NATIONAL ADULT PROTECTIVE SERVICES ASSOCIATION

THE NATIONAL APS RESOURCE CENTER

Technical Assistance Brief

Health Insurance Portability and Accountability Act: Implications for Adult Protective Services

Candace Heisler, JD

NAPSRC Consultant

The National Adult Protective Services Resource Center (NAPSRC) provides monthly Technical Assistance (TA) calls on subjects requested by the field. Our team of adult protective services (APS) experts provides this national TA to state APS administrators. This brief summarizes the information provided during the January 2015 call.

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted to protect the confidentiality of health records and information. The Office for Civil Rights in the United States Department of Health and Human Services is responsible for developing the rules, many of which are contained in the HIPAA "Privacy Rule." (45 CFR 164.500 et seq.)

HIPAA and its Privacy Rule give "covered entities" (those with the health care data) discretion to comply with requests for release of protected health records, while attempting to balance patient privacy and confidentiality with those with a need to know the content of such records. HIPAA is intended to "*assure 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. The Rule strikes a balance that permits important uses of information, while protecting the privacy of people who seek care and healing.*" (Office for Civil Rights, 2003, p. 3).

HIPAA's complexity can lead to conflict between entities that hold confidential health records and agencies such as Adult Protective Services and law enforcement that investigate allegations of abuse.

About the National Adult Protective Services Resource Center (NAPSRC)

The National Adult Protective Services Resource Center (NAPSRC) is a project (No. 90ER0003) of the Administration for Community Living, U.S. Administration on Aging, U.S. Department of Health and Human Services (DHHS), administered by the National Adult Protective Services Association (NAPSA). Grantees carrying out projects under government sponsorship are encouraged to express freely their findings and conclusions. Therefore, points of view or opinions do not necessarily represent official Administration on Aging or DHHS policy.

HIPAA protects individually identifiable health information held or transmitted electronically by a covered entity or its business associate, in any form or media, whether electronic, written, or oral. It requires that covered entities protect such information, and except for certain exceptions, requires that if and when a covered entity releases protected health information the entity must notify the patient whose information was released.

Violations of HIPAA rules are subject to civil and criminal penalties. (42 U.S.C. §§1320d-5 and 1320d-6). Actions may be brought by federal and state Attorneys General. For more information refer to the Health and Human Services Health Information Privacy page.

Key Definitions under HIPAA

HIPAA applies to health plans, health care clearinghouses, and all health providers that transmit records in electronic form, whether the provider itself transmits that information or uses a billing service or subcontractor to do so.

In order to understand the Privacy Rule, it is critical to understand the terminology and definitions within HIPAA. Key terms include the following (See 45 CFR 160.103):

- **Protected Health Information** (PHI) is all "*individually identifiable health information held or transmitted by a covered entity or its business associates in any form or media, whether electronic, paper, or oral.*"

  "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. This information includes many common identifiers (e.g., name, address, birth date, Social Security Number). (Office for Civil Rights, 2003, at pp 5-6).

- **Covered Entities** include health plans, health care clearinghouses, and health care providers.
  - ***Health Plans*** include providers of medical services and entities that pay for the services, including nearly all individual and group plans that provide or pay the cost of medical, dental, and/or vision services, or prescription drugs, as well as HMOs, Medicare and Medicaid insurers, and long term care insurers (other than nursing home fixed indemnity policies).
  - ***Health Care Providers*** include "*a provider of services, a provider of medical or health services, and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business,*" and who transmits health information in electronic form.
  - ***Health Care Clearinghouses*** process or assist in processing health information received form another entity, including billing and repricing companies. They are included in the Privacy Rule only when using and/or disclosing identifiable health information.

Is APS a "Covered Entity"?

Careful thought should be given to whether there are any circumstances in which an APS agency could be considered a covered entity.

Given the array of actions undertaken by APS, careful thought should be given to whether there are any circumstances in which an APS agency could be considered a covered entity. For example, does APS employ health professionals, and if so, for what purposes? Do they review medical records, conduct medical or cognitive assessments, or treat client medical conditions? How do they record their findings? Are their services billed and if so, to what entity?

There is no simple answer to this determination. APS managers should review the role of such employees with their legal advisors for clarification. If deemed a covered entity, APS is subject to many standards and requirements.

The Privacy Rule

A "covered entity" may not use or disclose protected health information (PHI) except in accordance with the Privacy Rule and/or as authorized in writing by the individual whose information is used or disclosed. (45 CFR 164.502(a)). The Privacy Rule requires that a Covered entity disclose PHI in two situations:

- To the United States Department of Health and Human Services (HHS) when HHS is conducting a compliance investigation or review or enforcement action; and
- To the individual or their personal representative when they request access to or an accounting of disclosures of their PHI (45 CFR 164.508).

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 (45 CFR 164.508).

Authorizations must be in plain language and contain specific information about the information to be disclosed or used, the person or persons disclosing and receiving the PHI, expiration, right to revoke, and other data. The person giving consent is entitled to a copy of the authorization form. (45 CFR 164.508).

The easiest way for APS to obtain PHI is with client informed consent. To do so requires that the individual be capable of giving legal consent and have decision-making capacity. If an individual has a surrogate decision-maker (such as an agent or attorney-in-fact under a power of attorney for health care decisions or a guardian or conservator with similar authority) that person can give consent for a client who lacks capacity to consent.

Situations in which the duty to provide access and accountings of disclosures does not apply include:

- **When a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is likely to endanger the life or physical safety of the individual or another person;**
- **The PHI makes reference to another person other than a health care provider, and the access requested is reasonably likely to cause substantial harm to such person; or**
- **The request for access is made by the individual's personal representative and providing such access to the personal representative is reasonably likely to cause substantial harm to the individual or another person (45 CFR 164.524).**

If there is a doubt about the client's capacity to consent APS should not seek the client's consent. Not only is relying on consent in such circumstances improper, it may undermine a civil law action or criminal prosecution.

HIPAA requires that the covered entity treat an individual's personal representative the same as the entity would treat the individual as to access to, and accountings about, release(s) of PHI. A personal representative is defined as a person legally authorized to make health care decisions for the individual or to act on behalf of the decedent or estate. *"The Privacy Rule permits an exception when a covered entity has a reasonable belief that the personal representative may be abusing or neglecting the individual or that treating the person as the personal representative could otherwise endanger the individual" (*Office for Civil Rights 2003, p. 16).

Situations in which the duty to provide access and accountings of disclosures does not apply include:

- When a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is likely to endanger the life or physical safety of the individual or another person;
- The PHI makes reference to another person other than a health care provider, and the access requested is reasonably likely to cause substantial harm to such person; or
- The request for access is made by the individual's personal representative and providing such access to the personal representative is reasonably likely to cause substantial harm to the individual or another person (45 CFR 164.524).

The person denied access has a right to have the denial reviewed by a licensed health professional who is designated by the covered entity and did not participate in the initial denial decision.

If APS is conducting an investigation that identifies an alleged perpetrator who is also the individual's personal representative, APS may want to consider if they should share concerns about release of PHI to that personal representative. APS cannot make the decision to grant or deny access for the covered entity but can provide important information that may assist the entity in deciding how to proceed with requests for release of PHI.

A covered entity is permitted but not required to disclose PHI without providing the individual an opportunity to agree or object for the covered entity's own treatment, payment, and health care operations. However, virtually any use and/or disclosure of psychotherapy notes for treatment, payment, and health care operations requires the individual's authorization (45 CFR 164.508(a)(2)).

Finally, a covered entity must make reasonable efforts to limit disclosures to the *minimum* amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request (45 CFR 164.502(b); 164.514(d)). An entire medical record cannot be provided unless it is the minimum necessary to accomplish the purpose of the request.

The minimum necessary standard **does not** apply to several situations including:

- Disclosure to the individual who is the subject of the information or their personal representative
- Use or disclosure subject to authorization (e.g., court order, subpoena, or search warrant)
- Use or disclosure is required by law (45 CFR 164.512(a); 45 CFR 164.502(b)(2)(v)), (e.g., mandatory elder or vulnerable adult reporting law, duty to warn situations).

  Although the minimum necessary standard may not be applicable to an APS request for PHI, covered entities may nevertheless attempt to limit disclosures to the minimum necessary in the "spirit and purpose of HIPAA" and may be unaware that APS may be exempted from minimum necessary requirements.

Psychotherapy Notes

"Psychotherapy notes" are treated differently from other mental health information and afforded special privacy protections because of their sensitive content. Such notes are recorded by a mental health professional providing health care that document or analyze conversations during counseling sessions and are separate from the rest of the patient's medical record. (45 CFR 164.501).

A covered entity must obtain a patient's authorization prior to a disclosure of psychotherapy notes except when disclosures are required by law such as mandatory reporting of abuse and duty to warn situations. A general consent for release of all health care or medical records is not sufficient for disclosure of psychotherapy notes. It is suggested that authorization for disclosure of PHI (medical records) should be on a separate form from authorization for disclosure of psychotherapy records. (45 CFR 164.508(a)(2). More information is available at *HIPAA Privacy Rule and Sharing Information Related to Mental Health* and *HIPAA Privacy Rule*.

Mental health clinicians generally prefer to converse with other professionals seeking information regarding psychotherapy notes (including investigating APS workers) to answer specific questions rather than turn over copies of notes. The APS worker will still need written authorization from the client to obtain this information. That conversation may in fact be more helpful than the notes themselves. If such notes become relevant in a court matter they can be subpoenaed.

A general consent for release of all health care or medical records is not sufficient for disclosure of psychotherapy notes. It is suggested that authorization for disclosure of PHI (medical records) should be on a separate form from authorization for disclosure of psychotherapy records.

Disclosures: How APS Obtains PHI

The Privacy Rule permits use and disclosure of PHI without an individual's authorization or consent for 12 national priority purposes (45 CFR 164.512). These are permitted disclosures "*in recognition of the important uses made of health information outside of the health care context*"; they are not mandated (Office

for Civil Rights, 2003, at p. 6). Those most relevant to APS practice are:

- Required by Law
- Victims of Abuse, Neglect, or Domestic Violence
- Judicial and Administrative Hearings
- Serious Threat to Health or Safety

"Required by law": covered entities may use and disclose PHI without the individual's consent when there is a relevant statute, regulation, or court order. (45 CFR 164.512 (a)).

"Victims of Abuse, Neglect, or Domestic Violence": covered entities may use and disclose PHI to appropriate governmental agencies regarding such victims. These include situations in which there is mandatory reporting of child, elder or vulnerable adult abuse or domestic violence, as well as situations in which persons must report violent crime victimizations or the duty to warn (protect) of a credible threat directed to or at an identifiable target. (See, e.g., Tarasoff v. Regents of the University of California (1976) 17 Cal. 3d 425, 131 Cal. Rptr. 14, 551 P.2d 334)(45 CFR 164.512(c)(1)(i)).

The duty to warn/protect authorizes a covered entity to disclose PHI, including information from mental health records. The Privacy Rule permits a provider who has a good faith belief that a warning is necessary to prevent or lessen a serious and imminent threat to the health or safety of the patient or others, to alert persons reasonably believed to be able to prevent or lessen the threat (45 CFR 164.512(j)). The client is entitled to notice. (45 CFR 164.512(c)(2); 164.512 (c) (1) (ii)(B)). For more information, please refer to the HHS Health Information Privacy page.

Judicial and Administrative Proceedings: Covered entities may disclose PHI in such a proceeding when the request for PHI is through a court or administrative tribunal order, a subpoena, or other lawful process (45 CFR 164.512(f)(1)(ii)(A)-(B)-(C)). If APS cannot obtain PHI by request, it may need to seek a court or administrative order.

Serious Threat to Health or Safety: Covered entities may disclose PHI when necessary to limit/prevent a serious and imminent threat to a person or the public, to an entity able to address the threat, or to apprehend an escapee or violent criminal. (45 CFR 164.512(j)).

Application to APS Practice

HIPAA permits, but does not require, covered entities to comply with requests for PHI. A covered entity may violate a state law about disclosure of PHI disclosure without violating HIPAA. Therefore, APS officials must know the precise statutory requirements under which APS has authority to seek PHI.

APS should always seek written consent from a client to obtain PHI if that client's capacity to understand and grant informed consent is not in question. If there is a concern about the client's capacity then APS should seek assistance from appropriate experts to assess the client's capacity. If the client clearly cannot give informed consent, a personal representative who is not suspected of abuse, neglect or exploitation can give informed consent on behalf of the client. If there is no appropriate representative, APS can seek the appointment of a representative such as a temporary guardian or conservator or a guardian ad litem, depending on local statutes.

APS workers seeking client consent for disclosure of PHI are urged to assure that:

- the client understands that you, the APS worker, will request disclosure and use of the client's PHI held by the covered entity,
- the client understands the nature of the information being sought,
- the client understands the included time frame (previous date to present or a specific ending date),
- the client has the right to revoke the authorization in writing at any time (45 CFR 164.508; 164.532).

Of course, the APS worker must also insure that the client is informed and understands that he or she has the right to deny access to PHI.

APS should assure that authorizations:

- are written in plain language and large font,
- specifically describe the information to be disclosed and used,
- provide the identity of persons disclosing and receiving the PHI,
- include the date the authorization expires, and
- inform the client of the right to revoke their informed consent (45 CFR 164.508).

It is suggested that forms be translated into languages commonly used in the community other than English.

APS managers may want to review existing authorization forms and assure that they comply with HIPAA legal requirements.

APS requests for PHI should describe what is sought in clear terms. Avoid open-ended and generic requests that may be interpreted as a request for the entire record unless that is actually required. An example of a specific request is: *"all records of medical treatment, nursing notes, consultations, prescriptions, and diagnosis for Mary Jones, DOB, medical record number, relating to her treatment for trauma (or neglect or suspected abuse) for the period XX to YY"*.

The presence of a legal basis for seeking records under a state law, regulation, or court order does not mean that APS will receive what it has requested. A covered entity may be justifiably concerned about providing too much information and running afoul of HIPAA. APS can enhance its success in obtaining medical information by more precisely defining what it seeks, limiting requests to specific events and dates, and obtaining written authorization from the client or the client's legal representative.

Building strong and positive relationships with covered entities and assuring that they understand the role and legal authority of APS is critical to minimizing conflict and assuring maximum compliance with requests for records. APS can request additional or other PHI at later points in their investigation. A covered entity may continue to disclose to governmental authorities throughout the duration of an investigation (45 CFR 164.512 (b); (c); Campanelli, 2004).

If APS requests are not subject to the "minimum necessary" rule, the request for PHI should clearly state so. It is suggested that the request describe how the request is authorized by law by referencing applicable statutes or regulations.

Language such as *"This is a disclosure required by law, specifically: (name of law and statute number/reference), and is therefore not subject to the minimum necessary requirement"* may be helpful. In addition, consider attaching a copy of the law to the request if there are concerns about compliance.

In addition the request for disclosure should include the following language: *"The information sought is relevant and material, specific, and limited in scope, and de-identifiable information cannot be used."* (See 45 CFR 164.512(f)(1)(ii)(C).) APS management may want to have legal counsel prepare a form with legal and helpful information to use for such requests for disclosure.

Once APS has received PHI it must treat records as confidential and not disclose them without legal or statutory authority, and only to those authorized to receive them. APS management should assure that policies are in place describing how the confidential nature of PHI will be protected.

State vs. Federal Laws

In general state laws contrary to HIPAA and its Privacy Rule are pre-empted by federal law. "Contrary to federal law" means that it would be impossible for a covered entity to comply with both state and federal requirements, or

that the state law is an obstacle to accomplishing the purpose and objectives of HIPAA. (Office for Civil Rights, 2003 at p. 17). The Privacy Rule provides exceptions to the general rule of federal preemption for state laws that:

- Relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such PHI
- Provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention… (Office for Civil Rights, 2003 at p. 17; 45 CFR 160.202 and 203).

There is no conflict between elder and vulnerable adult reporting laws and HIPAA. When state or other law authorizes such reports be made to APS and directs that APS conduct investigations which include obtaining medical and other health records subject to HIPAA, a covered entity can comply with the state or other requirement and comply with HIPAA.

In light of this guidance there is no conflict between elder and vulnerable adult reporting laws and HIPAA. When state or other law authorizes such reports be made to APS and directs that APS conduct investigations which include obtaining medical and other health records subject to HIPAA, a covered entity can comply with the state or other requirement and comply with HIPAA.

One example of where there could be seeming conflict between the Privacy Rule and state reporting laws concerns disclosure of the identity of the reporter to APS. State laws typically require that the name of the reporter be kept confidential and not disclosed except under specific circumstances such as consent of the reporter or pursuant to a court order or to rules of criminal discovery if a case is criminally prosecuted. (See, e.g., MN Stats. 626.557, subd. 12b).

HIPAA authorizes an individual or their personal representative to receive an accounting of disclosures which would likely include the identity of the reporter. (See 45 CFR 164.502(g) and 164.528(a)). Can these apparent conflicts be resolved?

The answer is *"yes."* The Privacy Rule permits a covered entity to refrain from telling an individual or their personal representative that a report to APS has been made if the notification would place the individual at risk of serious harm or would not be in their best interest. A covered entity can decline to provide an accounting to a personal representative if it reasonably believes that the representative is an abuser or that providing the accounting could endanger the individual. (45 CFR 164.502(g)(5)). Additionally, the covered entity can suspend an accounting for a period of time when the disclosure is to law enforcement or a health oversight entity for whatever period is specified by the agency if the accounting is reasonably likely to impede the agency's efforts (45 CFR 164.528(a)(2)). Finally, the Privacy Rule does not actually require that the covered entity release the name of the reporter. Instead, the covered entity can limit its accounting to the date of disclosure, the recipient of the information, the purpose of the disclosure, and a brief description of the information disclosed (Campenelli, 2004, p. 3).

Conclusion

HIPAA is complex and APS should exercise caution when obtaining client informed consent, requesting PHI, and maintaining the confidentiality of records once received from a covered entity.

It is suggested that APS agencies have clear policies and protocols for compliance with HIPAA and relevant state laws and regulations and that staff receive training on the Privacy Rule, state laws, and policies and protocols. The better these requirements are understood and applied, the better staff will be equipped to work effectively with clients, covered entities, courts, and allied professionals.

Let us know what you think of this brief. Please take a quick six question survey.

Citations

Campanelli, R.M. (2004) "Letter to Ms. Joyce Young," Department of Health and Human Services, Office for Civil Rights, available at http://www.centeronelderabuse.org/docs/HIPAAGIVES.pdf

Office for Civil Rights (May, 2003) "Summary of the HIPAA Privacy Rule", OCR Privacy Brief, United States Department of Health and Human Services, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

HIPAA-Related References

HIPAA Combined Statute, available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/combined/index.html

"When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials?" FAQs , retrieved July 1, 2015, from http://www.hhs.gov/ocr/privacy/hipaa/faq/disclosures_for_law_enforcement_purposes/505.html.

HIPAA Privacy Rule and Sharing Information Related to Mental Health, retrieved July 1, 2015 from http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html

HIPAA Privacy Rule, retrieved July 1, 2015 from www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.htm

HIPAA Privacy Rule and "State Attorneys General" retrieved July 1, 2015 from http://www.hhs.gov/ocr/privacy/hipaa/enforcement/sag/index.html.

About the Author

Candace J. Heisler served as an Assistant District Attorney for the City and County of San Francisco for over 25 years. During her career, she headed the Domestic Violence, Charging, Misdemeanor, and Preliminary Hearing Units. She served as the Chairperson of the California District Attorneys Association Domestic Violence Committee. She has planned and presented training for that organization for approximately 20 years in the areas of Domestic Violence and Elder Abuse.

Ms. Heisler has edited four judicial and curricula and a prosecutors' manual on Domestic Violence. She helped develop curricula on elder abuse for judges, prosecutors, and victim advocates for the Office on Violence Against Women, US Department of Justice, the American Bar Association and the California Administrative Office of the Courts. She has authored numerous articles on Domestic Violence and Elder Abuse, including several in the Journal of Elder Abuse and Neglect. She co-authored Elder Abuse Detection and Intervention: A Collaborative Approach and wrote a chapter on "Elder Abuse" in the book Victims of Crime. She has participated in developing numerous distance learning courses and training courses for California law enforcement. She provides law enforcement training on Domestic Violence for recruits, first responders, and investigators in California. She also trains probation officers, emergency dispatchers, and victim advocates about elder abuse and domestic violence.

Ms. Heisler served as a member of the California Violence Against Women Act Stop Task Force and as an officer and board member of The National Committee for the Prevention of Elder Abuse for many years, and was a member of the Texas Medical Association Blue Ribbon Panel on Family Violence.

Ms. Heisler has received numerous awards to include the California Governor's Victim Services Award, the California Crime Victims United "Prosecutor of the Year" Award, and the National College of District Attorneys presented her with its Lecturer of Merit (2001) and its Distinguished Faculty Awards (2007).

She has presented on elder abuse and domestic violence subjects throughout the United States. She is also an Assistant Adjunct Professor of Law at the University of California's Hastings College. She now teaches for and consults with a wide variety of state, local, and national governmental agencies as well as private organizations.