IMPLICATIONS OF HIPAA ON PROFESSIONALS WORKING WITH OLDER ADULTS

BY: SAVANNAH GRIGNON, BSW CANDIDATE

OVERVIEW

A major goal of HIPAA is to make sure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being. HIPAA strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing and covers the variety of uses and disclosures that need to be addressed.

BACKGROUND OF THE POLICY

"The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") establishes, for the first time, a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")."

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996.

WHO HAS TO FOLLOW HIPAA GUIDELINES

- Health plans
  - Individual and group plans that provide or pay the cost of medical care
- Health Care Providers**
  - Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions
- Health Care Clearinghouses
  - *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.

For help in determining whether you are covered, use CMS's decision tool:

https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/AreYouaCoveredEntity.html

WHAT INFORMATION IS PROTECTED?

- HIPAA 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. HIPAA calls this information "protected health information (PHI)."

WHAT IS INDIVIDUALLY IDENTIFIABLE INFORMATION?

"Individually identifiable health information" is information that can be used to identify and individual, including:

- Name
- Date of Birth
- Health care provider/payment methods
- Medical history/ current state of health
- Social Security number
- Current residence
- Any thing else that can be used to identify an individual

LETS DISCUSS THIS FURTHER…

- Client's birthday
- Name of client
- Name of client's favorite pet
- Where a client lives
- Where a client went on vacation

DE-IDENTIFIED HEALTH INFORMATION

- There are no restrictions on the use or disclosure of de-identified health information.
- This means that the information would not identify or give someone a reasonable guess, as to the person you are referring to, based on the information given.

EXAMPLE

- 1) Identifiable information: Sharon Andrews, born 2/14/1938 is a 80 year old woman suffering from dementia and schizophrenia. She resides at Rainbow Hills Nursing Home and was reported to the Ombudsman program by Adult Protective Services (APS).

- 2) De-identified information: Client A is 80 years old. She has dementia and schizophrenia and is needing assistance from Ombudsman program.

REQUIRED DISCLOSURES

- Cases where one must disclose identifiable or protected information include
  - (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information; and
  - (b) to HHS when it is undertaking a compliance investigation or review or enforcement action.

PERMITTED USES AND DISCLOSURES

- One is permitted, but not required, to use and disclose protected health information, without an individual's authorization, in certain scenarios, including:
  - (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

*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.

3) 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.

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."

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.[28] 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.

EXAMPLES OF THE 12 NATIONAL PRIORITY PURPOSES

- Victims of Abuse, Neglect, or Domestic Violence
- Health Oversight Activities
  - Audits/investigations etc.
- Serious Threat to Health or Safety
- Law Enforcement Purposes
  - 1) as required by law 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.
  - (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.

DISCUSSION

- Brainstorm scenarios in which you might be asked or required to disclose otherwise confidential information during your involvement with this program
- In those scenarios, would the disclosure of information be permitted under HIPAA?
- If not, how would you respond to the individual asking for information?

EXAMPLES: TO DISCLOSE OR NOT TO DISCLOSE

- Mary Wright is your elderly client. She confides in you that another care provider hit her in the head during her assisted shower.
- Clifford Jackson, a former client, passed away under questionable circumstances after he was transitioned into a nursing home. One day, a detective knocks on your door and asks you to provide personal information about your experience with Clifford as a client.
- Hilda Richards is a client. One day, a family member of Hilda's contacts you and asks where Hilda has been living, because they have not heard from her and are worried about her safety.

IMPLICATIONS FOR SOCIAL MEDIA

- Social Media is used by 74% of internet users.
- Social media can be a powerful tool for communication between professionals and the public. However, it also creates a vast possibility of HIPAA violations.
- With over 800 million people on social networks, it is not surprising that HIPAA violations are a growing societal trend.

EXAMPLES OF HIPAA VIOLATIONS ON SOCIAL MEDIA

- Posting verbal "gossip" about a patient, even when the name is not disclosed
- Sharing photographs of patients without their written consent
- Sharing seemingly innocent comments or pictures, such as a workplace lunch which happens to have visible patient files underneath

EXAMPLES OF THINGS YOU CAN POST

- Health tips that people might find useful
- Upcoming events that people might like to attend
- Honors or awards your organization has been granted
- Advertisements of your services, as long as it does not contain any PHI

CONCLUSION

- In one word, how would you describe the HIPAA policy?
- Do you feel competent in your knowledge of what is considered identifiable information and when to share it?
- Are there any other questions that you have that would help clarify these concepts better for you?

REFERENCES

Posting with Caution: The DO's and DON'Ts of Social Media and HIPAA Compliance. (2018, February 14). Retrieved March 13, 2018, from http://www.healthcarecompliancepros.com/blog/posting-with-caution-the-dos-and-donts-of-social-media-and-hipaa-compliance-2/

Secretary, H. O., & (OCR), O. F. (2013, July 26). Summary of the HIPAA Privacy Rule. Retrieved February 19, 2018, from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Sivilli, F. (2017, November 10). HIPAA and Social Media | HIPAA Social Media Guidelines. Retrieved March 13, 2018, from https://compliancy-group.com/hipaa-and-social-media/