Stony Brook Medicine

Stony Brook Medicine
Administrative Policy and Procedures

Subject: IM0090 Information Blocking and Usage of the Confidential Non-Portal Note Type	**Published Date:** 12/18/2024
Management of Information	**Next Review Date:** 12/18/2027
Scope: SBM Stony Brook Campus	**Original Creation Date:** 07/03/2024

Policy:

Stony Brook University Hospital (including all its locations, collectively "SBUH") complies with information blocking provisions as outlined in section 4004 of the 21st Century Cures Act (Cures Act) and codified under 45 CFR Part 171. SBUH employs blocking practices in relation to EHI access, exchange, "confidential note types", and use.

Definitions:

Access: The ability or means necessary to make electronic health information available for Exchange or Use.

Actor: A health care provider, health IT developer of certified health IT, health information network or health information exchange.

Confidential Non-portal Note: A document type within the Cerner EHR that is not available on the patient portal (nor is it released as part of an information access request) at the discretion of the clinician authoring the note. Using this note type is made on a case-by-case basis by the clinician either at the request of the patient or to prevent physical harm to the patient or other individual.

Electronic Health Information (EHI): Electronic Protected Health Information contained in a Designated Record Set. It does not include Psychotherapy Notes or information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding. EHI also excludes any information that has been de-identified in accordance with HIPAA's de-identification standards.

ePHI- means electronic Protected Health Information that is electronically created, received, maintained or transmitted.

Protected Health Information (PHI) – A individual's oral, written or electronic health information created or received by a Covered Entity, that is identifiable or for which there is a reasonable basis to believe that the information can be used to identify the individual, and relates to 1) the past, present, or future physical or mental health condition of an individual, or 2) the provision of health care or payment for health care to an individual. HIPAA details the below 18 identifiers that render health information identifiable:

1. Names;
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code in certain situations.
3. All elements of dates (except year) for dates directly related to a patient, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code.

Information blocking: A practice that - except as required by law or covered by an information blocking exception - is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information; and if conducted by a health care provider, such provider knows that such practice is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information.

Interfere with* or *interference: To prevent, materially discourage, or otherwise inhibit.

Procedures:

1. SBUH does not engage in information blocking when the practice falls within an exception.
    A. The Cures Act has defined eight specific exceptions. These exceptions serve to clarify circumstances under which certain actions affecting EHI is not deemed as information blocking. Not meeting the conditions of an exception does not inherently imply information blocking. Practices not fully aligning with an exception's criteria are subject to a detailed evaluation on an individual basis to ascertain the presence of information blocking.
    B. The eight exceptions to the CURES act fall into two categories, (1) Exceptions that allow for denying requests to access, exchange, or use EHI and (2) Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI;

        (1) Exceptions permitting the denial of requests for EHI Access, Exchange, or Use.

        a) **Preventing Harm Exception**: It is not be information blocking for an actor to engage in practices that are reasonable and necessary to prevent harm to a patient or another person, provided the below conditions are met.
            1) The actor must hold a reasonable belief that the practice substantially reduces the risk of harm.
            2) The actor's practice must be no broader than necessary.
            3) The actor's practice must satisfy at least one condition from each of the following categories: type of risk, type of harm, and implementation basis.
            4) The practice must satisfy the condition concerning a patient's right to request review of an individualized determination of risk of harm.
        b) **Privacy Exception:** It is not information blocking if an actor does not fulfill a request to access, exchange, or use EHI in order to protect an individual’s privacy, provided at least one of the below four conditions is met.
            1) Precondition not satisfied: If an actor is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing

access, exchange, or use of EHI, the actor may choose not to provide access, exchange, or use of such EHI if the precondition has not been satisfied under certain circumstances.

2) Health IT developer of certified health IT not covered by HIPAA: If an actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule, the actor may choose to interfere with the access, exchange, or use of EHI for a privacy-protective purpose if certain conditions are met.
3) Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a) (1) and (2): An actor that is a covered entity or business associate may deny an individual's request for access to his or her EHI in the circumstances provided under 45 CFR 164.524(a)(1) and (2) of the HIPAA Privacy Rule.
4) Respecting an individual's request not to share information: An actor may choose not to provide access, exchange, or use of an individual's EHI if doing so fulfills the wishes of the individual, provided certain conditions are met.
    i. Individual requests that the Actor not provide such access, exchange, or use of the EHI without any improper encouragement or inducement of the request by the Actor.

c) **Security Exception:** It is not information blocking for an actor to interfere with the access, exchange, or use of EHI in order to protect the security of EHI, provided certain conditions are met. The practice must be:
    1) Directly related to safeguarding the confidentiality, integrity, and availability of EHI
    2) Tailored to specific security risks; and
    3) Implemented in a consistent and non-discriminatory manner.
    4) The practice must either implement a qualifying organizational security policy or implement a qualifying security determination.
d) **Infeasibility Exception:** It is not information blocking if an actor does not fulfill a request to access, exchange, or use EHI

due to the infeasibility of the request, provided one of the below conditions is met.

1) Uncontrollable events: The actor cannot fulfill the request for access, exchange, or use of electronic health information due to a natural or human-made disaster, public health emergency, public safety incident, war, terrorist attack, civil insurrection, strike or other labor unrest, telecommunication or internet service interruption, or act of military, civil or regulatory authority.
2) Segmentation: The actor cannot fulfill the request for access, exchange, or use of EHI because the actor cannot unambiguously segment the requested EHI.
3) Infeasibility under the circumstances: The actor demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of certain factors that led to its determination that complying with the request would be infeasible under the circumstances.
4) The actor must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.

e) **Health IT Performance Exception**: It is not information blocking for an actor to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT, provided certain conditions are met. The practice must:

1) Be implemented for a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable or the health IT's performance degraded;
2) Be implemented in a consistent and non-discriminatory manner; and
3) Meet certain requirements if the unavailability or degradation is initiated by a health IT developer of certified health IT, HIE, or HIN.

<u>(2) Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.</u>

a) **Content and Manner Exception:** Addresses the specifics of what EHI content can be provided and the manner in which it is delivered when fulfilling requests.
b) **Fees Exception:** Details the conditions under which fees may be charged for accessing, exchanging, or using EHI, ensuring that any costs imposed are reasonable and fair.
c) **Licensing Exception:** Outlines how intellectual property related to interoperability elements for EHI can be licensed, balancing the protection of innovations with the need for access and use of EHI.

C. These exceptions pertain to specific operational, financial, and legal considerations that may not directly impact the day-to-day clinical operations or patient care activities at Stony Brook University Hospital. For actors seeking a more comprehensive understanding of all eight information blocking exceptions, including those related to procedural aspects of EHI requests a more detailed explanation of the CURES Act exceptions and
requirements can be found on the ONC website: Cures Act Final Rule: Information Blocking Exceptions (healthit.gov)
D. SBUH is committed to ensuring the confidentiality and security of patient information while adhering to federal and state regulations governing the access, exchange, or use of Electronic Health Information (EHI). As part of this commitment, the "Confidential-Non-Portal Note" type within the Cerner system is designated for use under specific circumstances that align with the exceptions to information blocking as outlined by the 21st Century Cures Act.
E. The Cures Act authorizes civil monetary penalties (CMPs) for any practice that is likely to interfere with, prevent, or discourage access, exchange, or use of EHI if the practice is conducted by an entity that is: a developer of certified health information technology (IT); offering certified health IT; a health information exchange (HIE); and the entity knows or that the practice is likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI.

2. **Use of the Confidential-Non-Portal Note Type Use:**

Once it is determined that an Information Blocking Rule exception applies, a "Confidential-Non-Portal Note" may be employed. This determination is a

critical first step to ensure compliance with regulatory requirements and protect patient interests.

A. SBUH Main Campus ONLY – Use of the Confidential-Non-Portal Note Type in Cerner
    a) For directions on specific ways to use the Confidential-non-portal note type please view Stony Brook Medicine – 21st Century Cures Act Technical FAQ. This document encompasses proper usage, ways to amend note types, and additional information on your role in complying with the CURES Act.
B. Stony Brook Southampton Hospital (SBSH) Campus ONLY - Use of the Confidential-Non-Portal Note Type in Soarian
    a) For directions specific ways to use the Confidential-non-portal note type please view How Do I Block a Note.
C. Stony Brook Eastern Long Island Hospital (SBELIH) Campus ONLY
    a) Medhost does not currently contain the capabilities for providers to use the confidential nonportal note-type.

3. **Monitoring:**
A. On a quarterly basis SBUH's Information Technology department provides OCAPS with a Crystal Report of all confidential note types utilized within the previous quarter for SBUH campus specific.
B. OCAPS reviews the report to identify risk areas and provide education to providers as necessary.

4. **Providing Access to Electronic Records Through Patient Portals**
A. Patient Portals are intended to give patients and their Personal Representatives immediate access to their health information. Therefore, EHI is made available on Patient Portals as promptly as possible.
B. For more information on obtaining/granting access to the patient portal please visit https://www.stonybrookmedicine.edu/MyHealtheLife

5. **Questions**
A. For questions about your role in complying with Information Blocking, contact OCAPS at 631-444-5864 Compliancehelp@stonybrookmedicine.edu , the Privacy Office at 631-444-5796 hipaa@stonybrookmedicine.edu or Information Security at InfoSec@stonybrookmedicine.edu.

B. For technical questions about how to pick a confidential non-portal note type Call the HELPDESK at 631-444-HELP (4357).
C. For questions relating to access to PHI please review the following policies:
    a. RC0008 – Patient Access to Protected Health Information
    b. RC0037 – Privacy Rights of Minors
    c. RC0065 – Personal Representative Access to Protected Health Information

Forms: (Ctrl-Click form name to view)

None

Policy Cross Reference: (Ctrl-Click policy name to view)

These cross-references supersede this policy in the event of a conflict between them.

RC0008 Patient Access to Protected Health Information

RC0037 Privacy Rights of Minors

RC0065 Personal Representative Access to Protected Health Information

IM0085 Information Security Policy

IM0086 Acceptable Use of IT Resources

IM0088 Requests for Data Containing Electronic Protected Health Information for External Purposes

Relevant Standards/Codes/Rules/Regulations/Statutes:

Tittle 45 CFR Part 171 – Information Blocking

References and Resources:

https://www.healthit.gov/topic/information-blocking