NYeC
NEW YORK eHEALTH COLLABORATIVE

Valerie Grey
Chief Executive Officer

April 14, 2021

Office for Civil Rights
U.S. Department of Health and Human Services
Hubert H. Humphrey Building, Room 509F
200 Independence Ave SW
Washington, DC 20201

RIN 0945-AA00: *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement*

Dear Acting Director Robinsue Frohboese,

The New York eHealth Collaborative (NYeC) is pleased to provide these comments in response to the Proposed Modifications to the HIPAA Privacy Rule to Support and Remove Barriers to Coordinated Care and Individual Engagement (Proposed Rule).

NYeC is a 501(c)(3) and New York's State Designated Entity (SDE) charged with the governance, coordination, and administration of the Statewide Health Information Network for New York (SHIN-NY). In this capacity, NYeC works in a public/private partnership with the New York State Department of Health (NYS DOH) on the development of policies and procedures that govern health information exchange through the SHIN-NY. The SHIN-NY is a "network of networks" consisting of six Qualified Entities (QEs) also known as Regional Health Information Organizations (RHIOs) and a statewide connector that facilitates secure sharing of clinical data from participating providers' electronic health records (EHRs). The SHIN-NY is a public utility that connects all hospitals in the state, is used by over 100,000 healthcare professionals, and serves millions of people who live in or receive care in New York.

As a leader in New York State (NYS), the SHIN-NY has created a strong statewide foundation for health IT and interoperability. We support the Office for Civil Rights' (OCR) goals in this Proposed Rule to remove perceived barriers to coordinated care and enhance the individual right of access. Health Information Exchanges (HIEs) and Health Information Networks (HINs), like the SHIN-NY, have a proven history of facilitating HIPAA permitted disclosures, including individual access to their health information. Our comments reflect this experience and urge additional regulatory clarity, coordination, and guidance to prevent future confusion. Highlights of our comments include:

- **Disclosures to Personal Health Applications – Request for Comment[1]:** In response to OCR's request for comment, NYeC believes that OCR should explicitly permit and encourage both covered health plans and providers to warn or notify individuals of the risks of sharing their EHI with a non-HIPAA personal health application before fulfilling an access request to that app. Such a permission would better inform individuals of the risks of sharing their data outside of the HIPAA framework. We believe it is a best practice and we urge the Department to

[1] 86 FR 6469, o and p

coordinate with the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health IT (ONC) to align such permissions across all covered health plans and providers, as well as CMS regulated health plans and actors subject to information blocking.

- **Addressing the Individual Access Right to Direct Copies of PHI to Third Parties – 45 CFR 164.524(d)(1)— and Adding Definitions for Electronic Health Record (EHR) and Personal Health Application – 45 CFR 164.501:** If OCR finalizes its proposal to limit the definition of EHR to PHI "created, gathered, managed, and consulted by authorized clinicians and staff," then NYeC suggests that OCR permit and encourage covered entities (CEs) and business associates (BAs) to also include PHI from health plans, if available, when responding to third-party directives.

- **Individual Access Right to Direct Copies of Protected Health Information (PHI) to Third Parties — 45 CFR 164.524(d)(7):** NYeC supports the newly proposed right for an individual to direct covered health care providers or health plans to submit an access request and believes HIEs can help to facilitate that access. NYeC agrees with OCR's interpretation that §164.506(c)(1) permits covered entities (CEs) to disclose PHI to HIEs to perform "broadcast queries" as part of a CE's own health care operations purposes[2], but cautions that this might conflict with some business associate agreements (BAAs) that prohibit business associates (BAs) from making disclosures in response to patient access requests to anyone other than the participant who is the source of the data. OCR can clarify this interpretation, and correct other misunderstandings about HIEs, by fulfilling the directive under the 21st Century Cures Act (Cures Act) for the Department for Health and Human Services (HHS) to educate health care providers on ways of leveraging the capabilities of HIEs to provide patients with access to their health information.[3]

- **Disclosure of PHI to Social Service Agencies for Individual-Level Care Coordination and Case Management that Constitutes Treatment or Health Care Operations — 45 CFR 164.506:** NYeC applauds OCR for seeking to encourage disclosures of PHI to social service agencies, community-based organizations (CBOs), home and community-based services (HCBS), and other similar third parties that provide health-related services (collectively referred to as CBOs), and has the following comments:
  - Rather than adding a new §164.506(c)(6) that narrows the permissible disclosure to individual-level care coordination and case management, NYeC suggests that OCR modify the existing §164.506(c)(1) to explicitly state that disclosures under (c)(1) may include but are not limited to disclosures to CBOs for care coordination and case management.
  - OCR should clarify that a CE may disclose PHI to a CBO that provides health related services for the CBO's *own* care coordination and case management activities even when the CBO is not a CE.

[2] 86 FR 6464
[3] 42 U.S.C 300jj-19(c)

- OCR should clarify their past guidance[4] on disclosures to CBOs to make clear that BAs (including HIEs) are permitted to disclose PHI on the CE's behalf for a HIPAA covered purpose without an individual authorization, as long as the Business Associate Agreement (BAA) permits the disclosure. OCR should also consider amending the title of this guidance to clarify that it addresses disclosures to CBOs.
- OCR could help address provider concerns about CBO disclosures if it issued guidance on ways that providers can securely transmit and ensure confidentiality of data disclosed to CBOs.
- To prevent confusion and variable interpretation across the industry, OCR should consider defining "health-related services" or developing guidance to expand on the examples of "health-related services" in the Proposed Rule.

- **Amending the Definition of Health Care Operations — 45 CFR 164.501:** NYeC supports OCR's proposal to clarify that the definition of health care operations encompasses all care coordination and case management by health plans, whether individual-level or population-based. In order to clarify any ambiguity, NYeC suggests adding the words "individual-level or population based" in front of the words "care coordination and case management" within the newly proposed definition.

- **Timely Action in Response to Requests for Access — 45 CFR 164.524(b):** NYeC supports OCR's proposal to modify §164.524(b)(2)(i) and (ii) to require that access be provided "as soon as practicable," but in no case later than 15 calendar days after receipt of the request, with the possibility of one 15 calendar-day extension.

- **Adjusting Permitted Fees for Access to PHI and ePHI — 45 CFR 164.524(c) and (d):** NYeC applauds OCR for seeking to re-instate fee limitations ("patient rate") for third party directives. However, NYeC believes that the patient rate should include fees for the supplies for making electronic copies of PHI and the actual postage and shipping for sending electronic copies of PHI through a non-internet-based method.

NYeC looks forward to continued collaboration with OCR and the larger Department of HHS in facilitating secure access to patient health information and improving healthcare delivery and the health of our communities.

Sincerely,

Valerie Grey

Chief Executive Officer (CEO)
New York eHealth Collaborative

[4] See Office of Civil Rights, 3008-Does HIPAA permit health care providers to share PHI about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes? https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html

Detailed Comments

Disclosures to Personal Health Applications — Request for Comment (o and p)

OCR requests comment on whether to require covered providers and/or health plans to provide education, notice, or warnings to individuals who request to share their Protected Health Information (PHI) with a non-HIPAA regulated personal heath application. We note that CMS released a Notice of Proposed Rule Making (NPRM)[5] in December 2020 that proposed to require that Medicaid and CHIP managed care and fee-for-service plans, as well as Qualified Health Plans on the Federally Facilitated Exchanges maintain a process for requesting that third party apps adhere to certain privacy practices prior to sending them Electronic Health Information (EHI) on behalf of an individual.[6]

We agree with the intent behind both CMS and OCR's proposals and believe there should be an explicit permission for both health plans and providers to conduct such warnings. Such a permission would further inform individuals of the risks of sharing their Protected Health Information (PHI) outside of the HIPAA framework. However, we urge OCR and CMS to coordinate with each other to align permissions across all covered health plans and providers. As HIPAA regulates the broader health plan and provider community, we believe it is appropriate for such a permission to fall within HIPAA, as opposed to a CMS regulation.

In addition, if OCR finalizes a warning or attestation requirement for covered health care providers under HIPAA, then such practice by health care providers would likely not be considered information blocking under ONC's Information Blocking Rule[7] since activities required by law are excepted from the definition of information blocking.[8] NYeC believes that this same protection should apply to other actors subject to ONC's Information Blocking Rule, including Health Information Exchanges/Health Information Networks (HIEs/HINs) and Health IT Developers.

While we are aware that ONC's Rule states that actors may educate or warn individuals about the risk of sharing EHI with third party apps, we also understand that an actor may not prevent an individual from deciding to provide its EHI to a third-party app despite any risks noted.[9] It is unclear at what point such a "vetting" or education practice becomes an undue delay that could implicate information blocking. OCR could work with ONC to clarify this by providing guidance or an FAQ that points to OCR's requirement for CEs as a permissible practice for all actors under information blocking.

Such alignment makes sense from a patient perspective: if the attestation or warning requirement results in a particular patient telling a CE not to share their data with a particular app, then presumably that patient would not want their HIE/HIN to share data with that app either. It is critical to promote alignment and consistency across and between healthcare entities subject to different regulatory authorities in order to reduce confusion from consumers to providers and health plans. As such, the rules that apply to CEs under HIPAA should be consistent with the rules that apply to HIEs/HINs and other actors subject information blocking.

---

[5] 85 FR 82586

[6] The rule was finalized on January 15 but was never published in the Federal Register. It is currently subject to a regulatory freeze; whether it will be published in some form remains to be seen.

[7] 85 FR 25642-25961

[8] 45 CFR 171.103

[9] 85 FR 25814-25817

Addressing the Individual Access Right to Direct Copies of PHI to Third Parties — 45 CFR 164.524(d)(1) and Adding Definitions for Electronic Health Record (EHR) and Personal Health Application" – 45 CFR 164.501

The proposal to limit third-party directives to electronic copies of PHI in an EHR combined with the proposed definition of EHR in 45 CFR 164.501 effectively excludes PHI from health plans from inclusion in a third-party directive response. This creates a misaligned requirement whereby traditional direct access requests would allow for an individual to access PHI in a designated record set, which includes PHI maintained by or for both covered providers and health plans, but third-party directive requests would be limited to PHI from authorized health care clinicians and staff. HIEs are increasingly engaging with and receiving data from both covered health providers and health plans. If an HIE were to receive an access request from an individual, they would have to determine whether it was a traditional access request or a third-party directive and then segment the individual's PHI by data source before responding to the request.

If OCR finalizes its proposal to limit the definition of EHR to PHI "created, gathered, managed, and consulted by authorized clinicians and staff," then NYeC suggests that OCR permit and encourage CEs and BAs to include PHI from health plans, if available, when responding to third-party directives. PHI originating from health plans can provide critical insights into patient care such as additional co-morbidities and/or prior procedures. Therefore, OCR should clarify that returning PHI in an EHR is the floor for third-party directives and responding entities would be permitted and encouraged to respond with all PHI in a designated record set, if available.

Addressing the Individual Access Right to Direct Copies of PHI to Third Parties — 45 CFR 164.524(d)(7)

NYeC supports the newly proposed right for an individual to direct covered health care providers or health plans to submit and facilitate access requests. This will greatly reduce the burden individuals face when tracking down health care providers individually. HIEs have a demonstrated capability of facilitating this exchange on behalf of health care providers and health plans.

OCR seeks comment on approaches it may take to clarify that the Privacy Rule permits covered entities to use HIEs to make "broadcast" queries on behalf of an individual to determine which covered entities have PHI about the individual and request copies of that PHI. NYeC agrees with OCR's interpretation that §164.506(c)(1) permits this disclosure to HIEs for a CE's own health care operations purposes.[10] As BAs, QEs in the SHIN-NY currently offer a similar type of service to their provider participants through both QE-level and SHIN-NY-wide master patient index and patient record locator services, which allow QEs to perform broadcast queries on behalf of their participants to locate patient data across their regions and the state (although the purpose of such broadcast queries is generally for treatment, not patient access or healthcare operations).

While we agree this type of request is permissible under the current health care operations purpose, OCR should clarify HIEs' responsibilities in cases where undertaking broadcast queries for health care operations or patient access purposes conflicts with the text of the applicable business associate agreement (BAA). Sometimes BAAs between HIEs and their participants prohibit the HIE from making disclosures in response to patient access requests to anyone other than the participant who is the source of the data. Confusion may arise if an HIE receives a request from a covered entity under the health care

[10] 86 FR 6464

operations purpose, but the requesting covered entity intends to use the PHI to fulfill an access request. OCR should clarify that if such a restriction exists, an HIE should comply with the terms of such a BAA and not be required to respond to the request.

We also note that the Cures Act amended §300jj-19 of the Public Health Services Act[11] to require the Secretary of HHS, in coordination with OCR, to educate health care providers on ways of leveraging the capabilities of health information exchanges to provide patients with access to their electronic health information and clarify misunderstandings by health care providers about using health information exchanges for patient access to electronic health information. To our knowledge, such guidance has not yet been issued. HIEs play a pivotal role in the nationwide health care landscape, yet there is still considerable confusion among the industry about the scope of their permissions under HIPAA, which creates unnecessary barriers to exchange. NYeC believes OCR should use this opportunity to coordinate with the Secretary of HHS, as well as other agencies within HHS, including CMS and ONC to fulfill the Cures Act directive.

Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management that Constitutes Treatment or Health Care Operations — 45 CFR 164.506

NYeC applauds OCR for seeking to encourage disclosures of PHI to social service agencies, community-based organizations (CBOs), home and community-based services (HCBS), and other similar third parties that provide health-related services, (collectively referred to as CBOs below).

As providers and health plans focus more on social determinants of health (SDoH), they have come to conclude that CBOs may have just as much of an impact on a patient's health as providers. The SHIN-NY has increasingly prioritized CBO engagement and the incorporation of SDoH information into a patient's medical record. Based on NYS DOH's Bureau of Social Determinants of Health CBO Directory[12], over 250 CBOs—including both covered and non-covered entities— participate within the SHIN-NY. QEs provide services to these CBOs, including access to event notifications, secure messaging, QE clinical viewers, and results delivery.

As evidence of our commitment to CBO engagement and SDoH data exchange, the SHIN-NY Policy Committee recently updated the Policies & Procedures (P&Ps) to facilitate further CBO participation in the SHIN-NY.[13] These policy modifications include allowing non-HIPAA entities access to the SHIN-NY (with privacy and security safeguards) and revising the definition of Care Management to better reflect CBO use cases.

We support OCR's proposal to codify in regulation its prior guidance to allow for disclosures to CBOs. While sub-regulatory guidance is useful, many providers are unaware of this guidance. However, the newly proposed §164.506(c)(6) seems redundant and in conflict with the existing §164.506(c)(1). Based on OCR's own interpretation, (c)(1) already permits CEs to disclose to CBOs for their own treatment,

---

[11] 42 U.S.C 300jj-19(c)

[12] https://www.health.ny.gov/health_care/medicaid/redesign/sdh/cbo_directory.htm

[13] Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under NYCRR § 300.3(b)(1), Version 3.8, January 2021, available at: https://www.health.ny.gov/technology/regulations/shin-ny/docs/privacy_and_security_policies.pdf

payment, and health care operations purposes.[14] OCR also states that health care operations includes both individual and population-level case management and care coordination by covered providers and health plans.[15] Thus (c)(1) already allows for individual and population-level case management and care coordination disclosures, as well as additional health care operations and payment purposes not captured by care coordination and case management. However, (c)(6) effectively narrows this permission to only allow disclosures to CBOs for individual-level care coordination and case management either as a treatment activity of a covered health care provider or as a health care operations activity of a covered health care provider or health plan. We do not believe OCR should narrow this permission, but rather we suggest modifying or adding a subsection to (c)(1) to expressly include CBOs. For example, OCR could add language stating that "permitted disclosures include but are not limited to disclosures to CBOs for care coordination and case management activities."

Second, OCR should clarify that a CE may disclose PHI to a CBO that provides health related services for the CBO's *own* care coordination and case management activities even when the CBO is not a CE. The NPRM states, "…OCR does not propose to limit the regulatory text of the permission to disclosures made by a covered health care provider or health plan as part of the discloser's own treatment and health care operations."[16] While we understand this sentence was referring to disclosures to other CEs, we believe the same principle should also apply to non-HIPAA covered CBOs conducting health-related activities. Often these entities provide health-related activities to individuals without initial provider referral. For example, an individual seeks the services of a food bank and, to serve that individual, the food bank needs access to the individual's allergy history. Or an individual may want to enroll in a CBO's nutrition education or congregate meal service, but in order to be enrolled the CBO needs to undertake an assessment that requires the CBO to access the individual's medical history. In these examples, the CBO, not the disclosing CE, is exercising judgment as to whether such a disclosure is a necessary component of or may help further the individual's health.

Third, OCR should clarify their past guidance on disclosures to CBOs[17] by stating that BAs (including HIEs) are permitted to disclose PHI to CBOs on behalf of a CE for a HIPAA covered purpose without an individual authorization, as long as the BAA permits this disclosure.[18] The guidance currently says that disclosures are permitted if a provider believes that the disclosure to "certain social service agencies" is a necessary component of, or may help further, the individual's health or mental health care. In an HIE model, a CBO may become a participant and request HIE access to PHI of individuals under the CBO's care. For example, a CBO may sign up with an HIE to receive event notifications from hospitals participating in the HIE. In this scenario, the hospital may be sending notifications to the HIE without specifying a certain recipient, and the HIE is subsequently routing the notifications to the appropriate recipients on behalf of the hospital. In such a model, the hospital is not making an assessment as to whether the notification to a certain recipient will help further the individual's health, but rather the HIE is making the determination on behalf of the CE that the disclosure is permissible.

---

[14] 86 FR 6477

[15] 65 FR 82462, 82627

[16] 86 FR 6476

[17] See Office of Civil Rights, 3008-Does HIPAA permit health care providers to share PHI about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes? https://www.hhs.gov/hipaa/for-professionals/faq/3008/does-hipaa-permit-health-care-providers-share-phi-individual-mental-illness-third-party-not-health-care-provider-continuity-care-purposes/index.html

[18] 45 CFR 164.502(a)(3)

OCR should also consider revising the title of this guidance: "Does HIPAA permit health care providers to share PHI about an individual with mental illness with a third party that is not a health care provider for continuity of care purposes?" to be clearer that the guidance addresses disclosures to CBOs.

Fourth, OCR could help address provider concerns about CBO disclosures if it issued guidance on ways that providers can securely transmit and ensure the confidentiality of data disclosed to CBOs. A mandate that the disclosing provider enter into a contract akin to a BAA with the CBO may not be necessary, but OCR could provide guidance on when an agreement between the disclosing provider and the recipient CBO may be useful, and OCR could provide recommendations as to potential terms in such agreement. For example, the SHIN-NY P&Ps place safeguards around disclosures to non-CE CBOs, including limiting the mechanisms through which CBOs can receive PHI, limiting disclosures to the minimum necessary, and limiting re-disclosures only to (i) the patient or the patient's Personal Representative; and (ii) another Participant for purposes of Treatment or Care Management.[19]

Finally, OCR should consider defining "health-related services" or developing guidance to expand on the examples of health-related services in the Proposed Rule in order to prevent confusion and variable interpretation across the industry on the types of services that qualify an organization to receive such disclosures. Without such clarity, CEs and BAs will withhold PHI rather than risk impermissible disclosures and the barriers to coordinated care that OCR intends to address through this proposal will persist.

Amending the Definition of Health Care Operations to Clarify the Scope of Care Coordination and Case Management – 45 CFR 160.103

NYeC supports the proposal to clarify that the definition of health care operations in §164.501 encompasses all care coordination and case management by health plans, whether individual-level or population-based. We agree with OCR that the current definition of health care operations is ambiguous as to whether it allows for both individual and population-level care coordination and case management. However, we believe the newly proposed definition does not appropriately clarify this ambiguity.

While the current definition appears to only allow for population-based care coordination and case management, the new definition appears to only allow for individual-level care coordination and case management. This is unclear for two reasons: 1) in the proposed change, the words population-based activities only modifies activities relating to improving health or reducing health care costs, which gives the impression that the absence of the modifier in the subsequent activities means those activities are not population-based; and 2) the definition of treatment refers to care coordination and case management without any modifier, yet OCR has stated in guidance[20] that treatment only refers to individual level activities. Therefore, one could logically argue that the phrase "care coordination and case management" with no modifier in the definition of health care operations is also limited to individual-level activities.

In order to limit additional ambiguity, OCR should specifically add the phrase "population-based and individual-level" to modify care coordination and case management, as well as any other activities within the definition of heath care operations that apply.

---

[19] Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under NYCRR§ 300.3(b)(1), Section 8.3

[20] 65 FR 82497 https://www.govinfo.gov/content/pkg/FR-2000-12-28/pdf/FR-2000-12-28.pdf

Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access – 45 CFR 164.524(b)

NYeC supports OCR's proposal to modify §164.524(b)(2)(i) and (ii) to require that access requests be fulfilled "as soon as practicable," but in no case later than 15 calendar days after receipt of the request, with the possibility of one 15 calendar-day extension. Currently, NYS law requires that any health care provider or facility provide the opportunity for a patient to inspect all information concerning or relating to their examination or treatment within 10 days of a written request. Copies of such records must be provided within a reasonable time.[21] The NYS DOH considers 10-14 days to be a reasonable timeframe for providers to respond to a written request for copies of medical records.[22] NYeC believes that applying such timely access requirements across all CEs will improve individuals' ability to manage their care and alleviate harm caused by delays or last-minute denials of access.

Adjusting Permitted Fees for Access to PHI and ePHI—45 CFR 164.524(c) and (d)

NYeC applauds OCR for seeking to re-instate fee limitations ("patient rate") for third party directives. As currently proposed, §164.524(d)(6) would limit fees to only labor required to copy the requested PHI in electronic form and preparing an explanation or summary of the electronic PHI. However, this does not take into account additional costs incurred by CEs and BAs when making and shipping electronic PHI through a non-internet-based method e.g., the US mail.

Similarly, the proposed §164.524(c)(4)(i) includes supplies for making non-electronic copies and the actual postage and shipping for mailing non-electronic copies. We believe it should also allow fees for the supplies for making and mailing electronic copies. CEs and BAs incur charges for the supplies and shipping of electronic copies in the same way they do for supplies and shipping of non-electronic copies of PHI and as such should be able to recoup those costs.

NYeC believes that the patient rate should always include the cost of supplies for making electronic copies of PHI e.g. a USB device, as well as the cost of postage and shipping for sending electronic copies through a non-internet based method. We further clarify this recommendation in the table below, with edits in red.

---

[21] N.Y. Public Health Law §18 (2), N.Y. Mental Hygiene Law §22.16(b).

[22] https://www.health.ny.gov/publications/1443/

Table summary on allowable fees[23]

Type of Access	Recipient of PHI	Allowable Fees
In-person inspection – including viewing and self-recording or -copying	Individual (or personal representative)	Free
Internet-based method of requesting and obtaining copies of PHI (*e.g.*, using View-Download-Transmit functionality (VDT), or a personal health application connection via a certified-API technology)	Individual	Free
Receiving a non-electronic copy of PHI in response to an access request	Individual	Reasonable cost-based fee, limited to labor for making copies, supplies for copying, actual postage & shipping, and costs of preparing a summary or explanation as agreed to by the individual
Receiving an electronic copy of PHI through a non-internet-based method in response to an access request (*e.g.*, by sending PHI copied onto electronic media through the U.S. Mail or via certified export functionality)	Individual	Reasonable cost-based fee, limited to labor for making copies and costs of preparing a summary or explanation as agreed to by the individual *Add: supplies for copying and actual postage & shipping*
Electronic copies of PHI in an EHR received in response to an access request to direct such copies to a third party.	Third party as directed by the individual through the right of access.	Reasonable cost-based fee, limited to labor for making copies and for preparing a summary or explanation agreed to by the individual. *Add: supplies for copying and actual postage & shipping when request is fulfilled through a non-internet-based method*

[23] 86 FR 6465