COMMUNITY HEALTH CARE ASSOCIATION of New York State
chcanys.org

PIVOT POINT CONSULTING
A Vaco Company

Cures Act Information Blocking Compliance Readiness Checklist Supplemental Information

Please use in conjunction with the Cures Act Information Blocking Compliance Readiness Checklist.

Item #	Explanation / Comments
Compliance Program / Team 1	If your health center has a compliance program, you can start with your existing structure, policies, procedures, and resources as a foundation for compliance with the information blocking regulation. The information blocking regulations and requirements are probably going to be new to most people in your organization, and your compliance staff may have limited knowledge about the information blocking provision and exceptions to sharing EHI. If your health center does not have a compliance program, create one to manage compliance with both HIPAA and the information blocking regulations.
2, 3	To review and modify an existing compliance program or to create a new program, your health center should **involve its subject matter experts**, such as **legal counsel** to interpret and advise on the regulations and laws, **IT staff and the information security officer** to understand how your organization handles access, exchange, and use of EHI now and what needs to be changed, and the **privacy officer** and **HIM staff** to understand how your organization protects the privacy of PHI and complies with federal and state privacy laws, such as HIPAA, and how requests for records and records release is handled now. **Your education/training and marketing/communications staff** will help with operationalizing the compliance program and informing internal and external stakeholders. Your health center may want to create a workgroup or task force under its compliance committee with broader representation needed to address compliance readiness for information blocking, rather than expanding its compliance committee membership.
Policies / Procedures / Agreements 5	Include both HIPAA privacy and security policies, including those governing confidential or sensitive patient information and adolescent health information, and your HIM policies and procedures. Your HIPAA and HIM policies and procedures should align with the information blocking requirements and consider any relevant state laws too. Your policies collectively must address each of the information blocking exceptions. If possible, you should have the policies and procedures addressing information blocking and use of the exceptions in place prior to using an exception. If not, the health center will have to handle and document the particular circumstances of using an exception to delay or not fulfill an EHI request on a case-by-case basis. Detail <u>what</u> your health center requires and expects of its providers and staff within the policy and

	describe how they will meet each exception in the procedures. This will help ensure the health center is applying the exceptions as narrowly as possible and in a non-discriminatory, reasonable manner.
5.a	Fundamentals of Legal Health Record and Designated Record Set https://library.ahima.org/doc?oid=104008#.YiBDecBMGEc. Designated record sets include medical records, billing records, payment and claims records, health plan enrollment records, case management records, as well as other records used, in whole or in part, by or for a covered entity to make decisions about individuals. The HIPAA Privacy Rule requires covered entities to document their designated record sets that are subject to access by individuals (§ 164.524(e)(1)).
6.b	Note the ONC Cures Act Final Rule requires as a Condition and Maintenance of Certification requirement under the ONC Certification Program that health IT developers do not prohibit or restrict communications about certain aspects of the performance of health IT and the developers' related business practices. The ONC finalized (in § 170.403(b)) provisions that permit developers to impose certain types of limited prohibitions and restrictions that strike a balance between the need to promote open communication about health IT and related developer business practices, with the need to protect the legitimate business interests of health IT developers and others. The provisions identify certain narrowly defined types of communications by health care providers which will receive "unqualified protection" under our ONC's Program, such as communications required by law, made to a government agency, or made to a defined category of safety organizations. Under this policy, ONC prohibits developers from imposing any prohibitions or restrictions on such protected communications in their contracts with health care providers. The ONC included provisions allowing health IT developers certified under the Program to place limitations on certain types of communications, including screenshots and video. The health IT developer must not impose or enforce any contractual requirements that contravene the requirements of this Condition of Certification around communications by a health care provider about the developer's health IT. If a health IT developer has contracts/agreements in existence that contravene the requirements of this Condition of Certification, ONC's rule requires the developer to notify all affected customers, other persons, or entities that they will not enforce the prohibition or restriction within the contract/agreement. ONC did not require health IT developers to amend their contracts/agreements to remove or make void such provisions within a specified time, only to do so when they next modify existing contracts/agreements for other purposes or renew/replace the contracts/agreements.

7, 7.a	Providers across a wide range of specialties and practice types usually have well-established protocols for the release of information. In circumstances such as genetic tests, adolescent health, mental health, and substance use disorder, consider how your health center's policies can incorporate important situational context your providers already use in their day-to-day practice, such as situations related to the release of lab tests prior to provider review. While a health center-wide policy to delay patient access until a provider has a chance to review results would likely implicate the information blocking provision of ONC's rule, can your health center create a policy that enables providers to consider the release of lab tests on a case-by-case basis and can the technology enable such a policy? The policy might consider the provider's relationship with the patient, the particular reason for the lab test, who other than the patient may have access to the test results, and the guidelines for the provider's medical specialty around the release of information. Under the ONC Cures Act Final Rule, patients will have broader and more immediate, near real-time access to their health information. On one hand, this is good because it enables patients (and their caregivers) to be better informed and more engaged in their health and health care. On the other hand, patients may misread or misinterpret/misunderstand provider notes in their EHI. Your providers should be vigilant and proactive in ensuring a patient's records are accurate and informative, and do not include terms or language that is offensive to the patient (avoiding use of sensitive words, such as "obese," "addict," "non-compliant," "non-cooperative," "patient refuses," etc.). Of course, your providers should document difficult issues but do it in a way that is non-offensive, yet accurately documents the issue. They should assume that the patient will read all notes and should recognize the practical and legal implications of this. Your providers should be careful when using templates, copy and paste, and the carry-forward features of the EHR. Greater patient access to their EHI will amplify the accuracy and completeness of the information.
7.b	The ONC Cures Act Final Rule defines information blocking as a practice that likely interferes or does interfere with access, exchange, or use of EHI. Slowing or delaying access, exchange, or use of EHI could constitute an "interference" and implicate information blocking. If your health center has the capability to give your patients same-day access to their results but instead has a blanket policy to delay <u>all</u> results for a specified period of time before posting to the patient portal or takes several days to respond to requests for results, this would likely be considered

	information blocking. Your providers should consider what is best for their patients on a case-by-case basis and communicate/engage the patient in their decision-making process when it comes to releasing results and ensure your organizational policies and procedures reflect this.
7.c	Prematurely releasing inaccurate information, such as incomplete clinical notes, may cause harm to a patient. If your health center considers a clinical note to be incomplete and not accurate until a provider signs the note before releasing the note to the patient's portal, consider how your health center's policies and procedures could incorporate the Preventing Harm Exception for these situations. However, ONC cautions that if data in an incomplete note are used to make health care decisions about an individual then that data would fall within the definition of "designated record set" (*see* 45 CFR § 164.501), and therefore, within the definition of EHI. To the extent a data point falls within the definition of EHI, practices likely to interfere with legally permissible access, exchange, or use of that EHI could implicate information blocking.
8	For a practice to be considered information blocking, the regulation requires that providers must know the practice is unreasonable and likely to interfere with access, exchange, or use of EHI. Developing and documenting scenarios where your providers may or may not take reasonable actions could assist in compliance audits. Procedures should provide a detailed workflow and address who will document the case-by-case findings and where.
EHI Inventory / Mapping 9	See USCDI V1, July 2020 Errata for data elements applicable until Oct 6, 2022, then all ePHI in designated record set. United States Core Data for Interoperability (USCDI) | Interoperability Standards Advisory (ISA) (healthit.gov) While the EHR may hold most of your patients' EHI, you should also consider other health IT systems, such as the picture archiving and communication systems (PACS), practice management and revenue cycle management systems (PM/RCM), and onsite laboratory systems or other diagnostic services owned or operated by your health center. These too may be subject to EHI requests since the definition of EHI includes clinical and billing records (i.e., all data in your designated record set as defined in the HIPAA Privacy Rule). This comprises medical records and billing records about individuals; enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; and other records that are used, in whole or in part, to make decisions about individuals. If you maintain identical EHI in more than one system, the regulations only require your health center to provide or produce the information once from one of the systems in response to a request for EHI access, exchange, or use. Therefore, indicate in your EHI inventory and system

	mapping which system will be the primary source for EHI duplicated across systems (e.g., lab orders and results residing in both the EHR and lab information system) when fulfilling an EHI request.
Medical, Billing, and Other Systems 11	Beginning on October 6, the definition of EHI includes all EHI in your systems, not just the USCDI data elements; however, ONC's Cures Act Final Rule or Interim Final Rule is not requiring the health IT vendors to provide an EHI export capability until the end of 2023. Some of the vendors are already working on this and may have this capability available now or later this year.
12	If your technology only has the option to either publish all test results upon receipt or apply a delay for a set amount of time to all results, then your health center should likely publish all test results upon receipt to comply with the information blocking regulation.
13, 14	In many instances, documenting a teen's confidential information within the teen's medical record means that a proxy or parent may also have access. Many teens' EHR portal accounts are established by their parents who would then have access to clinical notes, labs, and other sensitive information. EHRs often do not segment information based on who is accessing the patient's portal account.
Information Blocking General	The preventing harm, privacy, security and fees exceptions under the information blocking regulation closely align with the requirements of HIPAA in § 164.524 Access of individuals to protected health information; however, certain aspects of these HIPAA requirements in the information blocking regulation apply only to "EHI" but extend to all "Actors" as defined in the regulation, not just covered entities.
19	It is better and preferable if your health center has a way to document any use of an information blocking exception contemporaneously rather than retrospectively. Incorporating exception templates/forms into the EHR may simplify the documentation process and provide better integration and accountability within your health center's day-to-day practice.
20	Remember your providers must have the required knowledge and intent to interfere with access, exchange, or use of EHI to be considered information blocking.
Preventing Harm 21	The Preventing Harm exception allows for a provider to deny access to and decline to share data that is reasonably likely to cause substantial harm or danger to life or physical safety (the harm types in this exception align with and reference the HIPAA harm standards) as follows: 1. Substantial harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with access, use, or exchange of a patient's EHI by his/her legal representative.

	○ Type of harm is substantial harm to patient or another person. ○ Risk of harm is determined by a health care professional. 2. Substantial harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with a patient's or his/her legal representative's access, use, or exchange of the patient's EHI that references another person. ○ Type of harm is substantial harm to another person. referenced in EHI other than a health care provider. ○ Risk of harm is determined by a health care professional. 3. Danger to life or physical safety harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with a patient's access, use, or exchange of his/her EHI. ○ Type of harm is to life or physical safety of patient or other person (does not include emotional harm). ○ Risk of harm is either determined by a health care professional or arises from a data integrity issue. 4. Danger to life or physical safety harm standard where the practice is implemented to substantially reduce a risk of harm and is likely to or does interfere with a legally permissible. access, use, or exchange of EHI not described in 1-3 above. ○ For example, access, exchange, or use of EHI by health care providers furnishing services to the patient and type of harm is to life or physical safety of patient or another person. ○ Risk of harm is either determined by a health care professional or arises from a data integrity issue (i.e., declining to share data that is corrupt, inaccurate, or erroneous or that arises from misidentifying a patient or mismatching a patient's EHI). - For risk of harm determinations made by a licensed provider, provider must have made the determination in context of a current or prior clinician-patient relationship. Other "Actors," such as an HIN/HIE or hospital, can rely on such determination upon becoming aware of the determination and until such time they become aware the determination has been reversed or revised.
21.a.ii.1	ONC's Cures Act Final Rule does not require specific or unique documentation for risk of harm determinations made by a health care professional. Recommend your health center require that providers document these determinations in the EHR. ONC considers this appropriate approach to documentation.

Privacy 22.d	Unless otherwise required by law to share PHI/ePHI, a provider can elect to not provide access to an individual's EHI to respect an individual's request not to share the individual's EHI.
Health IT Performance	This exception does not apply for maintenance and improvements aimed at preventing harm to a patient or other person (e.g., in the case of addressing a data integrity issue) or to security-related practices—instead, you would need to comply with the Preventing Harm or Security exceptions, respectively.
Infeasibility 30	Uncontrollable events beyond a provider's control: • Natural or human-made disaster • Public health emergency • Public safety incident • War • Terrorist attack • Civil insurrection • Strike or other labor unrest • Telecommunications or internet service interruption • Act of military, civil or regulatory authority
32	Legitimate practical challenges may limit your health center's ability to comply with requests for access, exchange, or use of EHI. The health center may not have and may be unable to obtain the requisite technological capabilities, legal rights, or other means necessary to enable access, exchange, or use. It will not be information blocking if the health center does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request, under the circumstances, if the health center complies with the requirements under this condition.
Training and Education 35	Information blocking is new and many of your health center staff are not going to understand the requirements at first. Your front- and back-office staff will often be the first to encounter EHI requests. They should have a clear understanding of your organization's obligations, policies, and procedures; know how to respond (or not respond); and how to document the actions they take and why.
38.a	ONC encourages providers to provide educational information to their patients on what to consider when choosing a 3rd-party consumer app and authorizing access to their health data when it comes to the privacy and security practices of the app developer. Ensure the information your health center decides to provide patients is provided in an unbiased, fair, objective, and consistent fact-based manner. Check out the CARIN Alliance's resources. The Alliance's vision is to rapidly advance the ability for consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals. Specifically, the Alliance is promoting the ability for consumers and their authorized caregivers to

	gain digital access to their health information via open APIs. The Alliance developed a code of conduct for app developers to voluntarily sign and have their apps listed on the Alliance's "My Health Application" website. The Code of Conduct is a set of industry-leading best practices these application developers have voluntarily adopted to protect and secure consumers' health information. Here are links to the CARIN Alliance and their My Health Application website: https://www.carinalliance.com/ https://myhealthapplication.com/
38.b	Consider holding patient-focused educational webinars and recording the webinars and making them available on your health center's website. Consider distributing your health center's educational materials to patients during an office visit or posting them on your website or patient portal (if technically able to).
Communications 39.a.iv	The AMA stated the following in one of its publications on complying with the information blocking requirements: "You can expect the information blocking regulation to be "weaponized" by those seeking data access. We expect entities such as payers and health plans to leverage the info blocking rules to gain increased access to you EHR and patient records. While this may be communicated to you or your organization as a way to reduce administrative burden, (e.g., reduce the burden around prior authorizations), there is increasing concern that payers could threaten physician practices with 'info blocking action' if their requests for direct access into your EHR [are] denied. Payers having unfettered access to all your patients' records may impact patient coverage, access to care, narrowing of networks, or your autonomy to practice medicine. We strongly urge all physicians to seek counsel from an attorney prior to responding to any payer or health plan requests for direct access into their EHR." Cover fulfilling payer's and health plan's EHI requests in your health center's procedures and be clear in your communications with them about how your organization will fulfill payer/health plan requests for EHI access, exchange, or use in accordance with the Content and Manner exception and other exceptions as they may apply, such as the Privacy exception.