Public Comment for the November 17 meeting of the Health IT Advisory Council

HIPAA calls for only the minimum amount of patient information needed for a query to be exchanged as referenced in the State Medicaid letter sent by HHS. Footnote 8 on page 9 of the letter is a web link to the privacy rules of HIPAA that describes the "uses and disclosures that are permitted under HIPAA." The web links are: https://www.healthit.gov/sites/default/files/exchange_health_care_ops.pdf and https://www.healthit.gov/sites/default/files/exchange_treatment.pdf). In addition, the documents are enclosed.

It seems that the technology of any exchange must have that capability to target just certain parts of the whole patient medical record to share, but it is doubtful that current hospital and provider systems are able to remove just portions of a past medical history or a medication list to do so. Also, as per 45 CFR 164.501 referenced by footnote 8, "In general, before a CE (covered entity) can share PHI with another CE" … Both CEs must have or have had a relationship with the patient…" Given all the people involved in the exchange of medical data that SIM plans to include, will this HIPAA rule be met?

Was the goal of the original creators of the legislation PA 15-146 to allow patients to agree to send their medical records to multiple providers to facilitate their treatment or was it for SIM and the State to use/study their medical data (? identified) for provider evaluations and to set treatment guidelines?

Will the SIM program follow the HIPAA rule of only taking the minimum necessary information? And will patients be able to control who sees their intimate data that they expect their providers to keep private? One way to help achieve privacy would be for the EHR to have the technical capability of segmentation, whereby some information could be kept separate from the rest of the record and under patient control, as was suggested by a Council member at a previous meeting.

Does SIM intend for patient data to be kept private or just confidential, meaning it can be accessed by many without patient consent if need be? Unfortunately, it could be argued that the use of a Master Person/Patient Index number or the "de-identification" of data are not safe enough to justify taking patient data without consent. Even if a MPI number is used, the data must be carefully edited so as not to reveal so much medical information that the person could be identified. Additionally, just having the date of birth, gender and state of residence can be enough to re-identify a person by using all of the online databases available.

Thank you very much.

Susan Israel, MD

Enclosed:

Permitted Uses and Disclosers: Exchange of Health Care Operations
Permitted Uses and Disclosers: Exchange for Treatment

Permitted Uses and Disclosures: Exchange for Health Care Operations

45 Code of Federal Regulations (CFR) 164.506(c)(4)

The Health Insurance Portability and Accountability Act (HIPAA) governs how Covered Entities (CEs) protect and secure Protected Health Information (PHI). HIPAA also provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities *without first obtaining* an individual's authorization: including for **treatment and for health care operations** of the disclosing CE or the recipient CE when the appropriate relationship exists.

Other laws may apply. This fact sheet discusses only HIPAA. Under HIPAA, a CE can disclose (whether orally, on paper, by fax, or electronically) PHI *to another CE or that CE's business associate* for the following subset of health care operations activities of the *recipient* CE (45 CFR 164.501) without needing patient consent or authorization (45 CFR 164.506(c)(4)):

- Conducting quality assessment and improvement activities
- Developing clinical guidelines
- Conducting patient safety activities as defined in applicable regulations
- Conducting population-based activities relating to improving health or reducing health care cost
- Developing protocols
- Conducting case management and care coordination (including care planning)
- Contacting health care providers and patients with information about treatment alternatives
- Reviewing qualifications of health care professionals
- Evaluating performance of health care providers and/or health plans
- Conducting training programs or credentialing activities
- Supporting fraud and abuse detection and compliance programs.

In general, before a CE can share PHI with another CE for one of the reasons noted above, the following three requirements must also be met:

1. Both CEs must have or have had a relationship with the patient (can be a past or present patient)
2. The PHI requested must pertain to the relationship
3. The discloser must disclose only the minimum information necessary for the health care operation at hand.

Under HIPAA's minimum necessary provisions, a health care provider (hereafter "provider") must make reasonable efforts to limit PHI to the minimum necessary to accomplish the purpose of the use, disclosure or request. (45 CFR 164.502(b)). For example, in sharing information with an individual's health plan for population health programs (for example, a diabetes management program), a provider should disclose the PHI that is necessary for the program to be effective.

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

If the CEs are in an "Organized Health Care Arrangement," or "OHCA," as defined in the HIPAA Privacy Rule (45 CFR 160.103), additional capabilities may exist for interoperable exchange of PHI.

The following pages contain example Permitted Uses and Disclosures situations that fall into the health care operations category.

Exchange for Case Management by a Payer

A health plan hires a health care management company to provide semi-monthly nutritional advice and coaching to its diabetic and pre-diabetic members, making the care planning company the health plan's BA. To provide appropriate nutritional advice and coaching, the health care management company needs additional information about the members to make sure the advice is consistent with current treatment received from their medical providers.

The health care management company may query the members' medical providers to obtain information that could impact the nutritional advice being offered. Providers may respond to the query using Certified Electronic Health Record Technology (CEHRT) and may disclose PHI necessary to achieve the case management purpose for which the nutritional coach was hired by the health plan. Disclosure of electronic PHI by CEHRT or other method requires HIPAA Security Rule compliance.

In this scenario, the disclosures by the providers to the care management company (the health plan's BA) are for the health care operations ("population-based activities relating to improving health or reducing costs" and "case management") of the health plan, and therefore are permissible disclosures under HIPAA. A business associate agreement (BAA) is required only between the health plan CE that hires the health care management company BA and that company. The responding CEs may make permissible disclosures directly to the health plan's BA without a BAA between the discloser and the BA (without the need to execute their own BAA with the care management company), just as they could share this information directly with the health plan.

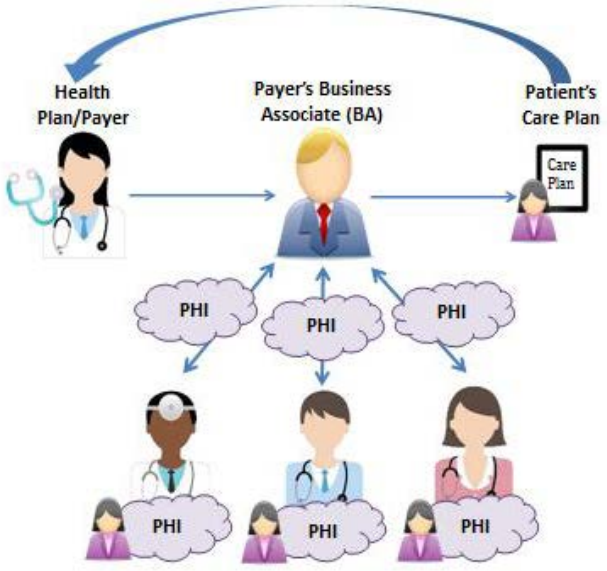

Figure 1: Case Management Scenario

As in the prior scenarios, the providers sharing PHI with the health plan's BA are not responsible under HIPAA for what the BA subsequently does with the information once information has been sent to the BA for a permissible reason and in a secure manner.

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Exchange for Quality Assessment (QA)/Quality Improvement (QI)

There are two examples in this scenario: an ACO quality committee and a quality assessment program using a health information exchange (HIE).

Example 1: ACO Quality Committee

An Accountable Care Organization (ACO) that consists of multiple providers operating as an Organized Health Care Arrangement (OHCA) sponsors a quality committee comprised of individuals who are in the workforce of the providers who operate as an OHCA. The quality committee plans to obtain and review treatment and health outcomes of ACO patients who experienced hospital-acquired infections and surgical errors for the quality assessment and improvement purposes of the ACO/OHCA.

Providers participating in the ACO/OHCA may permit the ACO quality committee to access the PHI needed for the quality assessment through CEHRT.

If the ACO were not operated as an OHCA, or the quality committee was evaluating care quality on behalf of individual providers in the ACO, the providers participating in the ACO could permit the ACO quality committee to access the necessary PHI for the quality assessment through CEHRT, but only for patients whom the requesting and disclosing providers have in common, pursuant to 45 CFR 164.506(c)(4).

Figure 2: QA/QI ACO Scenario

In both instances (OHCA and non-OHCA), access to, or disclosure of, electronic PHI can be made using CEHRT or other method so long as the HIPAA Security Rule is complied with.

Example 2: Quality Assessment using a Health Information Exchange:

As part of a quality review, a provider may need to know the health outcome of a patient that they treated but no longer have contact with (e.g., patient was transferred to another provider). The provider may query a HIE for the relevant health outcomes of the individual.

A provider who has treated the patient and is responding to this query may use CEHRT to send the relevant information to the requesting provider through a HIE. Disclosure of electronic PHI by CEHRT or

other electronic method requires HIPAA Security Rule compliance. This scenario works for any CEs who participate in a health information exchange and is not limited to provider CEs.

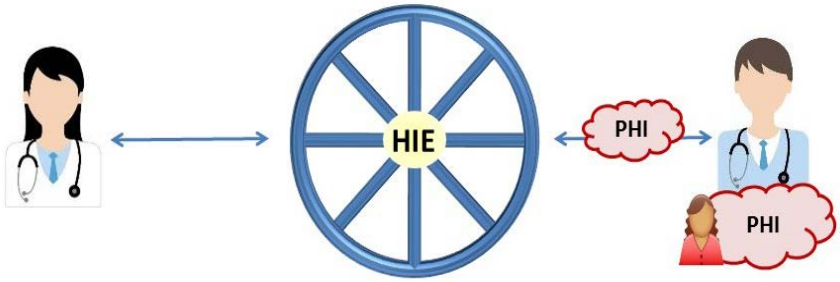

Figure 3: QA/QI Scenario

Quality Improvement Among Several Covered Entities for Population Health

Unaffiliated hospitals in the same community often see the same patients and may not be able to tell whether a patient's hospital-acquired infection resulted from care received at the current treating hospital or from a prior visit to a separate hospital in the community.

The hospitals that have treated or are treating the patient may use CEHRT or a health information exchange to share relevant PHI to try to determine the source for and cause of the infection, so further infections can be prevented.

Disclosure of electronic PHI by CEHRT or other means requires HIPAA Security Rule compliance.

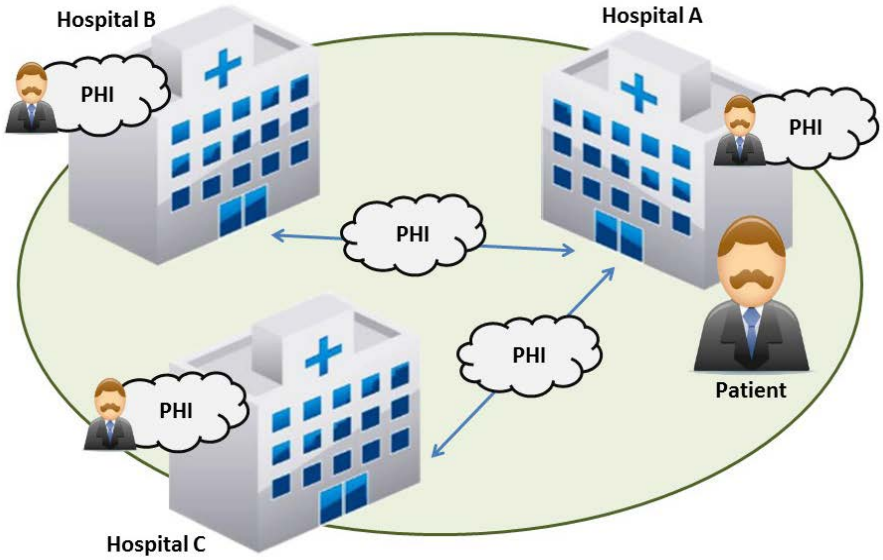

Figure 4: Population-Based Activities Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Permitted Uses and Disclosures: Exchange for Treatment

45 Code of Federal Regulations (CFR) 164.506(c)(2)

The Health Insurance Portability and Accountability Act (HIPAA) governs how Covered Entities (CEs) protect and secure Protected Health Information (PHI). HIPAA also provides regulations that describe the circumstances in which CEs are permitted, but not required, to use and disclose PHI for certain activities *without first obtaining* an individual's authorization: including for **treatment and for health care operations** of the disclosing CE or the recipient CE when the appropriate relationship exists. This fact sheet provides examples of exchange between or among health care providers (hereafter "providers") for **treatment**. There is a companion fact sheet that provides other examples of exchange for the health care operations of the discloser or of the recipient of the PHI that is exchanged.

Other laws may apply. This fact sheet discusses only HIPAA. Under HIPAA, CEs may disclose PHI (whether orally, on paper, by fax, or electronically) to another provider for the treatment activities of that provider, without needing patient consent or authorization (45 CFR 164.506(c)(2)). Treatment (45 CFR 164.501) is broadly defined as the provision, coordination, or management of health care and related services by one or more providers, including the coordination or management of health care by a provider with a third party; consultation between providers relating to a patient; or the referral of a patient for care from one provider to another. When providers share a patient in common and this rule applies, an illustration of how this rule works looks like this.

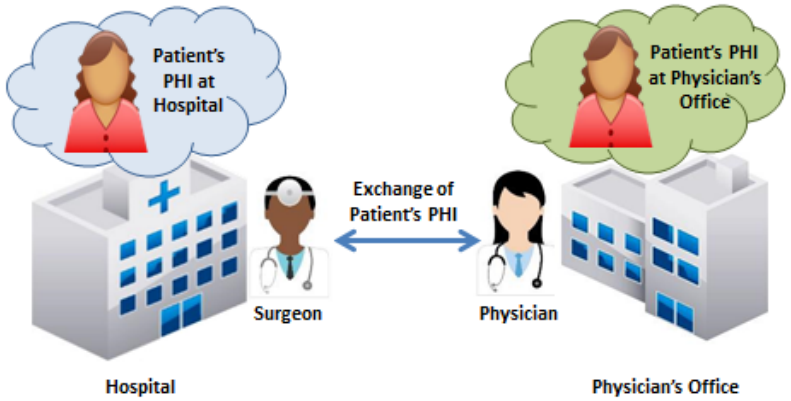

Figure 1: Hospital and Treating Physician exchange information scenario

A common question that arises is whether, in the above illustration, the disclosing hospital will be held responsible under HIPAA for what the receiving provider does with the PHI once the hospital has disclosed it in a permissible way under HIPAA. For example, what if the receiving physician experiences a breach of the PHI? Under HIPAA, after the receiving physician has received the PHI in accordance with HIPAA, the receiving physician, as a CE itself, is responsible for safeguarding the PHI and otherwise complying with HIPAA, including with respect to subsequent uses or disclosures or any breaches that occur. The disclosing hospital is responsible under HIPAA for disclosing the PHI to the receiving physician in a permitted and secure manner, which includes sending the PHI securely and taking reasonable steps to send it to the right address.

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Exchange for Treatment through Care Planning by a Health Care Provider

A provider wants to ensure that discharged patients have a comprehensive care plan for the immediate post-acute period. The provider hires a care planning company (i.e., a Business Associate (BA)) to develop comprehensive care plans for her patients, and signs a business associate agreement (BAA) with the care planning company.

To develop the plan, the BA requests pertinent PHI about the patient from the patients' other providers, such as hospitals the patients have been admitted to for the same or similar medical care, and the patients' health plans. Each of these CEs may disclose the relevant PHI for care planning purposes, using Certified Electronic Health Record Technology (CEHRT) or other electronic means. Disclosure of electronic PHI by CEHRT or other electronic method requires Security Rule compliance.

Note: In this scenario, a BAA is only required between the CE that hires the BA and the BA. The responding CEs may make permissible disclosures directly to the provider's BA for the provider's care planning purposes (without the need to execute their own BAA with the care planning company), just as they could share this information directly with the provider.

Under HIPAA, the patient's other providers and health plans, which have sent PHI to the initial treating provider's BA, are not responsible for what the BA does with the PHI once it has been disclosed permissibly and securely.

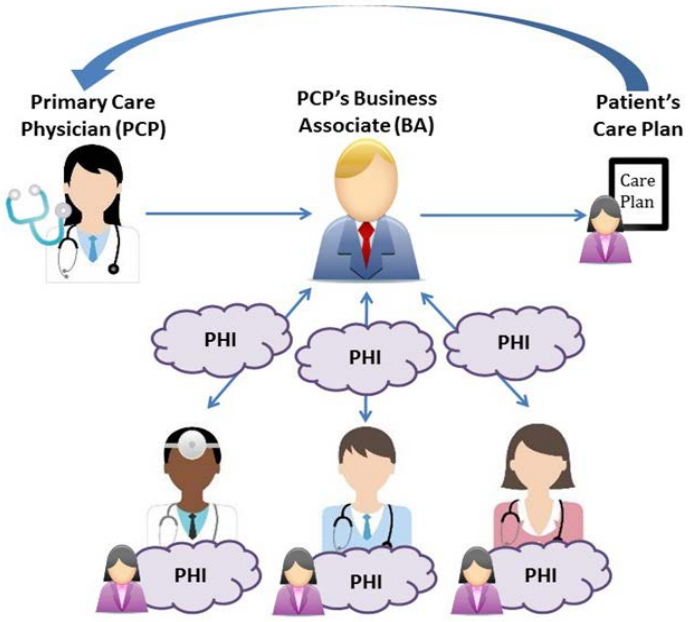

Figure 2: Provider Hires a Care Planner Scenario

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Treatment Includes Prospective Downstream Health Care Providers

When a hospital (an inpatient facility) is preparing to discharge a patient who will need ongoing, facility-based care, the inpatient facility, patient, and patient's family will need to identify a new facility to accept the patient, and the prospective rehabilitation facilities will need protected health information (PHI) about the needs of the patient to determine whether they can provide appropriate care.

The current hospital may disclose the relevant PHI to prospective recipient facilities, such as by using CEHRT. Disclosure of electronic PHI by CEHRT or other means requires HIPAA Security Rule compliance. This disclosure is a treatment disclosure (in anticipation of future treatment of the patient by the rehabilitation facility) and thus may be carried out under 45 CFR 164.506(c)(2).

The inpatient facility is responsible for complying with HIPAA in disclosing the PHI to the rehabilitation facility, which includes sending the PHI securely and taking reasonable steps to send it to the right recipient. After the rehabilitation facility has received the PHI in accordance with HIPAA, the rehabilitation facility, as a CE itself, is responsible for safeguarding the PHI and otherwise complying with HIPAA, including with respect to any breaches that occur. The sending provider/CE in this scenario would not be not responsible for the PHI once it has been received.

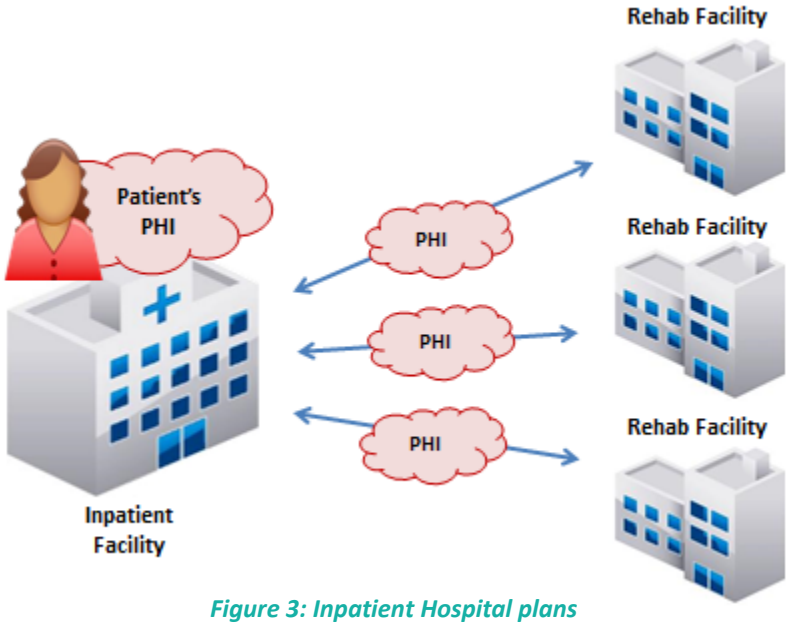

Figure 3: Inpatient Hospital plans Transfer to Rehab Hospital

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.

Using Certified Electronic Health Record Technology and Health Information Exchange

Two providers who need to share PHI for treatment may use CEHRT to send the information to the requesting provider, or may use a health information exchange. Disclosure of electronic PHI by CEHRT or other electronic means requires HIPAA Security Rule compliance.

Additional Resources

- Office for Civil Rights HIPAA Regulations Website
- ONC Guide to Privacy & Security of Electronic Health Information (2015)

The information in this fact sheet is not intended to serve as legal advice nor should it substitute for legal counsel. The fact sheet is not exhaustive, and readers are encouraged to seek additional technical guidance to supplement the information contained herein.