Questions from HIPAA Teleconference

Please note that the following is provided as adjunct to an educational program provided by CTAAP on March 2, 2011. This is not legal advice, and should not substitute for legal advice. Please consult your own legal counsel if you have specific questions or concerns about legal compliance.

Section 1: Updating Existing Policies.

We received several requests for updates to existing HIPAA policies, as well as for forms and templates for communicating with business associates. There are no materials available at this time. However, CTAAP is considering creating an update to previously distributed HIPAA materials that would include BAA forms. We first need to assess member interest (because some cost will be involved), and more importantly, we would not be able to create these documents until the final HIPAA rules are released by HHS (the date for this is still unknown).

In the meanwhile, with respect to business associates, be sure you have a written agreement already in place (you should already have these, since this has been the rule since 2003). A good practice would be to write a short letter or email to each of your business associate explaining that some HIPAA changes are in place (for example, breach reporting rules), and more changes are imminent. You should direct them to the OCR website for further information: http://www.hhs.gov/ocr/privacy/.

Section 2: Minors.

We received numerous questions about minors' records, focused who has authority to release the record (minors or parents) and how these rules interact with HIPAA.

Interestingly, HIPAA does not determine whether a minor or parent has rights to see or release records. You are required to follow state law and ethical standards when deciding. The answer will vary depending on many factors, such as patient age, the type of care, and whether the practitioner has offered confidentiality to the minor as part of the course of treatment.

Because minors rights are not a HIPAA issue, this FAQ does not address minors, but we invite and encourage you to refer back to prior seminar materials available at:

Ct-aap.org

- Look under teleconferences 2009

- Look for a September 2009 and then an April 2009 teleconference. Both of these program addressed adolescent confidentiality issues.

You may wish to consider purchasing a very comprehensive guide on adolescent healthcare rights in Connecticut, using the following link:

http://www.kidscounsel.org/order_publications_adolescent-health-care.htm

Section 3: Q&A: This section addresses questions that we received that do not fall into Section 1 or 2 above.

- Question: Jennifer mentioned that it is not advisable to take copies of drivers' licenses. Does that mean we should not ask to see one? Should we be asking for photo ID's?

    - Answer: Currently, you are permitted to ask for, and copy to your file, a driver's license. However, there is legislative activity in Connecticut to end this practice in the future. The legislature has until the end of its working year (June) to decide whether to prohibit you from making a copy of a license.

- Question: If we look at a driver's license to identify a patient's parents, is it okay to ask to look at the license and then not keep a copy in the file?

    - Answer: You may request to see a license. A request to view photo identification is a good practice in preventing identity theft and verifying identity generally.

- Question: We attended a webinar on HIPAA and we were told not to scan patients' licenses into our computers and not to have their Social Security numbers, have you hear anything about this? It is important because our collection agency really needs SSN to track patients effectively.

    - Answer: The trend is to move away from social security numbers in charts -- even though there is currently no effective substitute, particularly for payment and collections. Many EMR vendors and consultants are advising providers to stop collecting SSNs now, because these data will be very hard to extract from systems later if the rules change.

    - Additionally, as part of the trend, federal law states that a patient is not required to give a social security number out to a provider if they choose not

to. (Note: there is no useful explanation of how this works when the SSN is the patient's Medicare number.)

- Question: Credit checks on patients will trigger Red Flags rules, as discussed during the program. Does that include credit checks by our collection agency (who is our BA), or are we exempt from Red Flags because the check is performed by our BA?

    - Answer: Businesses that "use" credit reports "directly or indirectly" have typically been included under Red Flags. The AMA and other medical trade associations are hopeful that the upcoming guidance expected soon from the Federal Trade Commission will exempt a practice if the only use of credit reporting is by a vendor. But we cannot be sure until the final guidance is published.

- Question: Our web designer uses e-mail addresses that patients provided to us. Would HIPAA regulations cover his use of these e-mail addresses, if these addresses were somehow lost or misplaced?

    - Answer: E-mail addresses are a type of protected health information (PHI). If they were lost or stolen it could be a HIPAA Privacy violation. You should have a business associate agreement with any vendor with whom you share email addresses.

- Question: Please explain what is necessary to have in place to protect e-mail communications about patients with regard to the HIPAA rules? Can e-mails be used between patient and doctor or between treating doctors?

    - Answer: You are required to comply with the HIPAA Security rules, which indicate that email "over the internet" that is not protected by encryption, a VPN, or similar protection may lead to a HIPAA Privacy violation. E-mail "over the internet" is not considered secure.

- Question: Is the no e-mailing information over the regular internet effective now?

    - Answer: E-mailing over the internet, without other security provisions, is not considered secure, and could lead to a HIPAA Privacy or HIPAA Security violation.

- Question: A lawyer sends an authorization for a full health record to our office. We respond and ask exactly which documents he is requesting. He responds that

he wants everything. Do we have to send the entire record? We feel that does not meet the minimum necessary standard.

- Answer: If the attorney has provided a valid authorization for the entire record, you are required to provide the entire record. Disclosures made in response to a valid authorization are exempt from the minimum necessary standard.

- Question: A physician works at two different facilities. The first facility the MD owns and he is a contract employee at the second facility. An attorney sends a request for medical information to the facility that the MD owns for patient information on a patient who the MD saw at the facility where he is a contract employee. Do we have to get another authorization for the other site?

  - Answer: An authorization is directed to the provider entity that maintains the record set being requested. Generally, if a practitioner works in two different settings, the patient most likely has two different charts. Each setting would need a separate authorization before release. There are many nuances to this. For example, a hospital chart may have notes from a physician's office record in the chart. The hospital is permitted to release these in response to an authorization directed to the hospital, even though some records also exist in another file at the practice, and were not original to the hospital chart.

- Question: In the evolving enterprise systems for EMR between practices and hospitals or hospital systems, who is responsible for HIPAA information as others enter the information portal that has information you have put in?

  - Answer: The entity that maintains the record (officially) is responsible for HIPAA compliance, and anyone using the system will be obligated to follow the rules or policies for use of the system. However, HIPAA does not address the question of accuracy of the providers input of information, beyond assuring the integrity of the physical record. Liability for incorrect information entered into a chart or system is governed by a variety of sources, including: the medical standard of care, state and federal regulations and general malpractice risk assessment.

- Question: If a patient hasn't been seen in the office for seven years, we can shred their records. We save immunization records in a separate file because that we receive many requests for immunization information from patients that we haven't seen in many years. In the presentation, Attorney Cox said after 50 years we can make paper airplanes from a deceased person's file. Does this mean that first of all

we don't have to shred them and that second of all it only applies to records of deceased patients?

- Answer: The 50-year rule proposed by the federal government has not yet been adopted, and is still in the comment phase. If it becomes a HIPAA rule, HIPAA will no longer penalize you for anything you do with that record -- including making a paper airplane out of the records. But, current Connecticut laws would still require these records to be properly destroyed.

- Question: Please remind me of the HIPAA regulation about patient registration at the front desk. For example, if a patient signed in, writing her name after other names on a list at register for blood draws.

  - Answer: You are permitted by HIPAA to keep a sign-in sheet with full names, as long as there is no condition specific information (or other unnecessary PHI such as address or phone number) on the sheet -- meaning it is okay to use just full names. You should be willing and able to accommodate a patient who does not wish to use their name on the sign-in sheet through some alternative process.

- Question: DDS (Social Security Disability Office) wants medical records sent by fax. What do you think about to sending records by fax?

  - Answer: Faxing is permitted by HIPAA, as long as you are very careful about the numbers dialed, and who is at the other end. It is good practice to confirm numbers that will be dialed, and after sending, confirm receipt on the other end.

- Question: If a patient asks to "hide" some information from the insurance company, isn't this falsifying records to a degree? For example what if an insurance company wants to see if a condition is pre-existing?

  - Answer: HIPAA's new restriction rule seems to run counter to many well-established principles of transparency in medical billing. However, the federal government has decided the patient should have the right to restrict this information. Keep in mind the restriction is only for information to a health plan, and only if the patient has agreed to (and does) pay you out of pocket at the time of service. More detail is expected on how to handle this process when HHS publishes a final rule for this restriction, including whether government plans (e.g., Medicaid, Medicare, etc,) will be exempt from the rule.

- Question: School CHRs are transported by school mail and by US postal mail to other schools. What if the records get lost during this transportation process?

    - Answer: Transport of medical records is permitted through carriers and messengers, including the post office, without a business associate arrangement (assuming the records are closed from the view of the carrier). However, if records are known to be lost during transit (regardless of fault), a review of the situation for a possible breach report is required.

- Question: What is your opinion about keeping credit card information on file in your EHR?

    - Answer: Credit card or other payment information may be kept in a patient's file, paper or electronic. Theoretically, it is just as protected, and just as sensitive, as any other PHI you have. In reality, it is more sensitive because it can be used for identity theft and direct theft. If you do not need it, you may consider not retaining it. If you keep it -- be very careful with it.

- Question: Explain the restrictions psychotherapists need to follow in communicating treatment plans with PCPs under HIPAA.

    - Answer: Be very careful to apply the psychotherapy note rule only to true psychotherapy notes, as defined by HIPAA. The definition does not include many other types of entries about a patient or counseling session, and does not encompass all mental and behavioral health records. HIPAA Privacy defines psychotherapy notes as:

      "Notes recorded in any medium by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session that are separate from the rest of the individual's medical record. Psychotherapy notes **exclude** medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date."

    - Psychotherapy notes must:
        - Be kept physically separate from all other records.
        - Only be released with a stand-alone, psychotherapy note authorization (a general authorization may not be used for disclosure), even to other providers

- Question: Is there a website that has the Connecticut state laws regarding HIPAA?

    - Answer: Unfortunately, there is no official or highly reliable source for HIPAA as it relates to state law.

- Question: Will all seminar participants be certified for HIPAA training?

    - Answer: If you participated in this program and completed an evaluation form, CTAAP will provide a letter to you that indicates you have attended the training on the HITECH changes to HIPAA Privacy. We suggest you keep that with your HIPAA administrative materials.

- Question: Several abbreviations were used in the program. Please indicate to what they refer:
    - Answer:
        - FTC = Federal Trade Commission
        - HHS = federal Department of Health and Human Services
        - DOJ = federal Department of Justice
        - CE = Covered Entity
        - OCR = Office of Civil Rights (which enforces HIPAA)
        - AG = Attorney General (state level)

- Question: I have a question regarding HIPAA and state confidentiality for patients under 18 years of age and parental request for a patient's records. Can an office policy be more restrictive than what the State/HIPAA laws state?

    - Answer: While we refer you to the prior seminar materials for issues of who controls access to a minors record, as to the specific HIPAA aspect of this: you may not restrict access to a person if he or she has a HIPAA given right to see the record.

- Question: Do privacy policies have to be updated every year and given to patients? Or do they just sign one time that they have received a copy of the policies?

    - Answer: The Notice of Privacy Practices (NOPP) that patients acknowledge during their first encounter needs to be acknowledged only once, even if changes are made to it. It would be a good practice to tell patients if it has changed, perhaps by posting an announcement on the wall-affixed copy at the

registration area. You must always provide patients with a paper copy of your NOPP if they request it.

- Question: Do the HIPAA rules apply to city run immunizations programs when they are physically picking up or e-mailing patient information from hospitals and practices?

  - Answer: HIPAA applies to the hospital or practice providing the information, but it probably does not apply to the city or its public health director, which are likely acting as a "public health authority" when collecting immunization data. HIPAA allows a public health authority, including the state's vaccination and immunization programs, broad exemptions from most HIPAA rules. It is optimal to obtain the agency's agreement (preferably in writing) that it is acting in the role of public health authority in accessing the PHI. You are permitted to rely in the agency's good faith instructions to you when disclosing PHI.