Guidance to Significant Aspects of the HIPAA Privacy Rule

A Primer for CNAs

4.0 In-Service Hours

NOTE: This course is not accredited for RNs, LPNs, LVNs, or APNs.
This course is approved for 4 contact hours (4 in-service hours) for Certified Nursing Assistants.

Presented by:

CEU Professor®

www.CEUProfessorOnline.com

Guidance to Significant Aspects of the HIPAA Privacy Rule: *A Primer for CNAs*

By Marietta Farrell, RN, BSN and James D. Ealley, Esquire

NOTE: This course is not accredited for RNs, LPNs, LVNs, or APNs. This course is approved for 4 contact hours (4 in-service hours) for Certified Nursing Assistants.

OBJECTIVES:

At the completion of this course, the learner will be able to:

1. Explain the basic protections provided by the HIPAA Privacy Rule.
2. List the considered 'covered entities' of the HIPAA Privacy Rule.
3. Describe the policies and procedures covered entities must have in place.
4. Describe the specific types of information protected by the Rule
5. Explain Permitted Disclosures Under the Rule
6. Describe the Penalties for Non-Compliance

OVERVIEW:

The first-ever federal privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers took effect on April 14, 2003. Developed by the Department of Health and Human Services (HHS), these standards (the Privacy Rule) provide patients with access to their medical records and more control over how their personal health information is used and disclosed. They represent a uniform, federal floor of privacy protections for consumers across the country. State laws providing additional protections to consumers are not affected by this rule.

Congress called on HHS to issue patient privacy protections as part of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA included provisions designed to encourage electronic transactions and also required new safeguards to protect the security and confidentiality of health information. Health plans, health care clearinghouses, and those health care providers who conduct certain financial and administrative transactions (e.g., enrollment, billing and eligibility verification) electronically are required to comply with the provisions of the Privacy Rule. HHS has conducted extensive outreach and provided guidance and technical assistant to these providers and businesses to make it as easy as possible for them to implement the privacy protections established through the Privacy Rule. These efforts include answers to

hundreds of common questions about the rule, as well as explanations and descriptions about key elements of the rule.

PATIENT PROTECTIONS

The Privacy Rule ensures a national floor of privacy protections for patients by limiting the ways that health plans, pharmacies, hospitals and other covered entities can use patients' personal medical information. The regulations protect medical records and other individually identifiable health information, whether it is on paper, in computers or communicated orally. Key provisions of these standards include:

- **Access to Medical Records.** Patients generally should be able to see and obtain copies of their medical records and request corrections if they identify errors and mistakes. Health plans, doctors, hospitals, clinics, nursing homes and other covered entities generally should provide access these records within 30 days and may charge patients for the cost of copying and sending the records.
- **Notice of Privacy Practices.** Covered health plans, doctors and other health care providers must provide a notice to their patients how they may use personal medical information and their rights under the new privacy regulation. Doctors, hospitals and other direct-care providers generally will provide the notice on the patient's first visit and anytime thereafter upon request. Patients generally will be asked to sign, initial or otherwise acknowledge that they received this notice. Health plans generally must mail the notice to their enrollees upon initial enrollment and again if the notice changes significantly. Patients also may ask covered entities to restrict the use or disclosure of their information beyond the practices included in the notice, but the covered entities would not have to agree to the changes.
- **Limits on Use of Personal Medical Information.** The Privacy Rule sets limits on how health plans and covered providers may use individually identifiable health information. To promote the best quality care for patients, the rule does not restrict the ability of doctors, nurses and other providers to share information needed to treat their patients. In other situations, though, personal health information generally may not be used for purposes not related to health care, and covered entities may use or share only the minimum amount of protected information needed for a particular purpose. In addition, patients would have to sign a specific authorization before a covered entity could release their medical information to a life insurer, a bank, a marketing firm or another outside entity for purposes not related to their health care.
- **Prohibition on Marketing.** The Privacy Rule sets restrictions and limits on the use of patient information for marketing purposes. Pharmacies, health plans and other covered entities must first obtain an individual's specific authorization before disclosing their patient information for marketing. At the same time, the rule permits doctors and other covered entities to communicate freely with

patients about treatment options and other health-related information, including disease-management programs.

- **Stronger State Laws.** The federal privacy standards do not affect state laws that provide additional privacy protections for patients. The confidentiality protections are cumulative; the Privacy Rule sets a national "floor" of privacy standards that protect all Americans, and any state law providing additional protections continues to apply. When a state law requires a certain disclosure -- such as reporting an infectious disease outbreak to the public health authorities -- the federal privacy regulations does not preempt the state law.
- **Confidential Communications.** Under the Privacy Rule, patients can request that their doctors, health plans and other covered entities take reasonable steps to ensure that their communications with the patient are confidential. For example, a patient could ask a doctor to call his or her office rather than home, and the doctor's office should comply with that request if it can be reasonably accommodated.
- **Complaints.** Consumers may file a formal complaint regarding the privacy practices of a health plan or covered provider. Such complaints can be made directly to the covered provider or health plan or to HHS' Office for Civil Rights (OCR), which is charged with investigating complaints and enforcing the privacy regulation. Information about filing complaints should be included in each covered entity's notice of privacy practices.

HEALTH PLANS AND PROVIDERS

The Privacy Rule requires health plans, pharmacies, doctors and other covered entities to have policies and procedures to protect the confidentiality of protected health information about their patients. These requirements are flexible and scalable to allow different covered entities to implement them as appropriate for their businesses or practices. Covered entities must provide all the protections for patients cited above, such as providing a notice of their privacy practices and limiting the use and disclosure of information as required under the rule. In addition, covered entities must take some additional steps to protect patient privacy:

- **Written Privacy Procedures.** The rule requires covered entities to have written privacy procedures, including a description of staff that has access to protected information, how it will be used and when it may be disclosed. Covered entities generally must take steps to ensure that any business associates who have access to protected information agree to the same limitations on the use and disclosure of that information.
- **Employee Training and Privacy Officer.** Covered entities must train their employees in their privacy procedures and must designate an individual to be responsible for ensuring the procedures are followed. If covered entities learn an employee failed to follow these procedures, they must take appropriate disciplinary action.

- **Public Responsibilities.** In limited circumstances, the rule permits -- but does not require --covered entities to continue certain existing disclosures of health information for specific public responsibilities. These permitted disclosures include: emergency circumstances; identification of the body of a deceased person, or the cause of death; public health needs; research that involves limited data or has been independently approved by an Institutional Review Board or privacy board; oversight of the health care system; judicial and administrative proceedings; limited law enforcement activities; and activities related to national defense and security. The Privacy Rule generally establishes new safeguards and limits on these disclosures. Where no other law requires disclosures in these situations, covered entities may continue to use their professional judgment to decide whether to make such disclosures based on their own policies and ethical principles.
- **Equivalent Requirements for Government.** The provisions of the rule generally apply equally to private sector and public sector covered entities. For example, private hospitals and government-run hospitals covered by the rule have to comply with the full range of requirements.

MORE ON THE TYPES OF INFORMATION THAT IS PROTECTED

Protected Health Information. The Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "*protected health information (PHI).*"

"Individually identifiable health information" is information, including demographic data, that relates to:

- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,

and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.13 Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

De-Identified Health Information. 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 an individual. There are two ways to de-identify information; 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 has no actual knowledge that the remaining information could be used to identify the individual.

MORE ON WHO IS COVERED BY THE RULE?

The Privacy Rule, as well as all the Administrative Simplification rules, apply to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities").

Health Plans. Individual and group plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMOs"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. There are exceptions—a group health plan with less than 50 participants that is administered solely by the employer that established and maintains the plan is not a covered entity. Two types of government-funded programs are not health plans: (1) those whose principal purpose is not providing or paying the cost of health care, such as the food stamps program; and (2) those programs whose principal activity is directly providing health care, such as a community health center, or the making of grants to fund the direct provision of health care. Certain types of insurance entities are also not health plans, including entities providing only workers' compensation, automobile insurance, and property and casualty insurance.

Health Care Providers. Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. These transactions include claims, benefit eligibility inquiries, referral authorization requests, or other transactions for which HHS has established standards under the HIPAA Transactions Rule. Using electronic technology, such as email, does not mean a health care provider is a covered entity; the transmission must be in connection with a standard transaction. The Privacy Rule covers a health care provider whether it electronically transmits these transactions directly or uses a billing service or other third party to do so on its behalf. Health care providers include all "providers of services" (e.g., institutional providers such as hospitals) and "providers of medical or health services" (e.g., non-institutional providers such as physicians, dentists and other practitioners) as defined by Medicare, and any other person or organization that furnishes, bills, or is paid for health care.

MORE ON PERMITTED USES AND DISCLOSURES OF INFORMATION

Permitted Uses and Disclosures. A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: (1) To the Individual (unless required for access or accounting of disclosures); (2) Treatment, Payment, and Health Care Operations; (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations. Covered entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to make.

(1) To the Individual. A covered entity may disclose protected health information to the individual who is the subject of the information.

(2) Treatment, Payment, Health Care Operations. A covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities. A covered entity also may disclose protected health information for the treatment activities of any health care provider, the payment activities of another covered entity and of any health care provider, or the health care operations of another covered entity involving either quality or competency assurance activities or fraud and abuse detection and compliance activities, if both covered entities have or had a relationship with the individual and the protected health information pertains to the relationship.

> ***Treatment*** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another.
>
> ***Payment*** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual.
>
> ***Health care operations*** are any of the following activities: (a) quality assessment and improvement activities, including case management and care coordination; (b) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (c) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; (d) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (e) business planning, development, management, and administration; and (f) business management and general administrative activities of the entity, including but not limited to: de-identifying

protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

Most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization as described below.

Obtaining "consent" (written permission from individuals to use and disclose their protected health information for treatment, payment, and health care operations) is optional under the Privacy Rule for all covered entities. The content of a consent form, and the process for obtaining consent, are at the discretion of the covered entity electing to seek consent.

(3) Uses and Disclosures with Opportunity to Agree or Object. Informal permission may be obtained by asking the individual outright, or by circumstances that clearly give the individual the opportunity to agree, acquiesce, or object. Where the individual is incapacitated, in an emergency situation, or not available, covered entities generally may make such uses and disclosures, if in the exercise of their professional judgment, the use or disclosure is determined to be in the best interests of the individual.

Facility Directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information. A covered health care provider may rely on an individual's informal permission to list in its facility directory the individual's name, general condition, religious affiliation, and location in the provider's facility. The provider may then disclose the individual's condition and location in the facility to anyone asking for the individual by name, and also may disclose religious affiliation to clergy. Members of the clergy are not required to ask for the individual by name when inquiring about patient religious affiliation.

For Notification and Other Purposes. A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care. This provision, for example, allows a pharmacist to dispense filled prescriptions to a person acting on behalf of the patient. Similarly, a covered entity may rely on an individual's informal permission to use or disclose protected health information for the purpose of notifying (including identifying or locating) family members, personal representatives, or others responsible for the individual's care of the individual's location, general condition, or death. In addition, protected health information may be disclosed for notification purposes to public or private entities authorized by law or charter to assist in disaster relief efforts.

(4) Incidental Use and Disclosure. The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated. A use or disclosure of this information that occurs as a result of, or as "incident to," an otherwise

permitted use or disclosure is permitted as long as the covered entity has adopted reasonable safeguards as required by the Privacy Rule, and the information being shared was limited to the "minimum necessary," as required by the Privacy Rule.

(5) Public Interest and Benefit Activities. The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes. These disclosures are permitted, although not required, by the Rule in recognition of the important uses made of health information outside of the health care context. Specific conditions or limitations apply to each public interest purpose, striking the balance between the individual privacy interest and the public interest need for this information.

Required by Law. Covered entities may use and disclose protected health information without individual authorization as *required by law* (including by statute, regulation, or court orders).

Public Health Activities. Covered entities may disclose protected health information to: (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury, or disability and to public health or other government authorities authorized to receive reports of child abuse and neglect; (2) entities subject to FDA regulation regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury or workplace related medical surveillance, because such information is needed by the employer to comply with the Occupational Safety and Health Administration (OHSA), the Mine Safety and Health Administration (MHSA), or similar state law.

Victims of Abuse, Neglect or Domestic Violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.

Health Oversight Activities. Covered entities may disclose protected health information to health oversight agencies (as defined in the Rule) for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.

Judicial and Administrative Proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal. Such information may also be disclosed in response to a subpoena or other lawful process if certain assurances regarding notice to the individual or a protective order are provided.

Law Enforcement Purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions: (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness, or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

Cadaveric Organ, Eye, or Tissue Donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge. The Privacy Rule permits a covered entity to use and disclose protected health information for research purposes, without an individual's authorization, provided the covered entity obtains either: (1) documentation that an alteration or waiver of individuals' authorization for the use or disclosure of protected health information about them for research purposes has been approved by an Institutional Review Board or Privacy Board; (2) representations from the researcher that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purpose preparatory to research, that the researcher will not remove any protected health information from the covered entity, and that protected health information for which access is sought is necessary for the research; or (3) representations from the researcher that the use or disclosure sought is solely for research on the protected health information of decedents, that the protected health information sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is sought. A covered entity also may use or disclose, without an individuals' authorization, a limited data set of protected health information for research purposes (see discussion below).

Serious Threat to Health or Safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat). Covered entities may also disclose to law enforcement if the information is needed to identify or apprehend an escapee or violent criminal.

Essential Government Functions. An authorization is not required to use or disclose protected health information for certain essential government functions. Such functions include: assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services to the President, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs.

Workers' Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illnesses.

(6) Limited Data Set. A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed. A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.

STATE LAW

Preemption. In general, State laws that are contrary to the Privacy Rule are preempted by the federal requirements, which means that the federal requirements will apply. "Contrary" means that it would be impossible for a covered entity to comply with both the State and federal requirements, or that the provision of State law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. The Privacy Rule provides exceptions to the general rule of federal preemption for contrary State laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits.

Exception Determination. In addition, preemption of a contrary State law will not occur if HHS determines, in response to a request from a State or other entity or person, that the State law:

- Is necessary to prevent fraud and abuse related to the provision of or payment for health care,
- Is necessary to ensure appropriate State regulation of insurance and health plans to the extent expressly authorized by statute or regulation,
- Is necessary for State reporting on health care delivery or costs,
- Is necessary for purposes of serving a compelling public health, safety, or welfare need, and, if a Privacy Rule provision is at issue, if the Secretary determines that the intrusion into privacy is warranted when balanced against the need to be served; or
- Has as its principal purpose the regulation of the manufacture, registration, distribution, dispensing, or other control of any controlled substances (as defined in 21 U.S.C. 802), or that is deemed a controlled substance by State law.

PENALTIES FOR NON-COMPLIANCE

Compliance. Consistent with the principles for achieving compliance provided in the Rule, HHS will seek the cooperation of covered entities and may provide technical assistance to help them comply voluntarily with the Rule. The Rule provides processes for persons to file complaints with HHS, describes the responsibilities of covered entities to provide records and compliance reports and to cooperate with, and permit access to information for, investigations and compliance reviews.

Civil Money Penalties. HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement. That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. HHS may not impose a civil money penalty under specific circumstances, such as when a violation is due to reasonable cause and did not involve willful neglect and the covered entity corrected the violation within 30 days of when it knew or should have known of the violation.

Criminal Penalties. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.

REFERENCES

U.S. Department of Health and Human Services, "Protecting the Privacy of Patient's Health Information." March 12, 2007. http://www.ihs.gov/generalweb/webapps/sitelink/site.asp?link_gov=http://aspe.hhs.gov/admnsimp/index.shtml

U.S. Department of Health and Human Services, "Summary of the HIPAA Privacy Rule." May 2003. http://www.hhs.gov/ocr/privacysummary.pdf

Centers for Disease Control and Prevention, U.S. Department of Health and Human Services. "HIPAA Privacy Rule and Public Health, Guidance from the CDC." April 11, 2003. http://www.ihs.gov/generalweb/webapps/sitelink/site.asp?link_gov=http://aspe.hhs.gov/admnsimp/index.shtml