CheapNursingCEUs.com

HIPAA: Protecting Patients' Rights

Introduction

It has been argued that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is essential to health-related information, patients' rights, and the health care system. Thus, health care professionals should be familiar with current HIPAA regulations. This course will review HIPAA regulations, while providing insight on how current HIPAA regulations relate to the biggest cultural trends impacting today's health care system.

Section 1: HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) may refer to the specific federal regulations or laws which provide provisions for safeguarding medical information. HIPAA was enacted by the 104th United States Congress and signed into action by President Clinton in 1996. Since that time, HIPAA has undergone a variety of different modifications and updates to help increase its scope and effectiveness in protecting health-related information. Some of the more recent modifications/updates to HIPAA include the "Privacy Rule", the "Security Rule," and the "Final Omnibus Rule," otherwise referred to as the "Omnibus Rule." That being said, this section of the course will focus on the aforementioned modifications/updates to HIPAA. Relevant details from the Privacy Rule, the Security Rule, and the Final Omnibus Rule/Omnibus Rule will be highlighted below. The information found in this section was derived from materials provided by the federal government of the United States.[1,2]

The Privacy Rule

- The Standards for Privacy of Individually Identifiable Health Information, otherwise referred to as the Privacy Rule, establishes a set of national standards for the protection of certain health information.
- The Privacy Rule standards address the use and disclosure of individuals' health information, which is referred to as "protected health information" by organizations subject to the Privacy Rule. Organizations subject to the Privacy Rule are referred to as "covered entities." The Privacy Rule also sets standards for individuals' privacy rights to understand and control how their health information is used.
- One of the major goals of the Privacy Rule is to assure that individuals' health information is adequately protected while allowing the flow of health information needed to provide and promote high quality health care. Another major goal of the Privacy Rule is to protect the public's health and well being.

- The Privacy Rule applies to the following entities:
    - **Health plans** - in the context of this course, a health plan may refer to any plan which covers the cost of health care. Health plans that may be affected by the stipulations of the Privacy Rule 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). Additional health plans that may be affected by the stipulations of the Privacy Rule include: employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans.
    - **Health care providers** - essentially, every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions may be considered a covered entity.
    - **Health care clearinghouses** - in the context of this course, a health care clearinghouses may refer to any entity that processes nonstandard information from another entity into a standard format. Examples of health care clearinghouses include: billing services, re-pricing companies, and community health management information systems.
    - **Business associate** - in the context of this course, a business associate may refer to a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or to, a covered entity that involve the use or disclosure of individually identifiable health information.
- The Privacy Rule safeguards protected health information (PHI). PHI may refer to any information about health status, provision of health care, or payment for health care that is created or collected by a covered entity; individually identifiable health information. In essence, the Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate(s), in any form or media, whether electronic, paper, or oral.
- Health care professionals should note that individually identifiable health information is information, including demographic data, that relates to the following: an individual's past, present or future physical or mental health or condition, the provision of health care to an 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 it can be used to identify the individual (i.e., individually identifiable health information is

information that may be used to identify an individual and their relationship to the health care system). Health care professionals should also note that examples of individually identifiable health information includes patients': names, birth dates, home addresses, and Social Security Numbers (however, the Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and certain other records indicated by law).

- The Privacy Rule indicates that there are no restrictions on the use or disclosure of de-identified health information. De-identified health information may refer to information that neither identifies nor provides a reasonable basis to identify an individual (i.e., information that cannot, necessarily, link an individual to the health care system). Health care professionals should note the following two ways information may be de-identified: a formal determination by a qualified statistician may de-identify information; the removal of specified identifiers of the individual and of the individual's relatives, household members, and employers is completed, and is adequate only if the covered entity has no actual knowledge that the remaining information could be used to identify the individual.
- A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities.
- The Privacy Rule stipulates the following: a covered entity may not use or disclose protected health information, except as the Privacy Rule permits or requires; or as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing. Fundamentally, the Privacy Rule determines how PHI may be used and/or disclosed to protect individuals' privacy.
- The Privacy Rule indicates that a covered entity may use and disclose protected health information for its own treatment, payment, and health care operations activities.
- Health care professionals should note that treatment, in this context, may refer to the provision, coordination, or management of health care and related services for an individual/patient by one or more health care professional, including consultation between health care professionals regarding a patient and referral of a patient by one health care professional to another.
- Health care professionals should note that payment, in this context, 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 a patient and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to a patient.

- Health care professionals should note that health care operations, in this context, may include any of the following activities: quality assessment and improvement activities, including case management and care coordination; competency assurance activities, including health care provider or health plan performance evaluation, credentialing, and accreditation; conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance programs; specified insurance functions, such as underwriting, risk rating, and reinsuring risk; business planning, development, management, and administration; and 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.
- The Privacy Rule indicates the following: informal permission, regarding the use of PHI, may be obtained by asking an individual outright, or by circumstances that clearly give an individual the opportunity to agree, acquiesce, or object; when an individual is incapacitated (e.g., 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 an individual.
- The Privacy Rule does not require that every risk of an incidental use or disclosure of PHI be eliminated.
- The Privacy Rule indicates the following: covered entities may use and disclose PHI without individual authorization as required by law.
- The Privacy Rule indicates the following: covered entities may disclose PHI to 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.
- The Privacy Rule indicates the following: covered entities may disclose PHI to entities subject to the United Sates Food and Drug Administration's (FDA) regulations regarding FDA regulated products or activities for purposes such as adverse event reporting, tracking of products, product recalls, and post-marketing surveillance.
- The Privacy Rule indicates the following: covered entities may disclose PHI to individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law.

- The Privacy Rule indicates the following: covered entities may disclose PHI to 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 organizations such as the Occupational Safety and Health Administration (OHSA).
- The Privacy Rule indicates that in certain circumstances, covered entities may disclose PHI to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.
- The Privacy Rule indicates that covered entities may use or disclose PHI to facilitate the donation and transplantation of cadaveric organs, eyes, and/or tissue.
- The Privacy Rule indicates that covered entities may disclose PHI 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).
- The Privacy Rule indicates that an authorization is not required to use or disclose protected health information for certain essential government functions.
- The Privacy Rule stipulates the following: a covered entity must obtain the individual's written authorization for any use or disclosure of PHI that is not for treatment, payment or health care operations or otherwise permitted or required by the Privacy Rule.
- The Privacy Rule indicates that most uses and disclosures of psychotherapy notes for treatment, payment, and health care operations purposes require an authorization.
- The Privacy Rule stipulates the following: a covered entity must obtain an individual's authorization to use or disclose psychotherapy notes with the following exceptions - the covered entity who originated the notes may use them for treatment; a covered entity may use or disclose, without an individual's authorization, the psychotherapy notes, for its own training, and to defend itself in legal proceedings brought by an individual, for governmental investigations to determine the covered entity's compliance with the Privacy Rules, to avert a serious and imminent threat to public health or safety, to a health oversight agency for lawful oversight of the originator of the psychotherapy notes, for the lawful activities of a coroner or medical examiner or as required by law.
- Health care professionals should note the following: a central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum

amount of PHI needed to accomplish the intended purpose of the use, disclosure, or request. Essentially, the minimum necessary principle/rule can help prevent the disclosure of any unnecessary PHI. Health care professionals should always keep the minimum necessary principle/rule in mind when disclosing PHI.

- The Privacy Rule stipulates the following: a covered entity must establish and implement policies and procedures (which may be standard protocols) for routine, recurring disclosures, or requests for disclosures, that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure.
- The Privacy Rule stipulates the following: a covered entity, with certain exceptions, must provide a notice of its privacy practices.
- The Privacy Rule stipulates the following: a covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from patients of receipt of the privacy practices notice.
- The Privacy Rule indicates the following: individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.
- The Privacy Rule indicates the following: individuals have the right to request that a covered entity restrict use or disclosure of PHI for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death.
- The Privacy Rule indicates the following: a covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of PHI in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.
- The Privacy Rule requires a covered entity to treat a personal representative the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's rights under the Privacy Rule. A personal representative may refer to any individual legally authorized to make health care decisions on an individual's behalf or to act for a deceased individual or the estate.

- The Privacy Rule indicates the following: typically, parents are the personal representatives for their minor children (the term minor child may refer to any individual under a specific age, typically under the age of 18). Therefore, in most cases, parents can exercise individual rights, such as access to medical records, on behalf of their minor children.
- Health care professionals should note the following: generally, state laws that are contrary to the Privacy Rule are preempted by the federal requirements, therefore federal requirements will apply.

The Security Rule

- The Security Standards for the Protection of Electronic Protected Health Information, otherwise referred to as the Security Rule, was enacted to establish a national set of security standards for protecting certain health information that is held or transferred in electronic form.
- The Security Rule addresses the technical and non-technical safeguards that covered entities must put in place to secure individuals' electronic protected health information (e-PHI).
- The Security Rule was enacted to work in conjunction with the Privacy Rule.
- One of the major goals of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt and utilize technologies to improve the quality and efficiency of patient care (i.e., the aim of the Security Rule is to establish a means to protect patient-health related information as new technologies are incorporated into the health care system).
- Health care professionals should note the following: the Security Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form.
- Health care professionals should note the following: the Security Rule protects a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form; the Security Rule pertains to electronic health information.
- Health care professionals should note the following: the Security Rule does not apply to PHI transmitted orally or in writing.

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting e-PHI; the Security Rule indicates that electronic patient information must be protected.
- The Security Rule requires that covered entities ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit; covered entities identify and protect against reasonably anticipated threats to the security or integrity of the information; covered entities protect against reasonably anticipated, impermissible uses or disclosures; covered entities ensure compliance by their workforce (i.e., health care organizations must make sure health care professionals adhere to the stipulations put forth by the Security Rule).
- Health care professionals should note that according to the Security Rule, the term confidentiality refers to the following: e-PHI is not available or disclosed to unauthorized persons.
- The Security Rule allows covered entities to analyze their own needs and implement solutions appropriate for their specific environments.
- The Administrative Safeguards provisions in the Security Rule requires covered entities to perform risk analysis as part of their security management processes (i.e., covered entities must assess the implementation of all related electronic safeguards established to protect e-PHI). Health care professionals should note that the process of risk analysis should be ongoing.
- The Security Rule indicates that a covered entity must identify and analyze potential risks to e-PHI, and must safeguard individuals against potential risks to e-PHI.
- The Security Rule indicates that a covered entity designate a security official who is responsible for developing and implementing its security policies and procedures. Health care professionals should be aware of their health care organization's security official.
- Health care professionals should apply the minimum necessary principle/rule to e-PHI. The minimum necessary rule can help prevent the disclosure of any unnecessary e-PHI. Health care professionals should always keep the minimum necessary rule in mind when disclosing e-PHI.
- The Security Rule requires a covered entity to implement policies and procedures for authorizing access to e-PHI only when such access is appropriate based on the user or recipient's role. When considering the previous Security Rule stipulation, health care professionals should keep in mind the principle of role-based access.

Essentially, the principle of role-based access indicates that a health care professional may have access to e-PHI if his or her role deems such access appropriate or necessary (i.e., if a health care professional's designated role does not require access to specific e-PHI then a health care professional should not access said e-PHI). The term "need to know basis" may be applied to the previous concepts - health care professionals may access e-PHI only when they "need to know" or need such information to carry out safe and effective health care to those patients in need.

- The Security Rule indicates that a covered entity must train all workforce members regarding its security policies and procedures. If health care professionals believe they do not have such training, they should make attempts to receive training related to their health care organization's security policies and procedures.
- The Security Rule indicates that a covered entity must implement policies and procedures to specify proper use of and access to workstations and electronic media.
- The Security Rule indicates that a covered entity must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted over an electronic network.
- The Security Rule stipulates the following: if a covered entity knows of an activity or practice of a business associate that constitutes a material breach or violation of the business associate’s obligation, the covered entity must take reasonable steps to stop the breach or end the violation. With that in mind, health care professionals should consider reporting any potential business associate breaches into e-PHI to their associated health care organization.
- The Security Rule stipulates the following: a covered entity must periodically review and update its documentation in response to environmental or organizational changes that affect the security of e-PHI. Health care professionals should be aware of any such revisions if applicable.
- Health care professionals should note the following: the Security Rule establishes a set of national standards for confidentiality, integrity and availability of e-PHI; the Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR) are responsible for administering and enforcing Security Rule standards and may conduct complaint investigations and compliance reviews.
- Health care professionals should note the following: generally, state laws that are contrary to HIPAA/Security Rule regulations are preempted by the federal requirements, which means that the federal requirements will apply. In essence, if a

health care professionals has any questions regarding state and federal laws, they should consider following federal laws, when they relate to HIPAA/Security Rule concerns.

The Final Omnibus Rule

- The Omnibus Rule was needed to strengthen the privacy and security protections established under HIPAA for individual's health information maintained in electronic health records and other formats.
- The Omnibus Rule makes changes to HIPAA rules and are designed to increase flexibility and decrease the burden on the regulated entities.
- The Omnibus Rule is comprised of four final rules, which have been combined to reduce the impact and number of times certain compliance activities need to be undertaken by the regulated entities.
- The Omnibus Rule implements changes to the HIPAA rules under a number of authorities. The Omnibus Rule modifies the Privacy, Security, and Enforcement Rules to strengthen privacy and security protections for health information and to improve enforcement as provided for by the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The rule also includes final modifications to the Breach Notification Rule, which will replace an interim final rule originally published in 2009 as required by the HITECH Act. Second, the final rule revises the HIPAA Privacy Rule to increase privacy protections for genetic information as required by the Genetic Information Nondiscrimination Act of 2008 (GINA).
- One of the main goals of the Omnibus Rule is to expand patient rights.
- The Omnibus Rule allows patients to ask for a copy of their electronic medical record in electronic form.
- The Omnibus Rule implements HITECH's requirement that providers follow patient requests that their PHI not be disclosed to a health plan for payment or for health care operations purposes if the disclosure is not required by law and relates solely to items or services for which the patient paid out of pocket in full.
- The Omnibus Rule expands the definition of a "business associate" to include all entities that create, receive, maintain, or transmit PHI on behalf of a covered entity. Furthermore, the Omnibus Rule clarifies that the definition of a business associate also includes relevant subcontractors, ensuring that a covered entity's or business associate's security requirements encompass outsourced operations. Health

care professionals should note that the aforementioned changes/clarifications were made to strengthen the protection of PHI.

- The Omnibus Rule indicates that covered entities and their business associates must conduct an incident risk assessment for every data security incident that involves PHI.
- The Omnibus Rule indicates that PHI may no longer be used in most marketing activities without patient authorization if the covered entity is compensated for making the communication by a third party (e.g., a pharmaceutical company) that is promoting its own product; the Omnibus Rule requires authorization for all treatment and communications where the covered entity receives financial remuneration for making the communications from a third party whose product or service is being marketed. Health care professionals should note the aforementioned changes were made to strengthen the protection of PHI.
- The Omnibus Rule allows covered entities to disclose the immunization records of students or prospective students to a school if state law requires the school to have proof of immunization and the covered entity obtains and documents the agreement of the parent or guardian.
- The Omnibus Rule incorporates genetic information into the definition of PHI, which extends HIPAA's privacy protections to individuals' genetic information.
- The Omnibus Rule generally prohibits the sale of PHI, defined as remuneration (financial or otherwise) in exchange for PHI, without individual authorization. Health care professionals should note that exceptions may apply to the previous stimulation when PHI may be used for certain public health purposes.
- The Omnibus Rule indicates the following: research studies involving PHI that have been required to use multiple consent forms may use a single form. The aforementioned stipulation was made to limit patient confusion regarding consent forms.
- Health care professionals should note the following: the Omnibus Rule offers a means for researchers to obtain prospective consent for future research studies; prospective consent may be used in such cases, as long as an individual receives an adequate description of the scope of potential future research so that individuals can reasonably anticipate how their PHI may be used.
- The Omnibus Rule indicates the following: covered entities should treat improper disclosures of PHI presumptively as breaches unless certain statutory conditions

exist. Health care professionals should note and potentially report any observed improper disclosures of PHI.

- The Omnibus Rule requires health care organizations to conduct a risk assessment following every PHI privacy or security-related incident to determine if individual notification is required. Health care professionals should comply with security-related risk assessments, unless said assessments conflict with related HIPAA laws.
- The Omnibus Rule clarifies that the assessment of violations includes consideration of the number of individuals affected, the length of noncompliance, and the severity of culpability; enforced penalties for violations may reach a cap of $1.5 million per identical violation type per year.
- The Omnibus Rule also supports the use of both limited data sets and de-identified data without individual authorization.
- • The Omnibus Rule clarifies that a health plan may continue to use or disclose protected health information that is genetic information as required by other laws.
- The Omnibus Rule indicates that all copies of PHI to third parties must be authorized.
- The Omnibus Rule indicates the following: decedents' PHI is under HIPAA protection for 50 years after death.
- The Omnibus Rule indicates new categories of PHI may be used or disclosed for fundraising.
- The Omnibus Rule indicates that covered entities may combine "conditioned" and "unconditioned" authorizations for research to simplify authorization paperwork.
- The Omnibus Rule reinforces the importance of the following: health care professionals should meet all requirements regarding patient privacy and data security.
- The Omnibus Rule indicates the term willful neglect may refer to the conscious, intentional failure or reckless indifference towards PHI. Health care professionals should note that according to the Omnibus Rule, all case of willful neglect will be investigated.
- The Omnibus Rule works to align state and federal laws.
- The Omnibus Rule clarifies that contrary state laws are to be preempted by the federal breach law.

Section 1: Summary

HIPAA may refer to the specific federal regulations or laws which provide provisions for safeguarding medical information. HIPAA was enacted by the 104th United States Congress and signed into action by President Clinton in 1996. Since that time, HIPAA has undergone a variety of different modifications and updates to help increase its scope and effectiveness in protecting health-related information. Health care professionals should be aware of HIPAA updates to best serve patients.

Section 1: Key Concepts

- HIPAA provides provisions for safeguarding medical information.
- Since its initiation, HIPAA has undergone a variety of different modifications and updates to help increases its scope and effectiveness in protecting health-related information; some of the more recent modifications/updates to HIPAA include the "Privacy Rule", the "Security Rule," and the "Final Omnibus Rule" or "Omnibus Rule."
- One of the major goals of the Privacy Rule is to assure that individuals' health information is adequately protected while allowing the flow of health information needed to provide and promote high quality health care; another major goal of the Privacy Rule is to protect the public's health and well being.
- The Privacy Rule safeguards PHI.
- The Security Rule addresses the technical and non-technical safeguards that covered entities must put in place to secure individuals' e-PHI.
- One of the main goals of the Security Rule is to protect the privacy of individuals' health information while allowing covered entities to adopt and utilize technologies to improve the quality and efficiency of patient care; another goal of the Omnibus Rule is to expand patients' rights.
- The Omnibus Rule allows patients to ask for a copy of their electronic medical record in electronic form.
- A central aspect of the Privacy Rule/ Security Rule/ Omnibus Rule is the principle of "minimum necessary" use and disclosure; a covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of PHI/e-PHI needed to accomplish the intended purpose of the use, disclosure, or request; the minimum necessary rule can help prevent the disclosure of any unnecessary PHI/e-PHI; health care professionals should always keep the minimum necessary rule in mind when disclosing PHI.

- State laws that are contrary to HIPAA regulations are preempted by the federal requirements, which means that the federal requirements will apply.

Section 1: Key Terms

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) - specific federal regulations or laws which provide provisions for safeguarding medical information

Health plan *(in the context of this course)* - any plan which covers the cost of health care

Health care clearinghouses *(in the context of this course)* - any entity that processes nonstandard information from another entity into a standard format

Business associate *(in the context of this course)* - a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or to, a covered entity that involve the use or disclosure of individually identifiable health information

Protected health information (PHI) - any information about health status, provision of health care, or payment for health care that is created or collected by a covered entity; individually identifiable health information

De-identified health information - information that neither identifies nor provides a reasonable basis to identify an individual; information that cannot, necessarily, link an individual to the health care system

Treatment - the provision, coordination, or management of health care and related services for an individual/patient by one or more health care professional, including consultation between health care professionals regarding a patient and referral of a patient by one health care professional to another

Personal representative - any individual legally authorized to make health care decisions on an individual’s behalf or to act for a deceased individual or the estate

Minor child - any individual under a specific age, typically under the age of 18

Willful neglect - the conscious, intentional failure or reckless indifference towards PHI

Section 1: Personal Reflection Question

How do current HIPAA regulations protect patients' rights?

Section 2: HIPAA Regulations and Cultural Trends Impacting Today's Health Care System

As previously mentioned, HIPAA was established in 1996, and has since underdone a variety of different modifications and updates to expend both its scope and effectiveness in protecting patients' rights. With that said, how do the current HIPAA regulations relate to some of the biggest cultural trends impacting today's health care system? To best answer the aforementioned question, this section of the course will examine the relationship between current HIPAA regulations and two of the biggest cultural trends impacting today's health care system, the use of social media and the current opioid epidemic. The information found in this section was derived from materials provided by the federal government of the United States, the Centers for Disease Control and Prevention (CDC), and the FDA.[1,2,3,4]

Social Media

One of the biggest cultural trends impacting today's health care system is the use of social media. The term social media may refer to any electronically driven application that enables individuals to create and share content for the purposes of virtual communication. Since its initial inception, social media has impacted the greater cultural constructs it has been a part of, and, in more recent years, the use of social media has began to impact the health care system. That being the case, how do HIPAA regulations relate to the use of social media? In essence, HIPAA regulations relate to the use of social media under one very straightforward umbrella concept, which is as follows: under no circumstance should health care professionals use or disclose PHI on any form of social media. In other words, health care professionals should never share any health-related information, that may be used to identify a patient, on any form of social media. With that said, how can health care professionals ensure they do not violate HIPAA regulations regarding PHI and social media? Health care professionals can ensure they do not violate HIPAA regulations regarding PHI and social media by adhering to the following related recommendations.

Social Media Recommendations for Health Care Professionals

- Health care professionals should always remember that HIPAA regulations prohibit the use of PHI on any form of social media - when considering the use of health-related information on social media channels, health care professionals should always remember that HIPAA regulations prohibit the use of PHI on any form of social media (i.e., health care professionals should not use PHI on Facebook, Twitter, Snapchat or any other form of social media). Basically, this recommendation advises health care professionals to avoid using any individually identifiable health

information, that may link an individual to the health care system in any way, on social media. Health care professionals should note the following: individually identifiable health information is information, including demographic data, that relates to the following - an individual's past, present or future physical or mental health or condition, the provision of health care to an 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 it can be used to identify the individual; individually identifiable health information is information that may be used to identify an individual and their relationship to the health care system. Health care professionals should also note that examples of individually identifiable health information may include: patients' names, birth dates, home addresses, and Social Security Numbers.

- Apply the "When in Doubt Rule" to health-related information and social media - this recommendation builds upon the first recommendation. The When in Doubt Rule may be applied to health-related information and social media as follows: if a health care professional has any doubt whether he or she should use specific health-related information on social media, then the health care professional should not use the specific health-related information on social media. It is that straightforward: when in doubt do not use health-related information on social media forms.

- Health care professionals should not use patient pictures on social media - as previously indicated, health care professionals should not use any information that may link an individual to the health care system - that includes pictures of patients. Individuals may be identified in pictures and then eventually linked to the health care system, thus, health care professionals should avoid using any patient picture on social media.

- Health care professionals should not use health-related information about rare diseases or rare injuries on social media - this recommendation may raise an eyebrow or two, but it is important for health care professionals to avoid using health-related information about rare diseases or rare injuries on social media. Essentially, health-related information about rare diseases or injuries could link a specific individual to the health care system, even if the health-related details do not include any individually identifiable health information. For example, a third party could observe health-related information about a rare disease or injury on social media, and then through the process of elimination or though the process of correlating information from other sources, the third party could use said information to identify a patient. Health care professionals should note that examples, like the previous hypothetical example, have actually occurred. Health

care professionals used health-related information, which did not include individually identifiable health information, about a rare disease or injury on social media, which was then used by a third party to identify a patient - thus, violating the patient's privacy, personal rights, as well as HIPAA regulations. Health care professionals should consider such examples when considering the use of health-related information on social media, and should remember that the use of any health-related details on social media, whether those health-related details are associated with individually identifiable health information or not, may be used to identify a patient.

- Health care professionals should not gossip about patients on social media - much like with the use of health-related information about rare diseases or rare injuries on social media, the use of health care professional gossip on social media may be used by a third party to identify an individual. In the context of this course, gossip may refer to the transmission of messages regarding the personal and/or private details of other individuals' lives, health, overall well-being, quality of life and/or health care. Under no circumstance should health care professionals gossip about patients on social media. There have been several examples where health care professional gossip on social media has been used by a third party to link an individual to the health care system. Health care professionals should note that even if gossip may seem general or may not be associated with specific individually identifiable health information, it may still be traced back and used to identify a patient. The example below will illustrate the previous concept:

  Health Care Professional 1 posts gossip about a patient on social media. The gossip in question provides details about the patient's overall demeanor, attitude, and some general information about the patient's health care. The gossip posted on social media does not include any individually identifiable health information that may be directly associated with the patient, however it does refer to the patient as "The Drama Queen." Health Care Professional 2, who works in the same health care facility as Health Care Professional 1, observes the patient gossip posted by Health Care Professional 1. Health Care Professional 2 reads the gossip post and is intrigued - however, Health Care Professional 2 is not sure who Health Care Professional 1 is referring to until the reference "The Drama Queen" is observed. Upon reading "The Drama Queen" reference Health Care Professional 2 immediately associates the aforementioned reference with one specific patient. Health Care Professional 2 has heard the "The Drama Queen" reference while working and knows that it only pertains to one specific patient (i.e., Health Care Professional 2 links the gossip to a specific patient). From what Health Care Professional 2 knows about the patient in question and from what is obtained from the posted

gossip, Health Care Professional 2 is able to connect further health related details to the patient and the patient's health care, ultimately, learning information about the patient that would have, otherwise, been protected. Essentially, through Health Care Professional 1's gossip post on social media, Health Care Professional 2 was able to associate PHI with the patient referred to as "The Drama Queen," which may be viewed upon as a violation of the patient's rights.

In the previous example, the gossip posted on social media did not include any individually identifiable health information, however, it was still used to link a patient to health care. Health care professionals should consider the previous example, and ones like it, when attempting to use patient gossip on social media - doing so, could violate patient's privacy, personal rights, and related HIPAA regulations.

- Health care professionals should consider that information deleted on some social media channels may be saved in some capacity - essential, just because information is deleted on some social media channels, it does not mean it is not saved in some capacity - meaning that once information is posted on some social media channels it may perpetually exist in some format even if it is "removed" or "deleted" from the social media channel. Health care professionals should consider the previous concept before they use health-related information on social media.
- Health care professionals should consider the repercussions for violating HIPAA regulations before they use health-related information on social media - violations of HIPAA regulations could result in disciplinary actions for health care professionals. Disciplinary actions for HIPAA violations could range from formal reprimands, to termination, to fines, and even jail time. Health care professionals should consider those possibilities before they use health-related information on social media - doing so, could help prevent a health care professional from violating HIPAA regulations, and experiencing the negative repercussions that may follow such a violation. In essence, health care professionals should ask themselves the following question before using any form of social media: is the use of health-related information on social media worth jeopardizing my career? If the answer is no to the previous question, then maybe health care professionals should not proceed to use such information on social media.
- Along with health care professionals, health care organizations can also help prevent violations of HIPAA regulations via social media. Recommendations that may be used by health care organization to help prevent violations of HIPAA regulations via social media may be found below.

Social Media Recommendations for Health Care Organizations

- Health care organizations should develop policies regarding the use of social media - health care organizations should have policies, regarding the use of social media, in place to help guide health care professionals. Health care professionals should be aware of such policies. If no such policies exist within a health care organization, health care professionals should consider developing such policies to help prevent violations of HIPAA regulations via social media.
- Health care organizations should ensure health care professionals understand internal policies related to social media - it is not enough for a health care organization to have social media policies. Health care organizations should ensure health care professionals are aware of social media policies and understand them. Health care professionals should seek out health care organizations' policies regarding social media.
- Health care organizations should educate health care professionals regarding the use of social media - education seminars, course, and/or lectures may be used to educate health care professionals regarding the use of social media. Health care professionals are encouraged to participate in any educational offerings to further their knowledge and understanding of HIPAA regulations and social media.
- Health care organizations should consider including information regarding the use of social media in employee hand books or equivalent materials - including information regarding the use of social media in employee hand books or equivalent materials could provide a means for employee education.
- Health care organizations should not encourage health care professionals to engage with patients via private social media channels - such communication could potentially lead to HIPAA violations.
- Health care organizations should monitor related social media accounts - if a health care organization has a social media account(s), it should be monitored for potential HIPAA violations.
- Health care organizations should ensure they have a means to save information used on their social media accounts - the ability to save information used on health care organizations' social media accounts could prove to be invaluable if any potential HIPAA violations arise. Health care professionals should be aware that any information used on social media may be saved in some capacity.
- Health care organizations should encourage health care professionals to report any potential HIPAA violations - if a health care professional observes a potential HIPAA

violation, he or she should consider reporting the potential HIPAA violation to their health care organization.

- Health care organizations should have internal channels for HIPAA violation reporting
- It is not enough for a health care organization to encourage the reporting of potential HIPAA violations, a health care organization should have established, internal channels or networks for such reporting. Furthermore, health care organizations should make sure individuals are aware of such networks to encourage HIPAA reporting. Moreover, health care organizations should ensure reporting networks work to efficiently and effectively investigate and resolve any potential HIPAA violation. Health care professionals should be aware of their health care organizations' means for HIPAA violation reporting.

Opioid Epidemic

Many argue that the current opioid epidemic gripping the nation is among the biggest cultural trends impacting today's health care system. Thus, health care professionals should have some insight into the current opioid epidemic as well as how HIPAA, and similar laws which protect patients' rights, relate to the opioid epidemic. This subsection of the course will provide information regarding the current opioid epidemic and how HIPAA, as well as similar laws which protect patients' rights, relate to the opioid epidemic. Information regarding the current opioid epidemic may be found in Figure 1. Information regarding HIPAA/similar laws and the opioid epidemic may be found below Figure 1.

FIGURE 1: INFORMATION REGARDING THE CURRENT OPIOID EPIDEMIC

- The CDC reports that approximately 68% of the more than 70,200 drug overdose deaths in 2017 involved an opioid.
- The CDC reports that in 2017, the number of overdose deaths involving opioids (including prescription opioids and illegal opioids like heroin and illicitly manufactured fentanyl) was 6 times higher than in 1999.
- According to the CDC, on average, 130 Americans die every day from an opioid overdose.

- Evidence suggests that the recent rise in opioid overdose deaths can be attributed to an increase in the use of prescription opioids, heroin, and illicitly-manufactured fentanyl.
- Evidence suggests that more than 191 million opioid prescriptions were dispensed to American patients in 2017.
- Health care professionals should note the most common drugs involved in prescription opioid overdose deaths include: methadone, oxycodone, and hydrocodone.
- Health care professionals should note heroin is an illegal, highly addictive opioid drug; a heroin overdose can cause slow and shallow breathing, coma, and death.
- Evidence suggests the following: between 2010 and 2017, the rate of heroin-related overdose deaths increased by almost 400%.
- Health care professionals should note the following: pharmaceutical fentanyl is a synthetic opioid pain reliever, approved for treating severe pain, typically advanced cancer pain; fentanyl is 50 to 100 times more potent than morphine; fentanyl is prescribed in the form of transdermal patches or lozenges and can be diverted for misuse and abuse.
- Evidence suggests that the most recent cases of fentanyl-related harm, overdose, and death in the U.S. are linked to illegally made fentanyl.
- According to information provided by the CDC, overdose deaths involving synthetic opioids other than methadone, which includes fentanyl, increased by almost 50% from 2016 to 2017; roughly about 30,000 people died from overdoses involving synthetic opioids other than methadone in 2017.
- Evidence suggests that the rise in fentanyl-related deaths may be due to the increased availability of illegally made, non-pharmaceutical fentanyl.
- Health care professionals should note the following: evidence suggests that the best ways to prevent opioid overdose deaths are to improve opioid prescribing, reduce exposure to opioids, prevent misuse, and treat opioid use disorder.
- Health care professionals should be aware of the following signs of an opioid overdose: constricted pupils, loss of consciousness, slow, shallow breathing, choking sounds, limp body, and pale, blue, or cold skin.

- Health care professionals should note that the medication naloxone, an opioid antagonist, may be used for the emergency treatment of a known or suspected opioid overdose.
- Health care professionals should note that naloxone may be used to reverse the life-threatening respiratory depression associated with an opioid overdose.
- Health care professionals should note that a variety of naloxone products (nasal spray, injection, auto-injection) are available to respond to a potential opioid overdose.
- Health care professionals may be called upon to administer naloxone in cases of a known or suspected opioid overdose.

How HIPAA Relates to the Current Opioid Epidemic

As indicated in Figure 1, the current opioid epidemic has lead to an increase in the amount of overdoses in the U.S. Overdoses represent emergency or crisis situations that often require the transmission of vital health-related information, that may include PHI, to various individuals. Thus, it is essential for health care professionals to understand how HIPAA regulations apply to the transmission or sharing of health-related information during a crisis situation like an opioid overdose. Information regarding the application of HIPAA regulations to a crisis situation, like an opioid overdose, may be found below. Health care professionals should keep the following information in mind when administering health care to individuals that may be experiencing an opioid overdose. Such information may guide health care professionals as they attempt to share and disclose vital health-related information relating to a patient potentially experiencing an opioid overdose.

• HIPAA regulations do allow health care professionals to share health-related information with a patient's potential loved ones in emergency or crisis situations.

• HIPAA regulations indicate that health care professionals do have a broad ability to share health-related information with patients' family members during certain crisis situations without violating HIPAA privacy regulations.

• HIPAA allows health care professionals to disclose some health-related information without a patient's permission under certain circumstances, including the following:

    - A health care professional may share health-related information with the family and close friends of patients who are involved in care of the patient, and if the health care professional determines that doing so is in the best interest of an incapacitated or unconscious patient, and the information

shared is directly related to the family or friend’s involvement in the patient’s health care or payment of care.

- A health care professional may inform/potentially provide health-related information to individuals in a position to prevent or lessen a serious and imminent threat to a patient’s health or safety.

- Health care professionals should note the following: HIPAA regulations do respect individual patient autonomy by placing certain limitations on sharing health-related information with family members, friends, and others without the patient’s agreement (patient autonomy is an essential ethic principle of health care, which refers to a patient's right and capacity to think, act and form decisions about themselves and their personal health care; free from external control, influence, or force). Health care professionals should understand that the previous HIPAA regulation note applies to patients with a decision-making capacity (e.g., patients that are not incapacitated or unconscious).
- HIPAA regulations indicate the following: a health care professional must give a patient the opportunity to agree or object to sharing health information with family, friends, and others involved in the individual’s care or payment for care; a health care professional is not permitted to share health information about patients who currently have the capacity to make their own health care decisions, and object to sharing the information, unless there is a serious and imminent threat of harm to health.
- HIPAA regulations acknowledges that a patient’s decision-making capacity may change during the course of treatment. In the context of the health care system, the term decision-making capacity may refer to an individual's ability to formulate their own ideas, judgments and/or choices regarding health care.
- Health care professionals should note the following: a patient's decision-making incapacity may be temporary and situational, and does not have to rise to the level where another decision maker has been or will be appointed by law; if a patient regains the capacity to make health care-related decisions, a health care professional must offer a patient the opportunity to agree or object before any additional sharing of health information occurs.
- Health care professionals should note the following: HIPAA recognizes a patient’s personal representatives according to state law; generally, HIPAA provides a patient’s personal representative the right to request and obtain any information about the patient that the patient could obtain, including a complete medical

record; the term personal representatives may refer to individuals who have health care decision making authority for a patient under state law.

- HIPAA indicates the following: patient's personal representative rights/authority may be established through the parental relationship between a parent or guardian of an un-emancipated minor, or through a written directive, health care power of attorney, appointment of a guardian, a determination of incompetency, or other recognition consistent with state laws to act on behalf of the individual in making health care-related decisions.

Related Patient Privacy Law

- Along with the amount of overdoses in the U.S., the current opioid epidemic has also impacted the prevalence of substance use disorders. A substance use disorder may refer to a medical condition characterized by a cluster of symptoms that do not allow an individual to stop using legal or illegal substances such as: alcohol, marijuana, cocaine, and/or opioids. Due to the potential increase in the prevalence of substance use disorders, U.S. laws, regarding patients' rights, have been recently modified and updated to facilitate substance abuse treatment. One such law is Title 42 of the Code of Federal Regulations, Part 2, otherwise referred to as 42 CFR Part 2. Information regarding 42 CFR Part 2 and its relation to HIPAA as well as substance abuse disorders may be found below.
- The goal of the recent modifications/updates to 42 CFR Part 2 was to encourage individuals to seek substance abuse treatment by removing the potential fear of privacy violations and the subsequent legal and social ramifications that could follow a privacy violation.
- 42 CFR Part 2 heightens the restrictions, even beyond those of HIPAA, on an individual's protected health information related to addiction treatment.
- 42 CFR Part 2 protects the confidentiality of records containing the identity, diagnosis, prognosis, or treatment of any patient maintained in connection with the performance of any federally assisted program or activity relating to substance use disorder education, prevention, training, treatment, rehabilitation, or research.
- 42 CFR Part 2 indicates the following: health care professionals may not disclose information that identifies individuals as having, having had, or referred for a substance use disorder without the patient's consent unless a 42 CFR Part 2 exception applies.
- 42 CFR Part 2 indicates the following: health care professionals may not acknowledge that a person is a patient in a substance use program.

- Health care professionals should note that 42 CFR Part 2 permits the disclosure of health-related information under certain circumstances without consent such as a medical emergency.
- Health care professionals should note that when a disclosure is made in connection with a medical emergency, the 42 CFR Part 2 program must document in the patient's record the name and affiliation of the recipient of the information, the name of the individual making the disclosure, the date and time of the disclosure, and the nature of the emergency.
- 42 CFR Part 2 indicates that individuals may not use 42 CFR Part 2 program information to initiate or substantiate criminal charges against a patient.
- Health care professionals should note that they must limit the disclosure of substance use disorder/ substance use disorder treatment-related information to the minimum amount of information necessary for the permitted purpose of the disclosure.
- 42 CFR Part 2 indicates the following: if a minor patient acting alone has the legal capacity under the applicable state law to apply for and obtain substance use disorder treatment, any written consent for disclosure may be given only by the minor patient.
- 42 CFR Part 2 indicates the following: no person may require any patient to carry in their immediate possession while away from the part 2 program premises any card or other object which would identify the patient as having a substance use disorder.
- 42 CFR Part 2 indicates the following: if a part 2 program discontinues operations or is taken over or acquired by another program, it must remove patient identifying information from its records or destroy its records, including sanitizing any associated hard copy or electronic media, to render the patient identifying information non-retrievable.
- 42 CFR Part 2 indicates the following: 42 CFR Part 2 regulations do not prohibit a part 2 program from giving a patient access to their own records, including the opportunity to inspect and copy any records that the part 2 program maintains about the patient.
- 42 CFR Part 2 indicates the following: if a patient consents to a disclosure of their records, a part 2 program may disclose those records in accordance with that consent to any person or category of persons identified or generally designated in the consent, except that disclosures to central registries and in connection with criminal justice referrals.

- 42 CFR Part 2 indicates the following: patient identifying information may be disclosed to medical personnel to the extent necessary to meet a bona fide medical emergency in which the patient's prior informed consent cannot be obtained.
- 42 CFR Part 2 indicates the following: patient identifying information may be disclosed to medical personnel of the FDA who assert a reason to believe that the health of any individual may be threatened by an error in the manufacture, labeling, or sale of a product under FDA jurisdiction, and that the information will be used for the exclusive purpose of notifying patients or their physicians of potential dangers.
- 42 CFR Part 2 indicates the following: an order authorizing the disclosure of patient records for purposes other than criminal investigation or prosecution may be applied for by any person having a legally recognized interest in the disclosure which is sought.

Section 2: Summary

In recent years HIPAA has undergone a variety of different modifications and updates to help increase its scope and effectiveness in protecting both health-related information and patient rights. With that said, health care professionals should be aware of how the current HIPAA regulations relate to some of the biggest cultural trends impacting today's health care system such as the use of social media and the current opioid epidemic gripping the nation.

One of the biggest cultural trends impacting today's health care system is the use of social media. When using social media, health care professionals should be sure they do not violate HIPAA regulations regarding PHI. Health care professionals can ensure they do not violate HIPAA regulations regarding PHI and social media by adhering to the following related recommendations: health care professionals should always remember that HIPAA regulations prohibit the use of PHI on any form of social media, health care professionals should apply the "When in Doubt Rule" to health-related information and social media, health care professionals should not use patient pictures on social media, health care professionals should not use health-related information about rare diseases or rare injuries on social media, health care professionals should not gossip about patients on social media, health care professionals should consider that information deleted on some social media channels may be saved in some capacity, and health care professionals should consider the repercussions for violating HIPAA regulations before they use health-related information on social media.

Along with health care professionals, health care organizations can also help prevent violations of HIPAA regulations via social media. Recommendations that may be used by health care organization to help prevent violations of HIPAA regulations via social media are as follows: health care organizations should develop policies regarding the use of social media, health care organizations should ensure health care professionals understand internal policies related to social media, health care organizations should educate health care professionals regarding the use of social media, health care organizations should consider including information regarding the use of social media in employee hand books or equivalent materials, health care organizations should not encourage health care professionals to engage with patients via private social media channels, health care organizations should monitor related social media accounts, health care organizations should ensure they have a means to save information used on their social media accounts, health care organizations should encourage health care professionals to report any potential HIPAA violations, and health care organization should have internal channels for HIPAA violation reporting.

Another widespread cultural trend impacting today's health care system is the current opioid epidemic gripping the nation. Health care professionals should posses some insight into the current opioid epidemic as well as how HIPAA, and similar laws which protect patients' rights such as 42 CFR Part 2, relate to the opioid epidemic and the administration of care to those patients in need.

Section 2: Key Concepts

- Two of the biggest cultural trends impacting today's health care system include the use of social media and the current opioid epidemic.
- HIPAA regulations prohibit the use of PHI on any form of social media.
- Health care professionals and health care organizations can help prevent HIPAA violations by following related recommendations.
- The current opioid epidemic has lead to an increase in the amount of overdoses in the United States, while potentially impacting the prevalence of substance use disorders.
- HIPAA works to protect patients' rights while allowing health care professionals the ability to share some health-related information during an emergency/crisis situation such as an opioid overdose.
- Recent modifications/updates have been made to 42 CFR Part 2 to facilitate substance abuse treatment; 42 CFR Part 2 heightens the restrictions, even beyond

those of HIPAA, on an individual's protected health information related to addiction treatment.

Section 2: Key Terms

Social media - any electronically driven application that enables individuals to create and share content for the purposes of virtual communication

Gossip (in the context of this course) - the transmission of messages regarding the personal and/or private details of other individuals' lives, health, overall well-being, quality of life and/or health care

Patient autonomy - an essential ethic principle of health care, which refers to a patient's right and capacity to think, act and form decisions about themselves and their personal health care; free from external control, influence, or force

Decision-making capacity - an individual's ability to formulate their own ideas, judgments and/or choices regarding health care

Substance use disorder - a medical condition characterized by a cluster of symptoms that do not allow an individual to stop using legal or illegal substances such as: alcohol, marijuana, cocaine, and/or opioids

Section 2: Personal Reflection Question

How do current HIPAA regulations relate to the use of social media and the current opioid epidemic?

Case Study: HIPAA

A HIPAA-related case study is presented below to review the concepts found in this course. A case study review will follow the case study. The case study review includes the types of questions health care professionals should ask themselves when considering HIPAA and how it relates to health care and patients' rights. Additionally, reflection questions will be posed, within the case study review, to encourage further internal debate and consideration regarding the presented case study and HIPAA.

Case Study

Jim is a 28-year-old male patient with a history of drug and alcohol abuse. Jim has entered a health care facility for treatment. Upon questioning, Jim reports his battle with drugs and alcohol began in college. While attending college, Jim would often go to parties and/or bars and use drugs or drink excessively. Jim admits he would "black-

out" and wake up in random places and in "strange" women's beds after a "night of drinking." After college, Jim continued to binge drink and use drugs. Jim also admits his "black-outs" continued and he would often "pick up" women while he was out "partying." Jim has tested positive for several sexually transmitted diseases (STDs); however, he continued to engage in unprotected intercourse under the influence of drugs and alcohol. Jim reports he often engages in multiple relationships with different women at the same time and combines binge alcohol drinking, drugs, such as cocaine and opioids, and sex to numb the depression he feels over his past actions. Jim is not sure if he can stop his previously mentioned actions. Additionally, Jim reports he does enjoy himself when he is drinking and doing drugs even if it brings him "depression" later on. With that said, Jim understands he needs to stop his unhealthy lifestyle because his actions are putting his health, and the health of others, in jeopardy. Several days pass and Jim makes positive progress with his drug and alcohol addiction, although he reports he still would like to continue having unprotected sex with multiple partners. As time progresses, Jim continues to inform the team of health care professionals caring for him about his past drinking episodes and drug abuse. One member of Jim's health care team listens very carefully to Jim's reports and picks up several details which peak interest. Several days later, via social media outlets, the health care professional in question discovers that a close friend is romantically linked to Jim. Although the health care professional is not certain of the details regarding the relationship between the close friend and Jim, the health care professional is concerned for the health of both parties. The health care professional would like to leave both the close friend and Jim messages via social media about the potential concerns regarding their relationship and the possibility of STD transmission. The health care professional's concerns mount, however the health care professional is not sure how to proceed.

Case Study Review

What is the potential HIPAA-related dilemma involved in the Case Study?

It appears, the main HIPAA-related dilemma centers around the health care professional's concerns regarding both the patient and a close friend's health as well as the use of PHI, related to addiction/substance use disorder treatment, on social media. Essentially, the health care professional has become aware of PHI which may impact the health and overall well-being of the patient and a close friend, and the health care professional would like to use some of the PHI in question on social media in the form of messages to the patient and the close friend.

Are there any other potential HIPAA-related dilemmas involved in the Case Study; if so, what are they?

What patient details may be relevant to the potential HIPAA-related dilemma highlighted in the Case Study?

The following patient details may be relevant to the HIPAA-related dilemma highlighted in the Case Study: the patient has a history of drug and alcohol abuse, the patient's drug and alcohol abuse appears to be linked with "partying" and intimacy/sex with multiple partners, the patient has tested positive for STDs, the patient continued to engage in unprotected intercourse under the influence of drugs and alcohol after receiving information regarding positive STD status, the patient reports that he would like to continue having unprotected sex with multiple partners, the health care professional in question discovers that a close friend is romantically linked to the patient, the health care professional would like to leave both the close friend and the patient messages via social media about the potential concerns regarding their relationship and the possibility of STD transmission.

Are there any other patient details that may be relevant to the potential HIPAA-related dilemma; if so, what are they?

How are each of the aforementioned patient details relevant to the potential HIPAA-related dilemma?

Each of the previously highlighted patient details may be relevant to the potential HIPAA-related dilemma. The possible relevance of each patient detail may be found below.

The patient has a history of drug and alcohol abuse - the previous patient detail may be potentially relevant because it provides a context for the health care professional's concerns. The previous patient detail may also be relevant because it may represent PHI.

The patient's drug and alcohol abuse appears to be linked with "partying" and intimacy/sex with multiple partners - the previous patient detail may be potentially relevant because it also provides a context for the health care professional's concerns. Additionally, it may form some basis for the health care professional's concerns regarding the patient's health. For example, due to the possible patient link between "partying"/sex with multiple partners and drug and alcohol abuse, the health care professional may be concerned that continued "partying"/sex with multiple partners may lead to further drug and alcohol abuse. Furthermore, the previous patient detail may also be relevant because it may represent PHI.

The patient has tested positive for STDs - the aforementioned patient detail may be relevant because it may form some of the basis for the health care professional's concerns regarding the close friend. Essentially, the health care professional may be

concerned that the close friend was exposed to a STD or may be exposed to a STD in the future (i.e., the health care professional is concerned that the patient may have transmitted a STD to the close friend, or if the potential relationship with the patient and the close friend continues, the close friend's health may be in jeopardy due to the potential for STD transmission). The previous patient detail may also be relevant because it may represent PHI.

The patient continued to engage in unprotected intercourse under the influence of drugs and alcohol after receiving information regarding positive STD status - the previous patient detail may be potentially relevant because it may provide insight into the health care professionals mounting concerns and it may indicate why the health care professional wants to contact the patient and close friend via social media.

The health care professional in question discovers that a close friend is romantically linked to the patient - the aforementioned detail forms a large portion of the basis for the health care professional's concerns. It also serves as a catalyst for the potential HIPAA-related dilemma.

The health care professional would like to leave both the close friend and the patient messages via social media about the potential concerns regarding their relationship and the possibility of STD transmission - the previous detail is related to the overall Case Study and not necessarily, directly, to the patient; however, it is worth consideration because it points to the main HIPAA-related dilemma, which involves the potential use of possible PHI on social media.

What other ways, if any, are the patient details relevant to the potential HIPAA-related dilemma?

Will HIPAA-regulation violation occur if the health care professional leaves both the close friend and the patient messages via social media regarding their relationship and the possibility of STD transmission?

If the health care professional uses PHI on social media, HIPAA regulations may be violated because HIPAA regulations prohibit the use of PHI on any form of social media.

Why do HIPAA regulations prohibit the use of PHI on social media?

How can the health care professional from the Case Study ensure HIPAA regulations are not violated via the use of social media?

The health care professional could ensure HIPAA regulations are not violated via social media by adhering to the following recommendations: health care professionals should always remember that HIPAA regulations prohibit the use of PHI on any form of social media, health care professionals should apply the "When in Doubt Rule" to health-related information and social media, health care professionals should not use patient pictures on social media, health care professionals should not use health-related information about rare diseases or rare injuries on social media, health care professionals should not gossip about patients on social media, health care professionals should consider that information deleted on some social media channels may be saved in some capacity, and health care professionals should consider the repercussions for violating HIPAA regulations before they use health-related information on social media.

What other ways can health care professionals ensure HIPAA regulations are not violated via the use of social media?

How could the health care professional, from the Case Study, resolve the potential HIPAA-related dilemma without using PHI on social media or without violating HIPAA regulations?

The health care professional, from the Case Study, could resolve the potential HIPAA-related dilemma in a variety of different ways or through varying courses of action. One such course of action that may resolve the HIPAA-related dilemma is as follows: the health care professional could attempt to educate both the patient and the close friend, via separate conversations, about the importance of safe sex. Such an attempt could prompt each individual to practice safe sex in order to avoid exposure to STDs. Also, as long as the health care professional does not disclose any PHI, the aforementioned method could prevent a violation of HIPAA regulations.

What other courses of actions, that do not involve using PHI on social media or the violation HIPAA regulations, may be used by the health care professional to resolve the potential HIPAA-related dilemma?

Conclusion

HIPAA may refer to the specific federal regulations or laws which provide provisions for safeguarding medical information. HIPAA was enacted by the 104th United States Congress and signed into action by President Clinton in 1996. Since that time, HIPAA has undergone a variety of different modifications and updates to help increase its scope and effectiveness in protecting health-related information, as well as patients'

rights. Health care professionals should be aware of HIPAA updates to best serve patients. Health care professionals should also be aware of how HIPAA relates to the cultural trends impacting today's health care system such as the use of social media and the current opioid epidemic. Finally, health care professionals should work to protect patients' rights, while avoiding HIPAA violations when administering care to those in need.

References

1. www.hhs.gov
2. www.congress.gov
3. www.cdc.gov
4. www.fda.gov

-

-