COMMUNITY HEALTH CARE ASSOCIATION of New York State
chcanys.org

PIVOT POINT CONSULTING
A Vaco Company

Empowering Patients Through Information Sharing: Cures Act Compliance Series

February 23, 2022 / **Preparing for Cures Act Regulatory Compliance, Part 1 "Ask the Experts" Session** Polls / Discussion Outline

First poll:

1. Does your health center have a compliance program?
   a. Yes
   b. No
   c. I don't know

2. What areas/roles are represented on your compliance team? [can choose more than one answer]
   a. Legal
   b. Privacy Officer
   c. Security Officer
   d. Compliance / Audit
   e. Information technology
   f. Clinical operations
   g. All of the above

Health centers need a compliance program for HIPAA and the Cures Act as well as program integrity (RCM, coding, etc.). For participants that answered yes, we invited invite them to share with the others about their program. Who leads the program and what areas participate? What areas do they cover? How often do they meet? Are there defined measures that the program tracks and reports out on to your Compliance Committee? Consider what measures you want to track for the Cures Act compliance, and specifically for use of the information blocking exceptions. We reinforced all the areas/roles that need to be represented on a health center's compliance team.

Second poll:

1. Does your health center have written policies, procedures, and annual training that addresses HIPAA privacy and security and health information managements (i.e., records requests/release)?
   a. Yes
   b. No
   c. I don't know

2. [For those that answered Yes to question # 1]. Do you have specific policy/procedures for risk of harm determinations by your licensed healthcare providers; and, in the case of data integrity

issues, by other professionals when denying access to PHI or ePHI [because it is reasonably likely to cause substantial harm or endanger the life or physical safety of a patient or other individual]?

   a. Yes
   b. No
   c. I don’t know

3. Do you have state or local New York laws that require meeting a precondition prior to releasing certain types of health data?
   a. Yes
   b. No
   c. I don’t know

Existing policies, procedures and training for HIPAA privacy and security and HIM should be reviewed and updated to address the information blocking exceptions (including any documentation requirements) for delaying or not fulfilling legally permissible requests for access, exchange or use of EHI. Your existing policies and procedures that address the privacy / protection, availability and sharing of health information should be updated to cover the use of the following exceptions to sharing EHI: Preventing Harm, Privacy, Security, Health IT Performance, Content and Manner, Fees and Infeasibility. The Licensing exception likely does not apply to the health centers. The Preventing Harm, the Privacy sub-exception for pre-condition not satisfied, and the Security exceptions have conditions that require a written organizational policy or documented case-by-case determinations in the absence of a written policy.

For # 2, we invited participants who said yes to elaborate and share information about their policy and procedures.

For #3, we explained how the information blocking Privacy sub-exception for precondition not satisfied should be addressed to comply with the conditions of this exception under the information blocking provision.

Your health center and providers will not be engaging in information blocking if your organization does not provide access, exchange or use of EHI because a necessary precondition required by law is not satisfied. This sub-exception will apply to all instances where your ability to provide access, exchange or use is “controlled” by a legal obligation to satisfy a condition, or multiple conditions, prior to providing that access, exchange or use. The nature of the preconditions you must satisfy will depend on the laws that regulate your health centers and providers. For example, if you are regulated by a more restrictive New York state law, you may need to satisfy more preconditions than a provider regulated by less restrictive state laws.

You must have written organizational policies and procedures. We suggest that your policies and procedures require documentation on how you reached your decision to not fulfill a request for access, exchange or use of EHI including any precondition criteria that were not met and why to qualify for this

Privacy sub-exception. For any situations that doesn't conform to your organization's policies and procedures, you are required to document your decisions on a case-by-case basis.

Your health center must use reasonable efforts within the Center's control to provide the individual with a consent or authorization form when this is a precondition. If you receive a consent or authorization form that requires your assistance to satisfy missing elements on the form that are not required by law and you do not provide the assistance, you may be engaging in information blocking.

Examples that illustrate the precondition not satisfied sub-exception and would justify not providing access, exchange or use of an individual's EHI:

- Not being able to obtain consent of the individual required by certain federal and state laws for their EHI to be accessed, exchanged or used for specific purposes, such as state laws requiring an individual's consent for uses and disclosure of EHI regarding sensitive health conditions, (i.e., HIV/AIDS, mental health or genetic testing).
- An individual's refusal to provide a HIPAA authorization required by law prior to providing access, exchange or use of EHI.
- You are unable to verify the identity or authority of a person requesting access to EHI and such verification is required by law before providing access, exchange or use of EHI.
- Another health care provider is requesting EHI for a quality improvement project that requires your verification that the requestor has a relationship with the person whose information is being requested and you are unable to establish if the relationship exists.

We and the ONC recommend you carefully evaluate the state and federal law requirements imposed on your health center and its providers and that you tailor your responses to the legal precondition which protect and promote the privacy of EHI.

Third poll:

1. The Content condition in the Content and Manner exception only applies to EHI in your EHR system. (True or False) (Answer is False)

2. Who operates, maintains, and controls your clinical systems that contain EHI?
    a. Managed services provider (all systems are hosted off premise/in cloud) and/or by EHR vendor (i.e., using SaaS), we have no internal IT department/employees
    b. Internal IT department / all systems hosted and operated on premise
    c. Combination of internal IT department and external IT service providers (some or no systems hosted on premise)
    d. I don't know

We reinforced that while EHI is limited to the data elements represented in the USCDI standard until October 5, 2022 and most if not all of these data elements are collected and stored in the EHR, that is likely not the case when the EHI definition is no longer limited to the USCDI data elements beginning on October 6, 2022. We suggested IT, clinical ops and HIM work together to inventory and map out where all the ePHI in the health center’s designated record set resides. Remember that there are no requirements in the information blocking provision that require a healthcare provider to use certified health IT, and that the information blocking provision applies to EHI in all systems, regardless of provider type and provider’s participation in CMS payment programs.

For health centers without internal IT resources or with a combination of internal and contracted resources, we will talk about what they need to do with their external partners from a technology perspective at the next webinar in March. For those with internal IT departments/resources or a combination of internal and external resources, some of the things your internal IT staff will be responsible for leading and/or doing include completing an EHI inventory and configuring your systems holding EHI to fully employ available interoperability features and functions that enable fulfilling requests for EHI access, exchange or use in accordance with ONC Cures Act rule. IT will need to have written procedures for the Manner condition of the Content and Manner Exception (how EHI requests are fulfilled for the alternative manners); security policies, procedures, and technologies for data loss prevention, integrity, and availability; and health IT performance SLAs and downtime procedures for planned and unplanned downtime.