COMMUNITY HEALTH CARE ASSOCIATION of New York State
chcanys.org

PIVOT POINT CONSULTING
A Vaco Company

Cures Act Information Blocking Compliance Readiness Checklist

Purpose/Instructions: This checklist provides a framework for conducting a self-assessment of your health center's readiness to comply with the information blocking provision and requirements in the Office of the National Coordinator for Health IT (ONC) Final Cures Act Rule and ONC Interim Final Rule published in 2020. Completing this checklist will enable your health center to determine the policy, process, procedure, technology, and training and education gaps it needs to address to be ready to fulfill requests for access, exchange, or use of Electronic Health Information (EHI, as defined in the ONC Rule) and appropriately use the information blocking exceptions. Your health center should not assign this checklist and self-assessment to a single individual to complete. The recommended approach is for your organization to first identify a project lead, such as your compliance officer, and a team of subject matter experts, next assign portions of the checklist to the appropriate SME(s) to complete, and then compile and discuss the results as a team. The team will then develop a workplan and assignments to close the gaps they identified in their assessment. The project lead would start with the first section of the checklist, "Compliance Program/Team," before making assessment assignments.

Compliance Program / Team	**Response**	**Comments / Action Items / Assignments**
1. Does your health center have an existing compliance program?	Yes/No	
2. Does your health center have a compliance committee?	Yes/No	
3. Does the committee include representation with expertise in the following areas?		
a. Legal? Name/Title: _____	Yes/No	
b. Privacy? Name/Title: _____	Yes/No	
c. Technology? Name/Title: _____	Yes/No	
d. Information security? Name/Title: _____	Yes/No	
e. Clinical operations? Name/Title: _____	Yes/No	

f. Revenue cycle/Patient billing? Name/Title: _____	Yes/No	
g. Education and training? Name/Title: _____	Yes/No	
h. Communications and marketing? Name/Title: _____	Yes/No	
4. Has your compliance committee received an overview and orientation to the information blocking requirements and exceptions?	Yes/No	
Policies / Procedures / Agreements		
5. Have you completed an inventory and review of your health center's policies and procedures related to responding to health information requests and identified those requiring revisions to address the requirements of each information blocking exception? [Note: A section for each information blocking exception with assessment steps is provided in this checklist.]	Yes/No	
a. Do you have a policy that defines your health center's legal medical record (i.e., designated record set)?	Yes/No	
b. What do your current HIPAA and HIM policies say about patients, patients' personal representatives, non-affiliated providers, payers/health plans, and other third parties accessing patients' medical records, on paper and electronically?		
i. Do your current policies regarding an individual's right to access ePHI reflect the requirements of both the HIPAA Privacy Rule and the ONC Cures Act Final Rule?	Yes/No	
c. How long does it take your organization to make EHI available upon request?		
i. What actions would your health center need to take to make information available without delay or minimal		

delay?		
d. Do your procedures require special effort by the patient to access his or her ePHI?	Yes/No	
i. If yes, what could your health center do to minimize or reduce the effort required by patients?		
ii. Do you require the patient to fill out a form and sign a release to self to access his or her ePHI?	Yes/No	
1. If yes, what actions would your health center need to take to eliminate this requirement?		
6. Have you reviewed your health center's contracts and Business Associate Agreements (BAAs) with any "Actors" defined in the information blocking regulation, such as with health IT vendors, HINs/HIEs you are connected to, and other health care entities with whom you do business and share health information?	Yes/No	
a. Do any of the contracts or agreements have any terms or conditions that would prevent or interfere with legally permissible access, exchange, or use of EHI?	Yes/No	
i. If yes, what are the terms or conditions?		
b. Do any of the contracts have language restricting your communications about the vendor's health IT?	Yes/No	
i. If yes, are the restrictions consistent with what the ONC Cures Act Final Rule permits?	Yes/No	
ii. If not consistent with the what the rule permits, did the health IT vendor notify you to tell you they would not enforce these restrictions and would amend the contract?	Yes/No	
c. Have any of your health IT vendors notified you about other changes needed to your contracts with them due to the ONC Cures Act Final Rule requirements?	Yes/No	
i. If yes, what are the changes?		

ii. Are the changes consistent with the rule?	Yes/No	
d. Does your current BAA say anything about your Business Associate fulfilling your, your patients' or other providers requests for access, exchange, or use of a patient's EHI that would interfere with, delay, or prevent fulfilling legally permissible requests?	Yes/No	
7. Are clinical notes, lab results, and other diagnostic reports available electronically to patients on the patient portal as soon as your providers complete/sign their notes or receive an electronic copy of results/reports?	Yes/No	
a. If not, why? What actions would your health center need to take to make information available without delay or minimal delay?		
b. Does your health center delay patient electronic access to some or all lab results or other diagnostic reports for a specified time period until a provider has an opportunity to review the result (such as a 36- to 48-hour window after results become available)?	Yes/No	
c. How does your organization define accuracy and completeness with respect to clinical notes?		
8. Has your health center defined its reasonableness standard when it comes to practices/procedures or workflows that interfere with, delay, or prevent access, exchange, or use of EHI? If no, consider doing so.	Yes/No	
EHI Inventory / Mapping		
9. Has your health center identified, documented, and mapped where all patient EHI is held within its systems (reference 5.a for what is included your health center's designated record set)?	Yes/No	
Medical, Billing, and Other Systems (Consult/meet with your health IT vendor(s) and HIN/HIE organization if your health center is unsure or does not know the answers to the questions in this section.)		

10. Has your health IT vendor(s) released the required Cures Act updates for your certified 2015 Edition health IT?	Yes/No	
a. If no, when will the updates be available?		
b. If yes, has IT or your vendor(s) installed the updates and configured the technology to enable legally permissible electronic access, exchange, and use of EHI?	Yes/No	
c. Is your health center familiar with the features, functions, and required configuration to enable the updated features and functionality? If not, consult with your vendor(s) for training/resources.	Yes/No	
11. Does your health IT vendor(s) have a plan for distinguishing between data elements included in the USCDI and other EHI included in the EHR and other systems (i.e., PM, RCM, etc.) for purposes of responding to requests for EHI prior to October 6, 2022? If so, what is the plan?	Yes/No	
a. Has the vendor(s) developed a capability yet for EHI export (human and machine readable) of all EHI for a patient stored in the vendor systems' databases?	Yes/No	
12. What configuration options are presently available in your clinical systems for releasing notes, results, and reports to the patient portal?		
a. Can your providers selectively delay release of certain results for a patient when necessary?	Yes/No	
13. Does your EHR support data segmentation and how (i.e., either to comply with state or federal privacy laws for certain sensitive data or adolescent data or to respect a patient's request to not share certain health information)?	Yes/No	
14. Does your Patient Portal support restricted access for certain users and how (e.g., to remove parental/guardian access to certain health information that an adolescent can choose to keep private)?	Yes/No	
15. Who will manage the FHIR API server, endpoints, and registration for API		

access by 3rd-party application developers (i.e., your IT department, health IT vendor for your EHR, other health IT vendor, etc.)?		
a. How are 3rd-party apps registered and how does a patient authorize a 3rd-party consumer app to access his or her EHI via the certified APIs?		
16. Have your providers' digital endpoints (e.g., Direct secure messaging address) been added to NPPES? Adding Digital Endpoints in NPPES v2 (maxmddirect.com)	Yes/No	
17. Does or can your EHR vendor (or other health IT vendor) provide connectivity to your local, regional, or state Health Information Network (HIN)/Health Information Exchange (HIE)? Is your health center presently connected to and participating in a HIN/HIE?	Yes/No Yes/No	
a. If yes, have you met and consulted with your EHR or other health IT vendor(s) and/or the HIN/HIE organization to discuss any additional functionality/services available to respond to and fulfill EHI requests via the HIN/HIE and the requirements you must fulfill to use the services, and any costs?	Yes/No	
b. If no, have you met and consulted with the appropriate representative from the HIN/HIE organization and your EHR or other health IT vendor(s) to learn and document what you need to do to connect to the HIE (technical requirements, costs, contracting, BAA, etc.)?	Yes/No	
Information Blocking Exceptions		
General		
18. Have you consulted with your health IT vendor(s) on their preparations to comply with the ONC Cures Act Final Rule and information blocking requirements and how they will help you determine and document your health center's use of the exceptions?	Yes/No	

19. Have you created exception templates/forms that align with your health center's updated policies and procedures?	Yes/No	
a. If yes, have you asked your IT department or health IT vendor(s) to incorporate these templates in the EHR (and PM, RCM systems as applicable) to make them easily accessible within your providers' and support staff's workflows?	Yes/No	
20. What practices have you identified that your health center engages in that would not fit within an exception and would likely interfere with legally permissible access, exchange, or use of EHI and be considered information blocking?		
a. If you identified any, can your health center modify these practices to fit within an exception? Note the modifications you can make.	Yes/No	
b. For any practices that do not fit within an exception but are necessary for your business, has your health center documented that it does not intend for these practices to result in information blocking and why?	Yes/No	
Preventing Harm Exception		
21. Have you reviewed and assessed your health center's policies, practices, and procedures for denying access to health information to reduce substantial risk of harm to a patient or another person (in accordance with the HIPAA harm standards, § 164.524(a)(3) Reviewable grounds for denial), and identified and documented revisions or new policies/procedures needed to address the requirements of the Preventing Harm exception for delaying or denying EHI access, exchange, or use?	Yes/No	
a. Do you have an existing written policy and/or procedures? If yes:	Yes/No	
i. Do your policy and procedures address risk of harm due to data integrity or patient matching/misidentification	Yes/No	

issues?		
1. What are your IT department's and/or vendors' current processes, if any, for addressing data integrity or patient matching/misidentification issues?		
ii. How do your providers currently make determinations to deny a patient's or the patient's personal representative's access to a patient's health information when the provider believes the access is reasonably likely to cause substantial harm or endanger the life or physical safety the patient or another person (in accordance with HIPAA)?		
1. What are your current documentation requirements for these determinations?		
iii. Do your policy and procedures require the following for denials?		
1. Written notification of the denial in plain language, including basis for denial?	Yes/No	
2. Inclusion of information about individual's right to have a decision reviewed, how to request a review, and how to submit a complaint to the provider organization or HHS OCR in the written notification?	Yes/No	
3. Notification of denial within 30 days (or 60 if individual was notified of an extension)?	Yes/No	
4. A designated reviewing official to address denials having reviewable grounds?	Yes/No	
5. A set time period for the reviewing official to reaffirm or reverse a denial having reviewable	Yes/No	

grounds?		
6. Prompt written notification to individual on reviewing official's determination as well as other actions required to carry out the determination?	Yes/No	
b. If you do not have an existing written policy and/or procedures, develop a policy and require that any practices denying access to PHI/ePHI/EHI to reduce risk of harm conform to the following conditions in the Preventing Harm exception:		
i. Reasonable belief that denying access will substantially reduce risk of harm.		
ii. Breadth of practice to deny access is no broader than necessary.		
iii. Meets at least one condition from the "Type of Risk" and "Type of Harm" categories in the Preventing Harm exception.		
iv. Implemented by your providers in a consistent and non-discriminatory manner.		
v. Allows for a patient's review rights when applicable and reversal of provider's determination to deny or delay access to the patient's PHI/ePHI.		
Privacy Exception		
22. Have you reviewed and assessed your health center's policies, practices, and procedures for protecting patient privacy, and identified and documented revisions or new policies/procedures needed to address the requirements of the Privacy sub-exceptions for delaying or denying EHI access, exchange, or use?	Yes/No	
a. Does anything in your current HIPAA Notice of Privacy Practices (NPP) conflict with what the information blocking regulation requires regarding EHI?	Yes/No	

i. If yes, what are the conflicts?		
b. Do you need to make any revisions to your HIPAA NPP to address the following information blocking Privacy sub-exceptions?	Yes/No	
i. Meeting pre-conditions required by law prior to releasing/sharing EHI?	Yes/No	
ii. Denial of an individual's request for EHI consistent with the HIPAA Privacy Rule's "unreviewable grounds" for a denial of access?	Yes/No	
iii. Respecting an individual's request not to share information?	Yes/No	
c. Do you have NY state or federal laws that require you to obtain a patient's authorization prior to fulfilling a request for EHI? If yes, identify, document, and incorporate the following in your privacy policy and procedures:	Yes/No	
i. Reference to the specific law(s).		
ii. The EHI covered by the law(s).		
iii. The pre-conditions you must meet prior to sharing/releasing the EHI.		
iv. The process for obtaining any required consents.		
1. Do you need to revise your existing consent forms or develop a new form?	Yes/No	
v. How and where will your health center document use of this Privacy sub-exception when unable to meet a pre-condition prior to fulfilling an EHI request and must deny the request?		
d. Do your current privacy policies and procedures address denying an individual's request for PHI/ePHI that the HIPAA Privacy Rule does not permit you to share?	Yes/No	

e. Do your current privacy policies and procedures allow a patient to request orally or in writing not to share his or her EHI? If yes, do the policies and procedures include the following?	Yes/No	
i. Directs providers to not encourage or induce an individual not to share.	Yes/No	
ii. Requires providers to document the individual's request in a reasonable time period.	Yes/No	
iii. Permits providers to terminate an individual's request for a restriction on sharing the individual's EHI, if: 1. Individual requests termination in writing or agrees to termination in writing; or 2. Individual orally agrees to termination and provider documents the oral agreement; or 3. Provider informs the individual it is terminating the agreement.	Yes/No	
If the policies and procedures do not satisfy the requirements specified in 22.d., update the applicable policies and procedures accordingly to use this Privacy sub-exception to not fulfill an EHI request.		
f. Are documentation requirements for use of each of the Privacy sub-exceptions included in your policies and/or procedures?	Yes/No	
i. How and where will your health center document use of these Privacy sub-exceptions?		
Security Exception		
23. Have you reviewed and assessed your health center's policies, practices, and procedures for safeguarding the confidentiality, integrity, and availability of EHI, and identified and documented revisions or new policies/procedures needed to address the requirements of the Security exception for delaying or denying EHI access, exchange, or use?	Yes/No	

a. Are the security practices of your health center that are likely to interfere with access, exchange, or use of EHI directly related to safeguarding the confidentiality, integrity, and availability of its data and tailored to addressing specific risks to its network and infrastructure? Note the specific practices.	Yes/No	
b. Are these security practices implemented in accordance with a written organizational security policy?	Yes/No	
i. Is the policy based on and directly responsive to security risks your health center or someone on its behalf identified and assessed?	Yes/No	
ii. Do the security practices align with one or more applicable consensus-based standards or best-practice guidance? If yes, what standards or best-practice guidance?	Yes/No	
iii. Does the policy provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents?	Yes/No	
iv. If you do not have a written policy, does your health center make a determination in each case based on particular facts and circumstances that:		
1. The security practice is necessary to mitigate the risk to EHI; and	Yes/No	
2. There are no reasonable alternatives that address the security risk that are less likely to interfere with the access, exchange, or use of EHI?	Yes/No	
Do you have written procedures for making and documenting these determinations?	Yes/No	
c. Are the security practices implemented in a consistent and non-discriminatory manner?	Yes/No	

i. Do you treat similarly situated actors/entities whose interactions pose the same level of security risk consistently with one another in your security policy and practices?	Yes/No	
d. How and where will your health center document use of the Security exception when a security practice delays or interferes with access, exchange, or use of EHI?		
Health IT Performance Exception		
24. Do you have Service Level Agreements (SLAs) with your IT department and/or your managed services provider and health IT vendors? If you do not have SLAs in place with your IT department and/or in your contracts with your service providers and health IT vendors, then work with them to establish SLAs that will meet the requirements of the Health IT Performance exception.	Yes/No	
25. Do your practices or your vendors' practices to maintain and improve your health IT meet the following requirements?	Yes/No	
a. Implemented no longer than necessary?	Yes/No	
b. Implemented in a consistent and non-discriminatory manner?	Yes/No	
c. Consistent with SLAs for planned and unplanned downtime or for unplanned downtime agreed to?	Yes/No	
26. Has your IT department and/or service providers and health IT vendors documented their planned and unplanned downtime procedures and do they follow the procedures?	Yes/No	
27. How do you communicate with the following stakeholders when planned or unplanned downtime will impact their access, exchange, or use of EHI, if applicable?		
a. Your providers and clinical staff?		
b. Your patients?		
c. External non-affiliated providers and hospitals?		

d. Payers/health plans?		
e. Your local, regional, or state HIE?		
28. Do you have written procedures to address situations where a third-party application is operating or behaving in a way that does not pose a security risk but is negatively impacting the performance of your network, servers, or core functions of other applications?	Yes/No	
29. How and where will your health center document planned or unplanned downtime that interferes with the access, exchange, and use of EHI?		
Infeasibility Exception		
30. If an applicable uncontrollable event occurs (e.g., internet outage) that prevents your health center from providing access, exchange, or use of EHI, how and where will your health center document that this event occurred and for how long it impacted your ability to provide access, exchange, or use of EHI to qualify for the Infeasibility exception during this event?		
31. If you are required to withhold certain EHI due to a patient's preference, a law, or to prevent harm; and you cannot unambiguously segment the EHI you have to withhold from the requested EHI, how and where will your health center document these situations to qualify for the Infeasibility exception?		
32. Do you have a procedure for complying with the "Infeasible under the circumstances" condition of the Infeasibility exception that includes the determination factors in 32.a and requirements in 32.b-c for times when the burden of fulfilling an EHI request in "any manner" or an "alternative manner" is significant due to limited technical capability and resources? If no, develop a procedure that will address 32.a-c below for any "infeasible under the circumstances" determination.	Yes/No	
a. A contemporaneous written record or other documentation of any determination that it is infeasible under the circumstances	Yes/No	

for your health center to fulfill an EHI request and the determination considers, addresses, and documents these factors:		
i. Type of EHI requested and purpose for which it may be needed?	Yes/No	
ii. Cost of complying with the request in the manner requested?	Yes/No	
iii. Financial, technical, and other resources available to your health center?	Yes/No	
iv. Whether your health center provides comparable access, exchange, and use to itself or to its customers, suppliers, partners, and other persons with whom your health center has a business relationship?	Yes/No	
v. Whether your health center owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged?	Yes/No	
vi. Why your health center was unable to provide access, exchange, or use of EHI consistent with the Content and Manner exception?	Yes/No	
b. Does the procedure apply the determination factors in a consistent and non-discriminatory manner?	Yes/No	
c. Does your health center complete its contemporaneous written record of its determination and respond in writing to the requestor within 10 business days of the receipt of the request with the reason(s) why you are not fulfilling the request?	Yes/No	
Content and Manner Exception		
33. Does your health center have a process and procedure based on the Content and Manner exception that is followed when it receives and	Yes/No	

fulfills a request for EHI access, exchange, or use?		
a. As part of this procedure, does it outline when it is appropriate for your health center to deny a request and reference/link to the applicable health center policies and procedures relevant to the denial such as for preventing harm, patient privacy, inability to segment EHI, etc.?	Yes/No	
b. Does the procedure address fulfilling EHI requests for each of the three alternative manners in the "Manner Condition?"	Yes/No	
i. Using technology certified to Part 170 adopted standard(s)?	Yes/No	
ii. Using content and transport standards specified by the requestor and published by the federal government or standard developing organization accredited by ANSI?	Yes/No	
iii. Using a mutually agreeable alternative machine-readable format, including a means to interpret the EHI?	Yes/No	
Fees Exception		
34. Does your health center currently charge fees to fulfill requests for ePHI?	Yes/No	
a. If yes, will the fees your health center charges meet the "Basis of fees" condition and not include any fees addressed in the "Excluded fees" condition of the Fees exception? If not, revise your policy/fee schedule accordingly.	Yes/No	
Training and Education		
35. What is your health center's approach to education and training on regulations, such as HIPAA?		
a. Can your educational materials and training curriculum for HIPAA be adapted/revised to incorporate the information blocking regulatory requirements for fulfilling requests for EHI access, exchange, or use?	Yes/No	
b. Will you need to develop new educational materials and training	Yes/No	

curriculum for the information blocking regulatory requirements for fulfilling requests for EHI access, exchange, or use?		
36. Does your health IT vendor(s) have educational resources and/or training modules available, especially with regards to training on how to access and use the interoperability elements within your health IT?	Yes/No	
a. If yes, what is available and how do you access the educational resources and training?		
37. Has your health center developed and delivered training for its staff to orient them on the exceptions to sharing EHI under the information blocking regulation and inform them of changes to existing and of new privacy, security, and HIM-related policies and procedures that incorporate and address the information blocking exceptions?	Yes/No	
a. Have you educated your providers and clinical staff on the various technical ways available within your health center's systems to securely share EHI with their patients, with providers outside your organization to whom they refer patients, and with payers/health plans (e.g., as necessary for prior authorization)?	Yes/No	
b. Do all medical and office staff understand how to use any templates/forms created for documenting exceptions and where to find them?	Yes/No	
c. Have you developed scripts for your clinical staff on how to respond to requests for EHI?	Yes/No	
d. Are you tracking attendance and completion of the training and keeping records?	Yes/No	
i. Where are you storing this information?		
e. Have you added the information blocking regulation to your new employee and annual training requirements?	Yes/No	
38. Has your health center developed educational materials for its patients on the various ways available to them to request and electronically	Yes/No	

access their ePHI or EHI, including how to authorize a 3rd-party consumer app to access their ePHI (Common Clinical Data Set (CCDS)) or EHI (USCDI data) via APIs?		
a. Will you provide your patients education on what they should consider in choosing a consumer app when it comes to the app developer's privacy and security practices and the protection of their data?	Yes/No	
b. How will you disseminate the educational materials to your patients?		
Communications		
39. Has your health center developed a communication plan to inform its providers and staff, its patients, external providers (e.g., other providers treating your patients), and payers/health plans (e.g., for prior authorization) on how your health center is fulfilling requests for EHI access, exchange, or use?	Yes/No	
a. Does the plan include targeted messaging for the following?		
i. Internal teams?	Yes/No	
ii. Patients?	Yes/No	
iii. Non-affiliated providers in your referral network and hospitals?	Yes/No	
iv. Payers/health plans?	Yes/No	
v. Local, regional, or state HIE (if connected)?	Yes/No	
b. Does the plan include multiple forms of communication and media for the target audiences?	Yes/No	