking appropriate security measures to protect patient privacy and confidentiality remains a priority. Nurses must scrupulously follow all HIPAA-related policies and procedures outlined by their employers and take every reasonable action to prevent unauthorized people from viewing or having access to protected patient health data. In the spirit of professionalism, nurses must put patient well-being first and take responsibility for clinical practice. This includes questioning and working to change policies that don’t appear to be congruent with the intent of the law and published
HHS guidelines. Think twice before disclosing information to a third party. You don’t have to be tight-lipped about your patients; you should consult with and share information with colleagues who are directly involved in your patient's care.

In most cases you should consult with your manager, or your facility's compliance officer, regarding any apparent conflicts between the privacy rules and patient safety concerns. Many misconceptions arise from gaps in the regulations. These gaps are appropriately filled by professional judgment, informed by ethical guidelines. In the context of inadvertent disclosure of confidential patient information, the legal risks of good practice are very low.

Social networks, blogs, and other forms of Internet communications can enable nurses to have a professional presence online; however they can create new challenges. Nurses should weigh a number of considerations when maintaining a presence in cyberspace. Privacy settings are not absolute and once information or photos and videos are posted on the Internet, the content is likely to remain there permanently.

If nurses view content posted by their colleagues that is offensive and unprofessional, they have a responsibility to bring that information to the attention of the individual who posted it, so that he or she can remove it and take other appropriate actions as necessary. If the content appears to violate professional standards as discussed in the HIPAA Privacy and Security Rules and the individual does not take appropriate action to resolve the situation, you should discuss the matter with a union representative and the Professional Practice Committee. Referral of the matter to the facility compliance officer and/or other appropriate authorities may be necessary. Failure of the profession to regulate itself and hold its licensees accountable can undermine the public's trust of nurses.

HHS Answers to Frequently Asked Questions

Q: Can healthcare providers engage in confidential conversations with other providers or with patients, even if there is a possibility that they could be overheard?
A: Yes. The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this rule requiring covered entities to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that providers' primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, covered entities are free to engage in communications as required for quick, effective, and high-quality healthcare. The Privacy Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.

For example, the following practices are permissible under the Privacy Rule, if reasonable precautions are taken to minimize the chance of incidental disclosures to others who may be nearby:

- **Healthcare staff may orally coordinate services** at hospital nursing stations.
- **Nurses or other healthcare professionals may discuss a patient's condition over the phone** with the patient, a provider, or a family member.

A healthcare professional may discuss lab test results and plan of care with a patient or other provider in a joint treatment area.

A healthcare professional may discuss a patient's condition or treatment regimen in the patient's semi-private room.

Healthcare professionals may discuss a patient's condition during training rounds in an academic or training institution.

In these circumstances, reasonable precautions could include using lowered voices or talking apart from others when sharing protected health information. However, in an emergency situation, in a loud emergency room, or where a patient is hearing impaired, such precautions may not be practicable. Covered entities are free to engage in communications as required for quick, effective, and high-quality healthcare.

Q: Does the HIPAA Privacy Rule require hospitals and doctors’ offices to be retrofitted, to provide private rooms, and soundproof walls to avoid any possibility that a conversation is overheard?
A: No. The Privacy Rule does not require these types of structural changes be made to facilities.

Covered entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires that covered entities make reasonable efforts to prevent uses and disclosures not permitted by the rule. The department does not consider facility restructuring to be a requirement under this standard.

For example, the Privacy Rule does not require the following types of structural or systems changes:

- **Private rooms.**
- **Soundproofing of rooms.**
- **Encryption of wireless or other emergency medical radio communications which can be intercepted by scanners.**
- **Encryption of telephone systems.**

Covered entities must implement reasonable safeguards to limit incidental, and avoid prohibited, uses and disclosures. The Privacy Rule does not require that all risk of protected health information disclosure be eliminated. Covered entities must review their own practices and determine what steps are reasonable to safeguard their patient information. In determining what is reasonable, covered entities should assess potential risks to patient privacy, as well as consider such issues as the potential effects on patient care, and any administrative or financial burden to be incurred from implementing particular safeguards. Covered entities also may take into consideration the steps that other prudent healthcare and health information professionals are taking to protect patient privacy.

Examples of the types of adjustments or modifications to facilities or systems that may constitute reasonable safeguards are:

- Pharmacies could ask waiting customers to stand a few feet back from a counter used for patient counseling.

In an area where multiple patient-staff communications routinely occur, use of cubicles, dividers, shields, curtains, or similar barriers may constitute a reasonable safeguard. For example, a large
possible safeguard which reasonably limits incidental disclosures to the general public. The above examples of possible safeguards are not intended to be exclusive. Covered entities may engage in any practice that reasonably safeguards protected health information to limit incidental uses and disclosures.

Q. A hospital customarily displays patients’ names next to the door of the hospital rooms that they occupy. Will the HIPAA Privacy Rule allow the hospital to continue this practice?
A: Yes. The Privacy Rule explicitly permits certain incidental disclosures that occur as a by-product of an otherwise permitted disclosure—for example, the disclosure to other patients in a waiting room of the identity of the person whose name is called. In this case, disclosure of patient names by posting on the wall is permitted by the Privacy Rule, if the use or disclosure is for treatment (for example, to ensure that patient care is provided to the correct individual) or healthcare operations purposes (for example, as a service for patients and their families). The disclosure of such information to other persons (such as other visitors) that will likely also occur due to the posting is an incidental disclosure.

Incidental disclosures are permitted only to the extent that the covered entity has applied reasonable and appropriate safeguards and implemented the minimum necessary standard, where appropriate. See 45 CFR 164.502(a)(1)(iii). In this case, it would appear that the disclosure of names is the minimum necessary for the purposes of the permitted uses or disclosures described above, and there do not appear to be additional safeguards that would be reasonable to take in these circumstances. However, each covered entity must evaluate what measures are reasonable and appropriate in its environment. Covered entities may tailor measures to their particular circumstances.

Q: May mental health practitioners or other specialists provide therapy to patients in a group setting where other patients and family members are present?
A: Yes. Disclosures of protected health information in a group therapy setting are treatment disclosures and, thus, may be made without an individual’s authorization. Furthermore, the HIPAA Privacy Rule generally permits a covered entity to disclose protected health information to a family member or other person involved in the individual’s care. Where the individual is present during the disclosure, the covered entity may disclose protected health information if it is reasonable to infer from the circumstances that the individual does not object to the disclosure. Absent countervailing circumstances, the individual’s agreement to participate in group therapy or family discussions is a good basis for inferring the individual’s agreement.

How to HIPAA. The Office for Civil Rights, part of the Department of Health and Human Services, has a wide range of helpful information about HIPAA on its website, http://www.hhs.gov/ocr/hipaa, including the full text of the Privacy Rule, a HIPAA Privacy Rule Summary, fact sheets, and more than 200 Frequently Asked Questions, as well as many other resources to help healthcare providers and others understand the law.
HIPAA—The Health Insurance Portability and Accountability Act

For continuing education credit of 4.0 hours, please complete the following test, including the registration form at the bottom, and return to: NNU/Nursing Practice, 2000 Franklin St., Oakland, CA 94612. We must receive the completed home study no later than Dec. 15, 2011 in order to receive your continuing education credit.

1. A covered healthcare provider who provides a healthcare service at the request of an individual’s employer may not disclose the individual’s protected health information to the employer for the purposes of workplace medical surveillance.
   ❑ True    ❑ False

2. A suggested best practice for safeguarding your personal computer password includes sharing it with your team leader.
   ❑ True    ❑ False

3. Computers are infallible and have eliminated the need for the independent, professional clinical judgment of the RN.
   ❑ True    ❑ False

4. Covered entities and healthcare employers are required to keep all policies and procedures regarding HIPAA compliance in written format.
   ❑ True    ❑ False

5. Patient identifying information includes discharge data, fingerprint prints, and county of residence and individuals’ identifiable characteristics.
   ❑ True    ❑ False

6. Protecting patient confidentiality was always the sole responsibility of physicians until passage of the Health Insurance Portability and Accountability Act (Public Law 104-191) in 1996.
   ❑ True    ❑ False

7. RNs have a unique patient advocacy role in the healthcare delivery system and as information technology evolves, it is important that it is harnessed and controlled to best serve the privacy and confidentiality needs of our patients.
   ❑ True    ❑ False

8. The advantages of HIPAA are that employees can change jobs without losing coverage as a result of preexisting coverage exclusions as long as they have had 12 months of continuous group health coverage.
   ❑ True    ❑ False

9. The Food and Drug Administration, the Centers for Disease Control and Prevention, and the Occupational Safety and Health Administration are all considered public health authorities.
   ❑ True    ❑ False

10. The Health Insurance Portability and Accountability Act (HIPAA) was signed into law on August 21, 1996 by President George Bush after heated Congressional partisan debates.
    ❑ True    ❑ False

11. The HIPAA 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.
    ❑ True    ❑ False

12. The HIPAA Privacy Rule requires hospitals and doctors’ offices to be retrofitted to provide private rooms to avoid any possibility that a provider-patient conversation is overheard.
    ❑ True    ❑ False

Name:________________________________________________________________________________________
Address: ______________________________________________________________________________________
City:______________________________________________ State:_________ Zip: __________________________
Day phone with message machine: _____________________________ Email: _______________________________
RN license #: ______________________________Job Classification: ______________________________________

Continuing Education Test