NATE

NATIONAL
ASSOCIATION
FOR TRUSTED
EXCHANGE

November 23, 2016

U.S. Office of Science and Technology Policy (OSTP)
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Re: Request for Information Regarding Data Portability

To Whom It May Concern:

Thank you for the opportunity to respond to this important request for information on behalf of the National Association for Trusted Exchange (NATE) and several of its members and allies. NATE (http://nate-trust.org) is a 501(c)(3) organization that brings the expertise of its membership and other stakeholders together to find common solutions that optimize the appropriate electronic exchange of health information for greater gains in technology adoption and improvement of patient outcomes. Emerging from the Western States Consortium, a pilot project supported by the U.S. Department of Health and Human Services' (HHS) Office of the National Coordinator for Health IT (ONC) that began in 2011, NATE was established as a not-for-profit organization in May 2013. Consistent with NATE's mission to address the legal, policy and technical barriers that inhibit health information exchange between data holders and healthcare consumers, NATE leads and participates in a number of ongoing and emerging projects focused on exchange via multiple modes of transport, including Direct secure messaging and APIs. NATE boasts organizational members of all types, from interested individuals to large organizations such as the U.S. Department of Veterans Affairs (VA).

We understand that the OSTP is most interested in responses related to the following topics:

1) the potential benefits and drawbacks of increased data portability;
2) the industries or types of data that would most benefit or be harmed by increased data portability;
3) the specific steps the Federal Government, private companies, associations, or others might take to encourage or require greater data portability (and the important benefits or drawbacks of each approach);
4) best practices in implementing data portability; and
5) any additional information related to data portability policy making, not requested above, that you believe OSTP should consider with respect to data portability.

With regard to questions (1) and (2) – the benefits and beneficiaries of increased data portability – the healthcare industry, and the patients and families served by it, could greatly benefit from increased data portability and technical interoperability. NATE is the only national nonprofit focused exclusively on reducing the barriers that inhibit a consumer's access to their health information. The driving force behind NATE's activities is an understanding that one of the foundational elements of HIPAA, the HITECH Act, and their implementing regulations is that individuals have a right to electronic access to their health information. Individuals now have an unprecedented opportunity to exercise their HIPAA right of access and become more engaged in their care, based on healthcare providers' widespread adoption of certified electronic health record (EHR) technology and the Direct Project's secure exchange mechanism built into that technology. Furthermore, due to the availability of a wide variety of consumer-facing applications (CFAs), individuals have the ability to better receive, manage, and share their electronic protected health information (PHI). Secure electronic access to their PHI offers individuals a variety of benefits, including: (1) faster, less expensive access to health information; (2) receipt of the information in a form that is easier to review and manage; (3) increased ability to merge health records from multiple providers into one longitudinal record; (4) individual-centric health information exchange offers individuals an alternative means to ensure that their health information is transmitted from one healthcare provider to another in order to improve patient safety and care coordination; and (5) perhaps most important of all, the inherent patient safety benefits when the consumer and their proxy has the ability to identify and indicate corrections needed to their medical records to help ensure the highest quality care possible is delivered. In practice, however, individuals are finding that a great number of healthcare providers are not fully leveraging their EHR technology, either due to a lack of knowledge, vendor costs, or other barriers, to provide the consumer access to their protected health information as required by the HIPAA Privacy Rule (http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/).

NATE is committed to helping consumers access their health information via all appropriate means. NATE is a proud partner of the Get My Health Data Campaign (http://getmyhealthdata.org/), a collaborative effort among leading consumer organizations, healthcare experts, former policy makers and technology organizations working to enhance consumer access to digital health information. NATE's leadership is also committed to supporting Flip the Clinic's (http://driptheclinic.org/flips/accessourdata/) goals of making health information accessible to consumers, empowering them to make their own decisions about when and with whom their data is shared. NATE provides focused recommendations and useful education about the technical options available to achieve the objectives of Flip the Clinic #55. NATE was honored to stand beside the Get My Health Data Campaign and Flip the Clinic when they were recognized by the White House as "Precision Medicine Champions of Change" (http://nate-trust.org/nate-videos/) on July 8, 2016.

With regard to question (3) – specific steps that might be taken to encourage or require greater data portability – one of best methods that the healthcare industry has developed thus far to encourage and enable data portability is through the development of Trust Communities. NATE has been operating its own Trust Bundles in production since 2012 (http://www.healthit.gov/buzz-blog/state-hie/western-states-consortium-pilot-direct-demonstrates-power-federalstate-coordination/) (If needed, see Appendix for an explanation of Trust Communities and Trust Bundles within the context of Direct Secure Messaging). Since that time, NATE has become the recognized leader in enabling HIPAA-covered entities to compliantly share protected health information with consumers. In 2014, NATE was entrusted with the administration of ONC's Blue Button Trust Bundle (using Direct secure messaging protocols) (http://nate-trust.org/wp-content/uploads/2014/08/NATE-BB+-FINAL-as-released.pdf). Under the governance of NATE, the Blue Button community continues to flourish. In 2015, NATE made the first release of the NATE Blue Button for Consumers (NBB4C) Trust Bundle (http://nate-trust.org/nbb4c-trust-bundle). The NBB4C provides a technical solution to establishing scalable trust among organizations using Direct secure messaging to exchange protected health information between HIPAA-covered entities and the consumers that they serve. The NBB4C includes the trust anchors of multiple third party CFAs that have elected to adopt a common set of policies and practices that enable consumer mediated health information exchange while preserving personal privacy preferences. Working with a broad set of stakeholders through multiple task forces, crowdsourcing and a call for public comment, the process to determine the eligibility requirements that govern the NBB4C spanned two years and included multiple pilots funded by ONC and multiple State HIE programs. NATE undertook this effort in response to the needs expressed by all stakeholder types for the establishment of a national trust framework that reflects the distinct difference in regulatory requirements applicable to CFAs (that they are not subject to HIPAA, instead they are regulated by the Federal Trade Commission) and an ever-increasing demand on the part of consumers for secure access to this type of data via mobile and desktop applications. NATE is currently working to extend the utility of its trust community beyond Direct secure messaging to include other consumer-centric technologies, such as those that leverage APIs or other modes of exchange (NATE, in partnership with the Centers for Medicare and Medicaid Services' Blue Button API Team, will be leveraging FHIR-based resources and standard APIs to pilot the use of forward leaning technologies that allow a beneficiary to access their electronic health information from Medicare).

The NATE NBB4C is presently the only existing Trust Community that is specifically dedicated to maximizing opportunities for exchange between HIPAA-covered entities and the applications that consumers rely upon for managing their own data. One of the benefits of the NBB4C is the diversity of its participants and the services they offer through their applications. Because the NBB4C is a trust community that has agreed to a common set of security and privacy protections, HIPAA-covered entities that load the NBB4C into their trust stores can offer a wide range of trusted options for consumers looking to manage their health information for different purposes. One way that the Federal Government can specifically support greater healthcare data portability is to require that all HIPAA-covered entities subscribe to at least one consumer-focused trust bundle. When considering which trust bundles to subscribe to, it is important that HIPAA-covered entities are able to make local policy decisions that reflect their applicable policy requirements. However, NATE believes that it is also the patient's right to determine which CFA best serves their needs and that healthcare providers and/or their technology vendors should not be usurping this right by making their own determination about which consumer-facing applications should or should not be trusted (Additional information on this issue is available in the Appendix). Current guidance by the HHS Office of Civil Rights (OCR) supports this view, clarifying that once a patient's data is shared in the manner in which they request it, the provider sharing the data is no longer culpable in the event of a breach of that data.

Another way for the healthcare industry to encourage and enable greater data portability is by developing central portals through which common requests for information can be made and fulfilled. For example, NATE is currently working on developing a concept around the electronic submission of legal requests for medical records. Patients have a right under the HIPAA Privacy Rule to request copies of their personal health information from all of their providers, however this right of access typically hinges on the effective submission of a legal release of information form that is then acted upon by a medical records staffer. The person responsible for fulfilling the patient's request may not always be local to the provider's location. They may be part of a large Medical Records department or even an outsourced medical records warehouse. This can cause confusion for the patient and/or extra work for front office staff. Worse, if provider organizations are found by OCR to be preventing the patient from having access to their health information or otherwise acting as "information blockers," they can be fined significant amounts. In order to simplify and streamline this process to make it easier for patients and providers alike, NATE suggests creating a single portal between which patients and Medical Records staff could communicate. On the patients' side, the portal could streamline the collection of a standard set of data most often included on a release of information form. On the providers' side, every registered Medical Records department would create an account that includes a Direct address. In registering, the Medical Records department would populate a profile with information about the providers that they serve, so that consumers could discover where their providers' records are managed and how best to access them. By registering with this medical records portal, the healthcare organization, and those entities that serve them, would have a single, secure queue from which they could establish a reliable process to ensure compliance with applicable law. At the center of this new flow of information between the patient and the Medical Records department would be the NATE NBB4C. Because the NBB4C aggregates consumer-facing applications, consumers could choose any one of a number of applications through which to obtain a secure Direct address, use a Direct message to make their request and receive their information.

With regard to question (4) – best practices in implementing data portability – this topic was discussed in great detail during the development of the NBB4C requirements. The community felt very strongly that allowing a patient to move their data from one application to another was a foundational element of this Trust Community. The NBB4C Onboarding Application (http://nate-trust.org/wp-content/uploads/2015/07/1-NBB4C-Onboarding-Application-3-d-1-REVISED-v3.7.pdf) specifically states that the applying "CFA shall ensure that an end-user is able to extract all of their structured data captured in the CFA and be able transport it to another location via Direct or another secure transport method." The reasoning for this requirement is clearly stated in the application: "The community being established by this bundle is intended to enable consumer choice and prevent vendor lock-in where the consumer's PHI is trapped in a CFA."

NBB4C participation criteria also address the question of what happens to a patient's data after they terminate their participation with the application. The criteria state that the "CFA shall ensure that an end-user is able to terminate their participation in the CFA and be able to request that their data be expunged in its entirety from the application and any data stores controlled by the CFA that may contain the end-user's PHI." The stated justification for this requirement is that "The community being established by this bundle is intended to ensure that the consumer has control over how its PHI is used, including how it is used after termination of the consumer's use of the application."

Note that the NBB4C calls for the portability of all structured data held by a CFA. From an electronic data portability policy perspective, and especially with regard to data stored in provider-controlled EHRs, NATE would recommend that this definition in fact be expanded. Patients currently have the right to receive an entire designated record set as defined by the HIPAA Privacy Rule, but most EHRs can only produce a part of that in a single action. Therefore, part of the workflow for the Medical Records department may require them to not only export a CCDA but to actually pull additional information from their internal data sources to respond to a consumer's request. This additional information could include unstructured data, radiology/pathology reports, OpenNotes, etc. Having all of the available patient data becomes especially important in legal malpractice cases in which patient records are requested by subpoena. Many patient portals are capable of providing this additional data but are prevented from doing so by internal policy controls.

To take this even one step further, NATE suggests that providing the patient or an authorized designee with a complete copy of their health information from an electronic record in a computable format may not even be enough to enable the patient to receive the most value from the receipt of their health information. Rather, we would recommend that the best data portability implementations would include both machine- and human-readable formats for those members of the population that may not have access to software that can render the machine-readable content in an end-user friendly manner.

Another key component to any successful data portability implementation is full transparency with regard to the use and storage of patient information. After requiring that NBB4C participants comply with all applicable state and federal laws and regulations, the next most important requirement for NBB4C participants is that they make clearly available their Notice of Privacy Practices. Specifically, "The CFA shall display their Notice of Privacy Practices (NPP) in an easily accessible location prior to sign up or use. [It must] include language on the application's data practices, including those areas addressed by the ONC Personal Health Record (PHR) Privacy Notice."

With regard to question (5) – additional information OSTP should consider in this policy-making area – NATE would suggest that a truly landmark action that could be taken in support of accurate data portability is for the Federal Government to finally resolve the "patient matching" issue. In addition to NATE's work around trust frameworks, NATE has been an active participant in community efforts to address the question of accurate matching between a patient and their information. In communities in which many people share the same name and often share other identifying characteristics as well, it can be a significant challenge to ensure that a patient's electronically stored information is accurate. NATE believes that work to improve algorithmic patient matching is important and supports the investigation of voluntary unique patient identifiers. A solution that is controlled by the consumer, allowing them to establish the correlation between their identifier and those identifiers that have been assigned to them by their numerous encounters with different parts of the healthcare system would not only simplify technical interoperability – it would literally save thousands of lives and reduce untold and unnecessary suffering and costs. One example might be to leverage the cryptographic key associated with the unique Direct address set up by the patient as a voluntary patient identifier.

We are optimistic about the maturation of the health ecosystem and support innovation with regard to next generation technologies. In fact, NATE is actively collaborating with numerous organizations to establish a new trust mechanism known as the TrustHarbor, which is designed to be the flexible enabling infrastructure that fosters broad adoption of API-based technologies across all types of use cases. Regardless of the technology used, it is critical that trusted mechanisms be made readily available to connect the applications used by patients to manage their health information with the clinical systems that hold that data.

On behalf of NATE, its members, and the undersigned, thank you for the opportunity to provide feedback on this request for information. If we can provide any additional information or clarification, please do not hesitate to contact NATE's CEO, Aaron Seib, at aaron.seib@nate-trust.org.

Sincerely,

Aaron Seib

Aaron Seib, CEO
National Association for Trusted Exchange

Bart Carlson, CEO & Chief Patient Advocate
Azuba

Colin Wallis, Executive Director
Kantara Initiative

Brian Weiss, Founder
Carebox

MaryAnne Sterling, Co-Founder
Connected Health Resources

Kate Horle, Chief Operations Officer
CORHIO

Panha Chheng, CEO & Founder
Medyear

Bob Janacek, Co-Founder & CTO
DataMotion

Beth Davidson, State Health Information Technology Coordinator
Alaska Department of Health & Social Services

Elaine Scordakis, Assistant Director
California Office of Health Information Integrity

Christina Caraballo, Senior Healthcare Strategist
Get Real Health

Anand Prabhu, CEO/Founder
MediPortal

Tess Coody, Founder & CEO
Wellvana

Bettina Experton, MD, President & CEO
Humetrix

Linda Van Horn, President/CEO
iShare Medical

Paul Cartland, Owner
Total Link LLC

APPENDIX: What is Direct Secure Messaging?

(Credit to Adam Greene of Davis Wright Tremaine)

To understand NATE's perspective, some background on the Direct Project may be helpful. Direct is a technical standard for exchanging health information between healthcare entities in a trusted network (http://www.healthit.gov/sites/default/files/directbasicsforprovidersqa_05092014.pdf). For Stages 2 and 3 certified EHR technology, EHR vendors are required to either (a) certify their transitions-of-care modules or complete EHR product offerings to include Direct to meet certification requirements, or (b) work with a third party to provide Direct services.

To oversimplify Direct secure messaging, it can be thought of as encrypted e-mails that incorporate digital certificates (known as Trust Anchors) to verify the identity and trustworthiness of the other party. The sender sends a Direct message to the sender's Health Information Service Provider (HISP). The sender's HISP then routes the message to the receiver's HISP. The receiver's HISP routes the message to the receiver.

For example, a physician's practice implements certified EHR technology. The EHR vendor either operates as the physician practice's HISP, or contracts with a third party to act as the physician practice's HISP. The physician is assigned a unique Direct address (e.g. PhysicianName@direct.EHRvendor.com). On the other end, a CFA vendor provides a unique Direct address (e.g. patient.name@direct.somephr.org) to each user of their product. The CFA either acts as a HISP or contracts with a third party to act as a HISP.

Under this system, every patient can readily download a third party application that supports Direct secure messaging (there are many from which to choose) and securely obtain a copy of his or her medical record summary from any healthcare provider who has implemented certified EHR technology. *The primary obstacle, however, is that both the sender and receiver must have uploaded each other's Trust Anchors, otherwise the message will not be delivered.* (http://wiki.directproject.org/Direct+Project+Security+Overview)

The Direct Project's Trust Anchors, Trust Communities, and Trust Bundles

As referenced above, a fundamental part of Direct secure messaging is the exchanging of certain digital certificates, known as Trust Anchors. The purpose of these Trust Anchors is that each party in a Direct Message knows the other party is who it claims (i.e. authentication) and also to find out information about its privacy and security policies.

For example, a hypothetical patient requests that her healthcare provider send her a copy of her medical record through Direct to patient.name@direct.somephr.org. If the healthcare provider seeks to send the Direct message, then the healthcare provider's certified EHR technology will send the message containing the medical record to the EHR's HISP. The HISP maintains a "certificate store" (or "trust store") where a number of Trust Anchors (digital certificates) are maintained. The healthcare provider's HISP will contact a domain name server (DNS), the equivalent of an Internet phone book, which will respond that "somephr.org" is associated with a particular digital certificate. If the recipient's Trust Anchor is loaded into the HISP's trust store, then the transaction will proceed. If the recipient's Trust Anchor is not in the HISP's trust store, then the HISP will reject the healthcare provider's attempt to send the medical record to the patient's CFA.

The Direct Project promotes the creation of "Trust Communities" and corresponding "Trust Bundles." Trust Communities are formed by organizations voluntarily electing to follow a common set of policies and processes related to health information exchange. Examples of these policies include those that address identity proofing, certificate management, and privacy and security. (http://www.directtrust.org/trust-bundles/) Organizations such as NATE and DirectTrust create and maintain Trust Communities for users of Direct Secure Messaging (DirectTrust's Trust Community is focused on provider-to-provider exchange and NATE's Trust Community is focused on provider-to-patient exchange). Trust Communities' policies and procedures may differ significantly. For example, one Trust Community may require that its members go through an accreditation process with respect to their HIPAA compliance. Another Trust Community may rely on self-attestation with respect to privacy and security compliance, but may include requirements pertaining to state privacy laws or secondary use of data. NATE's Blue Button for Consumers (NBB4C) Trust Bundle is an example of a Trust Community.

For each Trust Community, there is a Trust Bundle, which is a collection of Trust Anchors (digital certificates) pertaining to members of the Trust Community. Through this process, a HISP can upload a single Trust Bundle, with knowledge that all Trust Anchors (digital certificates) correspond to a set of entities that meet certain minimum privacy and security requirements. An organization can choose to upload certain Trust Bundles but not others based on its own policy preferences. For example, a state-operated healthcare provider may choose to only accept Trust Bundles for Trust Communities that address compliance with both federal and state privacy and security laws. It is important to note that while Trust Bundles provide a means of uploading a large number of Trust Anchors at once, a HISP also can upload a single Trust Anchor.

The inclusion of a consumer-focused Trust Bundle, such as NATE's Blue Button for Consumers (NBB4C), is the stumbling block for widespread exchange between a provider and an individual's choice of third party health application, although it does not need to be. If the physician does not instruct its EHR vendor and/or HISP to include the Trust Anchor (or Trust Bundle) of the patient's CFA in the HISP's trust store, then the physician can attempt to send the patient's medical record summary to the Direct address of the patient, but the Direct message will not be delivered.

ONC provides the following guidance to healthcare providers on this issue:

> ONCE I HAVE A DIRECT ADDRESS, WILL I BE ABLE TO EXCHANGE WITH ANY OTHER PROVIDER WITH A DIRECT ADDRESS?
>
> Because Direct uses strong security to protect your communications (just like your trusted internet interactions with financial institutions, online retailers, and other secured

websites), certain steps may need to be taken to start exchanging information with another provider to ensure that they are a trusted connection. While much of the technical details of this will be handled by your EHR vendor, there are a few important points to note on establishing trust with other providers:

- Based on your system or the other provider's system, you may be required to indicate your wish to send and/or receive information from the other provider.
- Depending on the EHR and/or HISP you and the receiving provider are using, you need assistance from your vendor to establish this trusted relationship
- Some work between the two vendors may be required in order to communicate. If you have questions about communicating with another provider, check with your EHR vendor or Direct HISP as a first point of contact.

The problem is that, in practice, healthcare providers are not asking their EHR vendors or HISPs to be able to communicate with patients through third party applications. Accordingly, when a patient with a CFA-provided Direct address requests his or her records in a convenient, inexpensive, and readily producible manner, the request is denied or does not work. This may occur for any number of reasons. The healthcare provider may be confused and not know the step it needs to take. The healthcare provider may mistakenly believe that HIPAA does not permit them to exchange protected health information directly with a third party application at the individual's request. The healthcare provider may believe that it is inappropriate to exchange protected health information with an entity, such as a CFA, that is not subject to HIPAA. The healthcare provider may interpret that the requested form and format is not "readily producible" since the healthcare provider would need to take some action (e.g. contacting the EHR vendor or HISP) to enable the exchange. Or the healthcare provider simply may not want to go through the effort of contacting the EHR vendor or HISP and requesting the exchange of the relevant Trust Anchors (digital certificates). *Whatever the reason, the result is the same – one of the most convenient ways for the patient to receive his or her information and become better engaged in a secure manner is denied.*

The NATE NBB4C includes privacy and security requirements above the minimum legal requirements for participating CFAs. A healthcare provider need not initiate trust relationships with the third party application of the patient's choice on a one-off basis, but can instead take the single step of requesting that its EHR vendor or HISP permit exchange with all members of the NBB4C. This will immediately facilitate the healthcare provider being able to send Direct messages to a variety of PHR applications, all of which have agreed to meet certain privacy and security requirements. Despite the ease of this step, healthcare providers and their HISPs are not taking this action and instead are denying patients access to their electronic medical records through Direct secure messaging.

Trust Anchors and the HIPAA Right of Access

The use of Trust Anchors is invaluable in the exchange of health information between parties. Where a physician has discretion as to whether to provide protected health information to a recipient, the Trust Anchors model provides an easy and scalable means for the physician to know that the protected health information is going to the correct recipient and to have a level of comfort regarding that recipient's privacy and security safeguards. Otherwise, each physician would need to take steps to confirm the identity of each recipient, and may also wish to look at the recipient's privacy and security practices. But the Trust Anchor model should not be used as an impediment to an individual exercising his or her right of access.

While HIPAA generally provides a covered entity with discretion as to whether to disclose protected health information, a covered entity is required to disclose protected health information maintained in a designated record set to an individual upon the individual's request (45 C.F.R. §§ 164.502(a)(2)(i) and 164.524). A covered entity cannot refuse to provide an individual with a copy of the individual's designated record set because the individual does not maintain sufficient privacy and security practices.

The HITECH Act and its corresponding regulations clarified that an individual can require that the covered entity send an electronic copy of the designated record set to a designated third party (42 U.S.C. § 17935(e); 45 C.F.R. § 164.524(c)(3)(ii)). The covered entity must provide the electronic copy in the form and format requested by the individual, if it is readily producible in such form and format (45 C.F.R. § 164.524(c)(2)(i)). Nothing in HIPAA permits the covered entity to deny the individual's request because the designated recipient does not have sufficient privacy and security policies in place.

Accordingly, when a patient requests that a HIPAA-covered healthcare provider that has implemented certified EHR technology transmit protected health information in a designated record set to the patient's choice of CFA via Direct secure messaging, the healthcare provider is required to do so (An exception would be if a healthcare provider has a valid basis for denying the request, such as where the access is reasonably likely to endanger the life or physical safety of the patient or another person). The healthcare provider must verify the patient's identity (45 C.F.R. § 164.514(h)), but the healthcare provider may not claim that the requested form or format is not feasible, since the certified EHR technology readily allows for the exchange. The healthcare provider may not refuse to contact the EHR vendor or HISP and request that the CFA's Trust Anchor be added. The healthcare provider may not claim that it does not have a sufficient basis for trusting the third party application of the patient's choice, because it is not the healthcare provider's place to question the privacy and security practices, or even the identity verification, of the patient's designated recipient.

Make no mistake, we are not advocating for poor privacy and security practices for third party applications. We firmly believe that CFAs should be transparent in their privacy and security practices, such as through the ONC PHR Model Privacy Notice, and should not use health information for any purposes without the patient's knowledge. But it falls to the patient to decide whether he/she wants to trust his or her health information to a particular CFA. No healthcare provider should be permitted to deny an individual's request for access based on the provider's unwillingness to request the upload of a CFA's Trust Anchor to the HISP's trust store.