VNS HEALTH CORPORATE
POLICY & PROCEDURE

TITLE: Information Blocking Compliance

APPLIES TO: VNS Health Home Care, including the Home Care, and Care Management Organization (CMO) divisions;
VNS Health Personal Care;
VNS Health Behavioral Health, Inc.;
VNS Health Health Plans;
VNS Health Hospice Care; and
Medical Care at Home, P.C. (collectively, "VNS Health")

POLICY OWNER: Corporate Compliance Department

FIRST ISSUED: January 2022

NUMBER: HIPAA. 18

PURPOSE

The 21st Century Cures Act ("Cures Act") requires certain "Actors"—including Health Care Providers—not to take any action that constitutes "Information Blocking." A Health Care Provider engages in Information Blocking when it engages in a practice that

1. Except as required by law or covered by an Information Blocking exception, is likely to interfere with access, exchange, or use of Electronic Health Information ("EHI"); and

2. Such provider knows that such practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.

The VNS Health Programs are Health Care Provider Actors that are subject to this Information Blocking prohibition.

This Information Blocking Compliance Policy and Procedure, which applies to all VNS Health Programs, establishes general requirements for responding to requests to access, exchange, or use EHI made by any anyone outside of VNS Health in compliance with the Information Blocking Rule. These requests may be made, for example, by patients or their personal representatives (including attorneys), other health care providers, health plans, patient-facing apps, and life insurers. Requests for EHI and other protected health

information from patients or their personal representatives are also subject to the HIPAA.12, Access to Individual Information policy.[1]

POLICY AND PROCEDURE

I. DEFINITIONS

A. *Actor(s):* A term defined by the Information Blocking Rule that includes Health Care Providers, Health IT Developers of Certified Health IT, HINs, and HIEs. Actors are prohibited from engaging in Information Blocking.

B. *CMS:* The Centers for Medicare and Medicaid Services, which is part of HHS and oversees the federal Medicare and Medicaid programs.

C. *CMS Cures Act Final Rule:* The Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers Final Rule issued by CMS on May 1, 2020.

D. *Designated Record Set*: A group of records maintained by or for a VNS Health Program that (a) consists of a patient's medical records or billing records; or (b) is used, in whole or in part, by or for such VNS Health Program to make decisions about patients. Records maintained solely for quality improvement, patient safety, or business planning purposes generally will not be considered part of a VNS Health Program's Designated Record Set.

E. *Direct*: A protocol that allows EHI to be transmitted between different health care entities that functions similarly to a secure version of email.

F. *Electronic Health Information ("EHI")*: Electronic protected health information as defined under HIPAA (45 C.F.R. § 160.103) to the extent that it would be included in a designated record set as defined under HIPAA (45 C.F.R. § 164.501), regardless of whether the group of records are used or maintained by or for a covered entity as defined under HIPAA (45 C.F.R. § 160.103). However, EHI does not include: (a) psychotherapy notes, and (b) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. Prior to October 6, 2022, EHI only includes data elements represented by the United States Core Data

[1] As explained in the HIPAA.12, Access to Individual Information policy, "personal representative" includes parents and legal guardians, distributees of any deceased subject for whom no personal representative (as defined in the estates, powers and trusts law) has been appointed, or an attorney for any of the foregoing or for the patient's estate who holds a power of attorney explicitly authorizing the holder to execute a written request for the patient's information.

for Interoperability standard adopted at 45 C.F.R. § 170.213 ("USCDI"), which include, but are not limited to, patient demographics, allergies, immunizations, procedures, laboratory test results and values, medications, and clinical notes. A list of the USCDI data elements may be found at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.

G. *Electronic Health Record ("EHR"*): An electronic record of health-related information regarding a patient that can be created, gathered, managed, and consulted by authorized clinicians and staff within a single organization. VNS Health's EHR systems include Homecare Homebase ("HCHB"), eClinicalWorks, and Foothold.

H. *HHS:* The United States Department of Health and Human Services.

I. *Health Care Provider:* Defined in the Information Blocking Rule as including a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, healthcare clinic, community mental health center, renal dialysis facility, blood center, ambulatory surgical center, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician, a practitioner, a provider operated by, or under contract with, the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization, a rural health clinic, a covered entity under the 340B Drug Pricing Program, an ambulatory surgical center, and a therapist.

J. *Health IT Developer of Certified Health IT:* Defined in the Information Blocking Rule as an individual or entity, other than a Health Care Provider that self-develops health IT for its own use, that develops or offers health information technology (as that term is defined in 42 U.S.C. § 300jj(5)) and which has, at the time it engages in a practice that is the subject of an Information Blocking claim, one or more health IT modules certified under the ONC Health IT Certification Program.

K. *HIE ("Health Information Exchange") or HIN ("Health Information Network"):* An individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of EHI:

1. Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and

2. That is for a treatment, payment, or health care operations purpose, as such terms are defined under HIPAA (45 C.F.R. § 164.501) regardless of whether such individuals or entities are subject to HIPAA requirements (45 C.F.R. parts 160 and 164).

L. *HIPAA*: The Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended.

M. *Information Blocking*: With respect to Health Care Providers, a practice that – except as required by law or covered by an information blocking exception – (a) is likely to interfere with EHI and (b) the Health Care Provider knows is unreasonable and is likely to interfere with access, exchange, or use of EHI.

N. *Information Blocking Rule*: The Information Blocking provisions of the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule issued by ONC on May 1, 2020 and the Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID–19 Public Health Emergency Interim Final Rule With Comment Period issued by ONC on November 4, 2020, codified at 45 C.F.R. Part 171.

O. *MIPS:* The Merit-Based Incentive Payment System, which is an incentive program administered by CMS that monitors, rewards, and penalizes certain Health Care Providers participating in Medicare based on value and outcomes.

P. *NPPES:* The National Plan and Provider Enumeration System, which has been developed by CMS to assign unique identifiers to Health Care Providers and health plans.

Q. *ONC:* Office of the National Coordinator for Health IT, which is part of HHS and oversees the ONC Health IT Certification Program.

II. **GENERAL POLICY**: VNS Health Programs shall not engage in Information Blocking. Practices that could be considered Information Blocking include denying a legally permissible request for EHI when an Information Blocking exception does not apply, complying with such a request only in part, charging an unreasonable fee to fulfill a request, or unreasonably delaying a response to a request for EHI. However, a practice that does not meet the conditions of an Information Blocking exception does not automatically constitute Information Blocking. Instead, such practices will be evaluated on a case-by-case basis to determine whether Information Blocking has occurred.

III. **REVIEWING REQUESTS FOR EHI**: VNS Health Programs should review requests for EHI from patients and their personal representatives in accordance with the HIPAA.12, Access to Individual Information policy. VNS Health Programs should review all other requests for EHI according to the following 5-question analysis, which is reproduced in the diagram in Appendix A:

A. *Is the information being requested EHI?* If **no**, then the VNS Health Program may exercise discretion as to whether to comply with the request. If **yes**, then ask:

B. *Is disclosure of the requested information prohibited by law?* If **yes**, then the VNS Health Program should not provide the information. If **no**, then ask:

C. *Does an Information Blocking exception (Preventing Harm, Privacy, Security, Infeasibility, or Health IT Performance) allow the* VNS Health *Program to deny the request?* If **yes**, then the VNS Health Program may deny the request in accordance with the applicable exception. If **no**, then ask:

D. *Can the request be fulfilled in the manner requested?* If **yes**, then the VNS Health Program should fulfill the request in the manner requested. If **no**, then ask:

E. *Can the request be fulfilled in an alternative manner in accordance with the Information Blocking Content and Manner Exception?* If **yes**, then the VNS Health Program should fulfill the request in an alternative manner, complying with the Fees Exception (see Appendix B) and Licensing Exception, as applicable. If **no**, then the VNS Health Program should follow the "infeasible under the circumstances" requirements of the Infeasibility Exception as described under question C (but note that this option should be used only in rare instances when VNS Health is technically unable to provide the requested EHI in an alternative manner).

Each step of the analysis is explained in more detail below:

A. Is the information being requested EHI? The Information Blocking Rule applies only to EHI and not paper records (but note that paper records that have been scanned into PDF or another format and are available in electronic media typically will be considered EHI). In addition, electronic records not included in a Designated Record Set are not considered EHI and are therefore not subject to the Information Blocking Rule. Moreover, until October 6, 2022, EHI is limited to USCDI data elements. If a VNS Health Program receives a legally permissible request solely for records that are not EHI, then the VNS Health Program may exercise discretion as to whether to comply with the request.

B. Is disclosure of the requested information prohibited by law? The Information Blocking Rule does not require VNS Health Programs to provide access to EHI when applicable law prohibits them from doing so, and VNS Health Programs must ensure that any EHI disclosed is provided in compliance with applicable laws, including HIPAA. If applicable law prohibits disclosure of the requested information, the VNS Health Program shall not disclose it.

C. Does an Information Blocking exception allow the VNS Health Program to deny the request? There are five (5) Information Blocking exceptions that permit Actors to deny requests for EHI. These exceptions are summarized below; however, the requirements for each exception are detailed and complex, and all requirements specified for the applicable exception(s) in federal regulations at 45 CFR Part 171 must be met for the exception(s) to apply.

1. *Preventing Harm Exception:* This exception recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange, or use of EHI. The requirements of this exception are described in Appendix C.

2. *Privacy Exception:* This exception recognizes that if an Actor is permitted to provide access, exchange, or use of EHI under a privacy law, then the Actor should provide that access, exchange, or use. However, an Actor should not be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws. A VNS Health Program may satisfy this exception by meeting the requirements of one of the following sub-exceptions:

    (a) *Precondition not satisfied*: If the VNS Health Program is required by a state or federal law to satisfy a precondition (such as a patient consent or authorization) prior to providing EHI, the VNS Health Program may choose not to provide such EHI until the precondition has been satisfied. Denial of the request for failure to satisfy the precondition must be in accordance with the VNS Health Program's written organizational policies and procedures or documented on a case-by-case basis in a record that identifies the criteria used to determine when the precondition was satisfied, any criteria that were not met, and the reason why the criteria were not met. In the case of a lack of a legally required consent or authorization, the VNS Health Program must use reasonable efforts within its control to provide the individual with a consent or authorization form or provide other reasonable assistance to the individual to satisfy all required elements of the precondition. The VNS Health Program also must not improperly encourage or induce the individual to withhold the consent or authorization.

    (b) *Denial of an individual's request for their EHI consistent with 45 CFR 164.524(a)(1) and (2)*: A VNS Health Program may deny an individual's request for access to his or her EHI under the HIPAA right of access (45 CFR 164.524(a)(1)) in the circumstances provided under 45 CFR 164.524(a)(2) of the HIPAA Privacy Rule. See Section I.B.1 (Grounds for Denying Individual Access Without Review By Licensed Health Care Professional) of the HIPAA.12, Access to Individual Information policy for such circumstances that are applicable to VNS Health Programs.

(c) *Respecting an individual's request not to share information*: A VNS Health Program may choose not to provide access, exchange, or use of an individual's EHI if the individual has requested that the EHI not be disclosed without any improper encouragement or inducement by the VNS Health Program, and the VNS Health Program documents the request within a reasonable time period.

3. *Security Exception:* This exception allows Actors to deny requests for EHI to protect the security of the EHI under certain circumstances. This exception is intended to cover all legitimate security practices by Actors, but does not describe a maximum level of security or dictate a one-size-fits-all approach. For example, in certain cases, VNS Health Programs may deny a request for EHI if they have been unable to verify the requestor's identity through identity proofing requirements or if they have reasonable concerns about an IT vulnerability that may compromise the security of the EHI if disclosed. To satisfy the exception, a practice must (i) either implement a qualifying written organizational security policy or implement a qualifying security determination and (ii) be:

(a) Directly related to safeguarding the confidentiality, integrity, and availability of EHI;

(b) Tailored to specific security risks; and

(c) Implemented in a consistent and non-discriminatory manner.

4. *Infeasibility Exception:* This exception recognizes that legitimate practical challenges may limit an Actor's ability to comply with requests for EHI. An Actor 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. For example, this exception might apply if a legal entity that is unaffiliated VNS Health owns a particular program's records such that VNS Health does not have the authority to respond to requests for such records. To satisfy this exception, a VNS Health Program's practice must meet one of the following conditions:

(a) Uncontrollable events: The VNS Health Program cannot fulfill the request for EHI 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.

(b) Segmentation: The VNS Health Program cannot fulfill the request for EHI because the VNS Health Program cannot unambiguously segment the requested EHI from other EHI that either (i) cannot be made available due to an individual's preference or because the electronic health information cannot be made available by law or (ii) may be withheld in accordance with the Preventing Harm Exception. As an example, this condition may apply if the requested information cannot be segmented from records subject to federal substance abuse treatment confidentiality rules at 42 C.F.R. Part 2 that are not permitted to be disclosed.

(c) Infeasibility under the circumstances: The VNS Health Program demonstrates through a contemporaneous written record or other documentation its consistent and non-discriminatory consideration of the following factors that led to its determination that complying with the request would be infeasible under the circumstances:

- The type of EHI requested and the purposes for which it may be needed;
- The cost to the VNS Health Program of complying with the request in the manner requested;
- The financial and technical resources available to the VNS Health Program;
- Whether the VNS Health Program's practice is non-discriminatory and whether the VNS Health Program provides the same access, exchange, or use of EHI to others with whom the VNS Health Program has a business relationship;
- Whether the VNS Health Program owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged; and
- Why the VNS Health Program was unable to fulfill the request in accordance with the Content and Manner Exception (see questions D and E below).

Whenever a VNS Health Program denies a request for EHI under the Infeasibility Exception, the VNS Health Program must provide a written response to the requestor within ten (10) business days of receipt of the request with the reason(s) why the request is infeasible.

5. *Health IT Performance Exception:* This exception recognizes that for health IT to perform properly and efficiently, it must be maintained, and in some instances improved, which may require that health IT be taken offline temporarily. Actors should not be deterred from taking 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 health IT. To satisfy this exception, a VNS Health Program's practice must (i) be implemented for a period 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; and (ii) be implemented in a consistent and non-discriminatory manner. This exception also allows an Actor to take action against a third-party app that is negatively impacting the health IT's performance, provided that the practice is (i) for a period no longer than necessary to resolve any negative impacts; (ii) implemented in a consistent and non-discriminatory manner; and (iii) consistent with existing service level agreements, if applicable.

D. Can the request be fulfilled in the manner requested? There are three (3) Information Blocking exceptions that specify procedures for fulfilling requests for EHI: The Content and Manner Exception, the Fees Exception, and the Licensing Exception. The Content and Manner Exception provides that an Actor may fulfill a request for EHI "in the manner requested" without needing to comply with the Fees Exception or Licensing Exception. In other words, a VNS Health Program may provide all EHI requested in the manner that the requestor has requested it, or may negotiate agreed terms with the requestor to provide the requested EHI. For example, a VNS Health Program may fulfill a request for EHI by providing EHI via secure email (with a link and instructions to download a PDF) or fax via VNS Health's email-to-fax solution if the requestor has requested that the information be provided in that manner. As another example, a VNS Health Program may provide EHI via an HIE such as Healthix if the requestor is a participant in such HIE and agrees to receive the EHI in such manner.

If requested records are maintained electronically and the requestor requests the records electronically, VNS Health will provide the requestor copies of the records in the electronic form and format requested by the requestor, if readily producible. If the VNS Health Program cannot fulfill the request in the manner requested, it may be necessary to fulfill the request in an alternative manner (see below).

E. Can the request be fulfilled in an alternative manner in accordance with the Information Blocking Content and Manner Exception? The Content and Manner Exception permits an Actor to fulfill a request for EHI in an "alternative manner" if the Actor is technically unable or cannot reach agreement with the requestor to

fulfill the request in the manner requested. The Actor must fulfill the request in the first of the following alternative manners that it is technically able to support:

1. Using certified health IT specified by the requestor (such as Certified Electronic Health Record Technology ("CEHRT"));

2. Using content standards (e.g., FHIR, HL7 V2.5.1) and transport standards (e.g., Direct Project Standard ONC Applicability Statement for Secure Health Transport, Version 1.0) specified by the requestor and published by the federal government or a standards developing organization accredited by the American National Standards Institute; or

3. Using an alternative machine-readable format (such as a CSV, JSON, or XML file), including the means to interpret the electronic health information, agreed upon with the requestor.

When fulfilling a request for EHI in an alternative manner, the Content and Manner Exception requires that any fees the Actor charges must comply with the Fees Exception, and any licenses to technology or intellectual property used to access EHI must comply with the Licensing Exception. VNS Health has adopted the fee parameters in Appendix B to help ensure that any fees that VNS Health Programs charge for EHI comply with the Fees Exception. Note that as stated on Appendix B and in the HIPAA.12 Access to Individual Information policy, patients and their personal representatives should not be charged for electronic access to their information through internet-based methods that do not require manual effort, including without limitation through email, personal health apps, and standalone/untethered personal health records. It is unlikely that VNS Health Programs would need to license technology or intellectual property that would be subject to the Licensing Exception; however, if such licensing is required, the VNS Health Program should consult with the Corporate Compliance Department and the Legal Department.

IV. DOCUMENTATION OF REQUESTS FOR EHI

A. VNS Health Programs must keep the following documentation in connection with any request for EHI subject to this policy. These documents must be maintained by VNS Health Programs for six years from the date on which the request was fulfilled or denied.

1. The request for EHI, either in its original form or a notation if the request was not made in writing.

2. Copies of any notices advising that a fee may be charged.

3. Information about any EHI provided in response to the request.

4. A copy of any notice of denial provided in response to the request.

5. The titles of the persons or offices responsible for receiving and processing requests for EHI.

6. Whenever a VNS Health Program discloses patient information to a third party requestor, either a copy of the patient's written authorization or the name and address of the requestor and a notation for the purpose of the disclosure should be appended to the patient's medical or member record or scanned or uploaded into the medical record, depending on how the record is maintained. For disclosures made to government agencies making payments on behalf of patients or to insurance companies licensed pursuant to the insurance law, such a notation shall only be entered at the time the disclosure is first made. This requirement does not apply to disclosure to practitioners or other personnel employed by or under contract with a VNS Health Program, or to government agencies for purposes of facility inspections or professional conduct investigations.

B. VNS Health Programs should respond to requests for EHI by patients or their personal representatives in one of the Sample Letter formats included in the HIPAA.12, Access to Individual Information policy.

C. VNS Health Programs should respond to requests for EHI by requestors who are not patients or their personal representatives in one of the Sample Letter formats included in Appendix D.

V. PRACTICES UNRELATED TO SPECIFIC REQUESTS

A. While the Information Blocking Rule typically will be applicable in cases where a VNS Health Program receives a specific request for EHI, any practice that interferes with access, exchange or use of EHI—not just practices that are triggered in response to specific requests for EHI—potentially implicates the Information Blocking Rule. Some examples of actions that VNS Health Programs can take to mitigate Information Blocking risk prospectively include the following, in each case to the extent feasible:

1. Configure EHR systems to receive electronic messages from patients and providers.

2. Do not configure EHR systems to make it more difficult to send EHI to competing providers than to affiliated providers.

3. Configure EHR systems to disclose EHI in a standard, contemporary format.

4. Encourage sharing of EHI with other providers for treatment and health care operations purposes.

VI. <u>INFORMATION BLOCKING COMPLIANCE PROCEDURES</u>: Each VNS Health Program will take the following steps to facilitate Information Blocking compliance:

A. Inform its workforce members about this Policy as it applies to the VNS Health Program generally and workforce members in their individual roles.

B. Coordinate with health IT vendors to identify and implement (if not already in place) health IT solutions and workflows that can be used to support responses to EHI access requests from other providers, patients, third-party apps, health IT vendors, and others in accordance with Information Blocking requirements.

C. Review existing policies and procedures for receiving, processing, and responding to requests to access, exchange, or use EHI and revise them as necessary to ensure compliance with federal Information Blocking requirements. In undertaking such review, the VNS Health Program should consider whether a particular practice is required by law, falls within an Information Blocking exception and is reasonable given industry standards, the VNS Health Program's resources, and the costs and burdens of modifying such practice. The VNS Health Program may consider whether changing a practice would be unreasonably costly in determining whether to modify its processes. Implementing this Policy may require:

1. Reviewing any fees charged to other providers, patients, third-party apps, health IT vendors, and others for EHI access, exchange or use to ensure compliance with Information Blocking requirements (see Appendix B for recommended fee parameters);

2. Conducting an inventory of how the VNS Health Program stores and transmits EHI;

3. Developing policies and procedures for responding to requests for EHI from other providers, patients, third-party apps, health IT vendors, and others. This may include creating forms for receiving, processing, and responding to such requests and procedures specifying of how access to EHI may be provided; and

4. Reviewing data use, business associate, and other agreements governing the sharing of EHI to ensure compliance with Information Blocking requirements.

D. Verify the current status of secure digital endpoints,[2] such as a Direct Address[3] and/or a FHIR API endpoint, and ensure that digital contact information, such as FHIR service based URLs and Direct Addresses, is publicly accessible through the NPPES database.[4]

E. Conduct a review of the interoperability of its EHR technology, as well as the relevant standards, policies, practices, and agreements related to the EHR technology to confirm the ability of any MIPS-participating providers to attest "yes" to all of the MIPS Information Blocking attestation statements.[5]

VII. INFORMATION BLOCKING REVIEW PROCESS: To implement this policy and facilitate information blocking compliance, VNS Health will convene an Information Blocking Review Workgroup ("Workgroup"). The Workgroup will consist of employees from the VNS Health Legal, Compliance, Medical Records, and IT departments and other departments as needed. The Workgroup will be responsible for reviewing VNS Health's business operations to determine necessary information blocking compliance steps. The Workgroup will designate members to monitor and triage information blocking compliance questions and requests to access, exchange, and use EHI. These team members will be responsible for circulating issues to other Workgroup members as needed. The Workgroup may call upon additional resources or subject matter experts from other VNS Health teams and divisions in addressing information blocking issues. All VNS Health resources and subject-matter experts with whom the Workgroup consults in connection with an information blocking inquiry shall cooperate with the Workgroup's review. Inquiries that contain time-sensitive issues will take priority over other matters reported via the queue. The specific priority of each reported issue will be left to the discretion of the Workgroup.

VIII. INFORMATION BLOCKING COMPLAINT PROCESS: Information Blocking compliance concerns may be filed with VNS Health in accordance with the HIPAA.8 Internal HIPAA Complaints and Sanctions for Violations policy or through VNS Health's anonymous hotline and compliance reporting tool available at https://www.vnshealth.org/corporate-compliance-privacy/vns-health-compliance-program/reporting-a-compliance-concern/. All concerns will be investigated in accordance with the HIPAA.8 Internal HIPAA Complaints and Sanctions for Violations policy.

---

[2] More information about endpoints can be found at https://www.hl7.org/fhir/endpoint.html.

[3] More information about Direct Address can be found at https://www.healthit.gov/sites/default/files/directbasicsforprovidersqa_05092014.pdf.

[4] Providers can review their information using the NPPES NPI Registry (https://npiregistry.cms.hhs.gov/), the NPPES NPI Registry API (https://npiregistry.cms.hhs.gov/registry/help-api), or the NPPES Data Dissemination file (https://www.cms.gov/Regulations-and-Guidance/AdministrativeSimplification/NationalProvIdentStand/DataDissemination). CMS will report providers who do not list or update their digital contact information in the NPPES. *See* CMS Cures Act Final Rule, 85 Fed. Reg. 25,510, 25,680–84 (May 1, 2020).

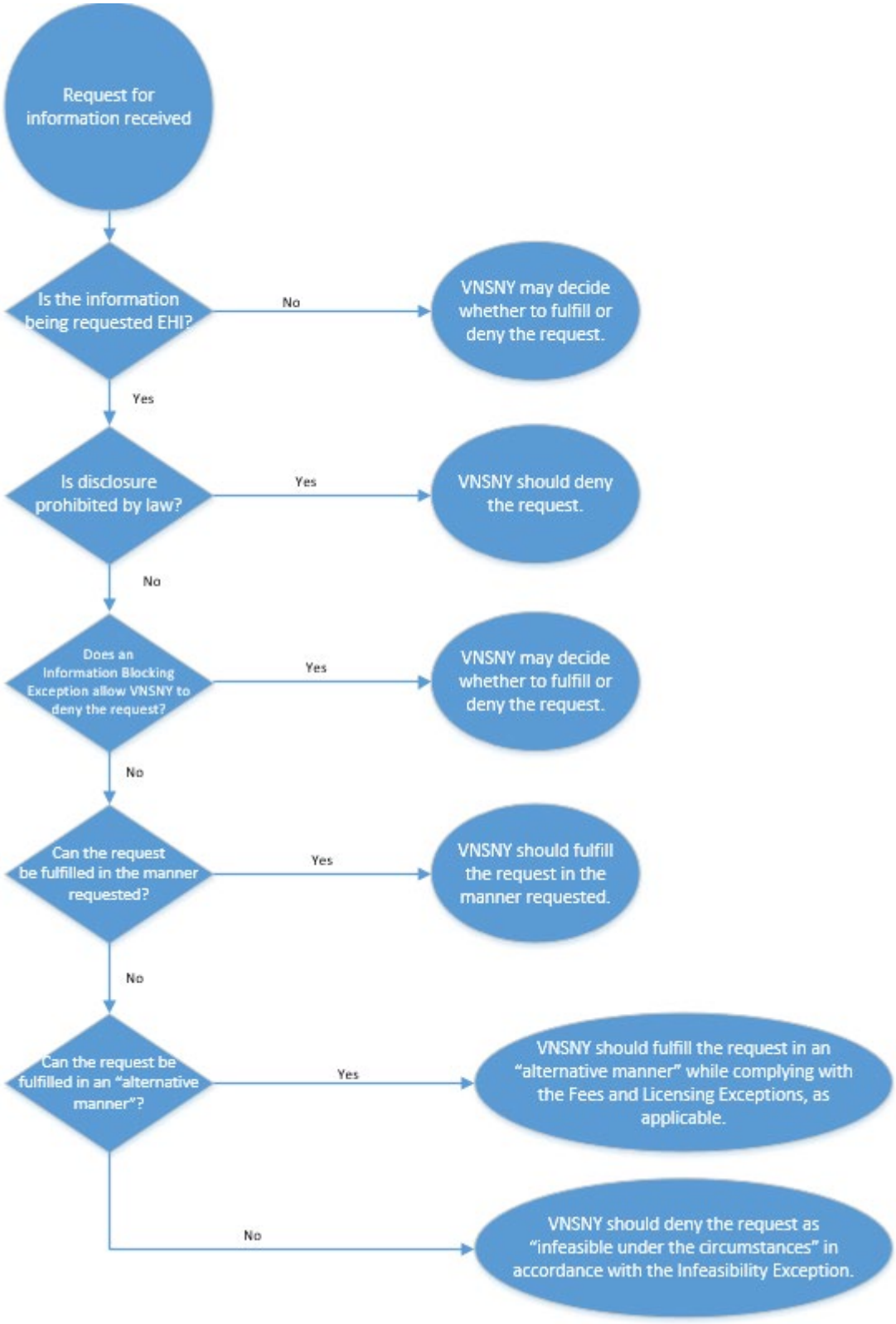
[5] The attestations for clinicians can be found at 42 C.F.R. § 414.1375(b)(3)(ii)(A)–(C). The attestations for hospitals can be found at 42 C.F.R. § 495.40(b)(2)(i)(I)(1)–(3). Pursuant to the CMS Cures Act Final Rule, CMS will publicly list providers who submit "no" as a response to any of the three MIPS Information Blocking attestation statements.

IX. **ENFORCEMENT AND SANCTIONS**: VNS Health Program personnel will be assessed on adherence to this Policy. Failure to comply may lead to disciplinary action in accordance with the HIPAA.8 Internal HIPAA Complaints and Sanctions for Violations Policy.

REFERENCES: 45 CFR Part 170 Subpart D, Part 171

Reviewed:	January 2022 (NEW)	3/2022	6/2023					
Revised & Approved:	1/2022	6/2022	9/2023					
Reviewed:								
Revised & Approved:								

Appendix A:
Analysis for Reviewing Requests for EHI



Appendix B:

Fee Parameters

To comply with the Fees Exception to Information Blocking, any fees that VNS Health Programs charge for access, exchange, or use of EHI should be:

1. Based on objective and verifiable criteria that are uniformly applied for all similarly situated classes of persons or entities and requests;
2. Reasonably related to the VNS Health Program's costs of providing the type of access, exchange, or use of EHI to, or at the request of, the person or entity to whom the fee is charged;
3. Reasonably allocated among all similarly situated persons or entities to whom the technology or service is supplied, or for whom the technology is supported;
4. Based on costs not otherwise recovered for the same instance of service to a provider or third party;
5. Not based on whether the requestor or other person is a competitor, potential competitor, or will be using the EHI in a way that facilitates competition with the VNS Health Program;
6. Not based on sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access, exchange, or use of the EHI;
7. Not based on costs the VNS Health Program incurred due to the health IT being designed or implemented in a non-standard way, unless the requestor agreed to the fee associated with the non-standard design or implementation to access, exchange, or use the EHI;
8. Not based on costs associated with intangible assets other than the actual development or acquisition costs of such assets;
9. Not based on opportunity costs unrelated to the access, exchange, or use of EHI; and
10. Not based on any costs that led to the creation of intellectual property ("IP"), if the VNS Health Program charged a royalty for that IP pursuant to the Licensing Exception to Information Blocking and that royalty included the development costs for the creation of the IP.

In addition, VNS Health should not charge the following "excluded fees" that are never protected by the Fees Exception:

A. A fee charged for a patient's electronic access to his or her information through internet-based methods that do not require manual effort, including without limitation through personal health apps, standalone/untethered personal health records, and email.

B. A fee charged for a patient's access to his or her EHI in physical media (such as paper copies), CD, or flash drive formats, unless such fees comply with the requirements for reasonable, cost-based fees under HIPAA (45 C.F.R. § 164.524(c)(4)). VNS Health may charge patients reasonable, cost-based fees for access to their health information in such formats as provided in the HIPAA.12, Access to Individual Information policy.

C. A fee to export EHI from one or more health IT systems via the capability of the system certified to the EHI export certification criterion (45 C.F.R. § 170.315(b)(10)) for the purpose of transitioning from the VNS Health Program's health IT to an alternate health IT or electronic health record system (to the extent applicable).

D. A fee to export or convert data from an EHR technology licensed or otherwise offered by a VNS Health Program, unless a fee for such data export or conversion was specified in the customer's

initial contract with the VNS Health Program when the customer first acquired the EHR technology (to the extent applicable).

Appendix C:

Requirements of the Preventing Harm Exception

1. The VNS Health Program must hold a reasonable belief that the practice will substantially reduce a risk of harm to a patient or another natural person;

2. The VNS Health Program's practice must be no broader than necessary to substantially reduce the risk of harm;

3. Type of risk. The risk of harm must:

    a. Be determined on an individualized basis in the exercise of professional judgment by a licensed health care professional who has a current or prior clinician-patient relationship with the patient whose EHI is affected by the determination ("Professional's Individualized Determination of Harm"); *or*

    b. Arise from data that is known or reasonably suspected to be misidentified or mismatched, corrupt due to technical failure, or erroneous for another reason ("Erroneous or Corrupted Data").

4. Type of harm. The type of harm must be one of the following:

    a. In the case of a request by the patient's personal representative or other legal representative, reasonably likely substantial harm to the patient or another person, as determined pursuant to a Professional's Individualized Determination of Harm;

    b. In the case of a request by the patient or his or her personal representative or other legal representative, if the requested EHI references a person other than the patient, reasonably likely substantial harm to such other person, as determined pursuant to a Professional's Individualized Determination of Harm;

    c. In the case of a request by the patient, reasonably likely endangerment of the life or physical safety of the patient or another person, as determined pursuant to a Professional's Individualized Determination of Harm or due to Erroneous or Corrupted Data.

    d. In the case of any other legally permissible request, reasonably likely endangerment of the life or physical safety of the patient or another person, as determined pursuant to a Professional's Individualized Determination of Harm or due to Erroneous or Corrupted Data.

5. The practice must be implemented based on an organizational policy or a determination specific to the facts and circumstances.

    a. An organizational policy must (i) be in writing; (ii) be based on relevant clinical, technical, and other appropriate expertise; (iii) be implemented in a consistent and non-discriminatory manner; and (iv) conform each practice to the applicable requirements of the Preventing Harm Exception described above.

    b. A determination must (i) be based on facts and circumstances known or reasonably believed by the VNS Health Program at the time the determination was made and while the practice remains in use; and (ii) be based on expertise relevant to implementing

the practice consistent with applicable requirements of the Preventing Harm Exception described above.

6. A patient may have the right under applicable law to request review of a Professional's Individualized Determination of Harm.

Appendix D:

Sample Letters

VNS Health

Denial Letter to Third Party Requestor

[Date]

Via Certified Mail
Requestor Name and Address

Re: Denial of Request for Access of Electronic Health Information for Patient/Member
Medical Record Number: _____

Dear_____:

Thank you for submitting your request to access the information referenced above. We received your request on _____ [insert date]. The Privacy Office has reviewed and is denying your request because:

- ☼ The information you are trying to access is not electronic health information that you have a right to access.[6]
- ☼ Federal or state law prohibits disclosure of this information to you.[7]
- ☼ We have denied your request in accordance with 45 C.F.R. § 171.201.[8]
- ☼ You did not provide a signed authorization from the individual for disclosure of the information to you that complies with applicable law. An authorization form that the individual can use to authorize disclosure of the information to you is available online at https://www.health.ny.gov/health_care/medicaid/redesign/docs/mltc_policy_13-24.pdf. [9]
- ☼ The following legally required precondition for disclosure of the information to you has not been satisfied: _____.[10]
- ☼ The individual has requested that we not disclose this information to you.[11]
- ☼ We were unable to verify your identity.[12]
- ☼ We have denied your request to safeguard the confidentiality, integrity, and availability of the information requested from a specific security risk.[13]
- ☼ We are unable to fulfill your request due to the following uncontrollable event: _____.[14]
- ☼ We are unable to unambiguously segment the requested information from information that cannot be made available due to legal requirements or the individual's preference.[15]
- ☼ We are unable to unambiguously segment the requested information from information withheld in accordance with 45 C.F.R. § 171.201.[16]

---

[6] See Section III.A of the Information Blocking Compliance Policy.
[7] See Section III.B of the Information Blocking Compliance Policy.
[8] See Section III.C.1 of the Information Blocking Compliance Policy (Preventing Harm Exception).
[9] See Section III.C.2(a) of the Information Blocking Compliance Policy (Privacy Exception).
[10] See Section III.C.2(a) of the Information Blocking Compliance Policy (Privacy Exception).
[11] See Section III.C.2(c) of the Information Blocking Compliance Policy (Privacy Exception). Section III.C.2(b) is applicable to a request by an individual or his or her personal representative and is therefore addressed in the HIPAA.12, Access to Individual Information policy.
[12] See Section III.C.3 of the Information Blocking Compliance Policy (Security Exception).
[13] See Section III.C.3 of the Information Blocking Compliance Policy (Security Exception).
[14] See Section III.C.4(a) of the Information Blocking Compliance Policy (Infeasibility Exception).
[15] See Section III.C.4(b) of the Information Blocking Compliance Policy (Infeasibility Exception).
[16] See Section III.C.4(b) of the Information Blocking Compliance Policy (Infeasibility Exception).

- ☼ We do not maintain this information. Instead, you can contact: [name and address of the health care provider who does maintain the information]. [17]
- ☼ The record no longer exists or cannot be found.[18]
- ☼ Fulfilling your request is infeasible under the circumstances for the following reasons: _____.[19,20]

You may file a complaint with VNS Health by contacting the Privacy Office at the address above or by calling (212) 609-7884.

Sincerely,

VNS Health Medical Records Department

[17] See Section III.C.4(c) of the Information Blocking Compliance Policy (Infeasibility Exception).
[18] See Section III.C.4(c) of the Information Blocking Compliance Policy (Infeasibility Exception).
[19] See Section III.C.4(c) of the Information Blocking Compliance Policy (Infeasibility Exception). When using this option, provide an explanation of why fulfilling the request is infeasible under the circumstances, considering the factors specified in Section III.C.4(c).
[20] We have not included any options for the Health IT Performance Exception (Section III.C.5) because that exception is not applicable to this type of denial.

Letter of Acceptance to Third Party Requestor (Paper or Encrypted Flash Drive) – Payment Not Yet Received

[Date]

Via Certified Mail
Requestor Name and Address

Re: Acceptance of Request for Access of Electronic Health Information for Patient/Member Record Number _____

Dear_____:

Thank you for submitting your request to access the information referenced above, which was received [insert date]. The Privacy Office has reviewed and is hereby granting your request.

A cost-based fee of [$0.75 per page] [$6.50 for an encrypted flash drive that contains the information] has been assessed for copying the information you requested. The associated cost of your request is: .

Enclosed please find a copy of the requested information and an invoice for the services stated above. Please provide a check or money order payable to VNS Health for the amount of _____ and submit it to the following address: _____
_____
_____.

Thank you for yourcooperation.

Sincerely,

VNS Health Medical Records Department

VNS Health

Letter of Acceptance to Third Party Requestor (Electronic Health Information in Other Format) – Payment Not Yet Received

[Date]

Via Certified Mail
Requestor Name and Address

Re: Acceptance of Request for Access of Electronic Health Information for Patient/Member Record Number _____

Dear_____:

Thank you for submitting your request to access the information referenced above, which was received on _____ [insert date]. The Privacy Office has reviewed and is hereby granting your request, as specified herein. The information you requested is now available for you in the following format [that you requested][21]: _____

[Consistent with our prior communications with you regarding your request, we have provided the information you requested in the manner above because we were technically unable or could not reach agreement with you to provide the information in the manner you requested.][22]

You can access the information by _____.

[A cost-based fee of $_____ has been assessed for providing the information you requested.

Please provide a check or money order payable to VNS Health for the amount of _____ and submit it to the following address: _____
_____.][23]

Thank you for your

cooperation.

Sincerely,

VNS Health Medical Records Department

[21] Include the bracketed clause if you are providing the EHI in the manner that it was requested.
[22] Include the bracketed clause if you are providing the EHI in an alternative manner. Please refer to the VNS Health Information Blocking Compliance Policy for a list of permissible alternative manners in which EHI may be provided.
[23] Include the bracketed clause if charging a fee. However, as explained in the Information Blocking Compliance Policy, VNS Health should not charge an individual for electronic access to his or her information through internet-based methods that do not require manual effort, including without limitation through personal health apps, standalone/untethered personal health records, and email.

VNS Health

Letter of Acceptance to Third Party Requestor (Paper or Encrypted Flash Drive) – Payment Received

[Date]

Via Certified Mail
Requestor Name and Address

Re: Acceptance of Request for Access of Electronic Health Information for Patient/Member Record Number _____

Dear_____:

Thank you for submitting your request to access the information referenced above, which was received _____ [insert date]. The Privacy Office has reviewed and is hereby granting your request.

A cost-based fee of [$0.75 per page] [$6.50 for an encrypted flash drive that contains the information] has been assessed for copying the information you requested. The associated cost of your request is: . We hereby confirm receipt of your payment of this amount.

Sincerely,

VNS Health Medical Records Department

Letter of Acceptance to Third Party Requestor (Electronic Health Information in Other Format) – Payment Received

[Date]

Via Certified Mail
Requestor Name and Address

Re: Acceptance of Request for Access of Electronic Health Information for Patient/Member Record Number _____

Dear_____:

Thank you for submitting your request to access the information referenced above, which was received on _____ [insert date]. The Privacy Office has reviewed and is hereby granting your request, as specified herein. The information you requested is now available for you in the following format [that you requested][24]: _____

[Consistent with our prior communications with you regarding your request, we have provided the information you requested in the manner above because we were technically unable or could not reach agreement with you to provide the information in the manner you requested.][25]

You can access the information by _____.

[A cost-based fee of $_____ has been assessed for providing the information you requested. We hereby confirm receipt of your payment of this amount.][26]

Sincerely,

VNS Health Medical Records Department

[24] Include the bracketed clause if you are providing the EHI in the manner that it was requested.
[25] Include the bracketed clause if you are providing the EHI in an alternative manner. Please refer to the VNS Health Information Blocking Compliance Policy for a list of permissible alternative manners in which EHI may be provided.
[26] Include the bracketed clause if charging a fee.

VNS Health

Requesting Extension from Third Party Requestor[27]

[Date]

Via Certified Mail
Requestor Name and Address

Re: Need for Extension in Processing Request for Access of Electronic Health Information for Patient/Member Record Number _____

Dear_____:

Thank you for submitting your request to access the information referenced above, which was received on _____ [insert date].

We are notifying you of the need for a thirty (30) day extension in processing your request for access to the information. This extension is necessary for the following reason(s):

(Insert Explanation/Reason for Extension)

We will notify you of our decision about your request within the next thirty (30) days.

Sincerely,

VNS Health Medical Records Department

[27] Only use this template when VNS Health *cannot* fulfill the request within the original timeframe. Delaying responses when it is not necessary to do so may pose Information Blocking risk. Also note that the Infeasibility Exception to Information Blocking requires you to respond to the requestor within 10 business days if you deny the request due to infeasibility in accordance with the exception.