

January 30, 2015

To: Ms. Jocelyn Samuels, Director  
Office for Civil Rights  
U.S. Department of Health & Human Services  
200 Independence Avenue, S.W.  
Room 509F HHH Bldg.  
Washington, D.C. 20201

cc: Dr. Karen DeSalvo  
National Coordinator  
Office of the National Coordinator for Health IT  
U.S. Department of Health and Human Services  
200 Independence Avenue, S.W.  
Washington, D.C., 20201

Re: Direct Messaging and Individual's Right of Access through Their Personal Health Record

Dear Director Samuels:

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 electronic medical record. Individuals now have an unprecedented opportunity to exercise their HIPAA right of access and become more engaged in their care, based on health care providers' widespread adoption of certified electronic health record ("EHR") technology and the Direct Project's secure exchange mechanism. Furthermore, through the widespread availability of personal health records ("PHRs"), individuals have the ability to better receive, manage, and share their electronic protected health information. Secure electronic access to their protected health information offers individuals with a variety of benefits: (1) faster, potentially 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 medical records from multiple providers; and (4) as widespread provider-to-provider health information exchange stumbles due to interoperability and business barriers, individual-centric health information exchange offers individuals an alternative means to ensure that their health information is transmitted from one health care provider to another in order to improve patient safety and care coordination.

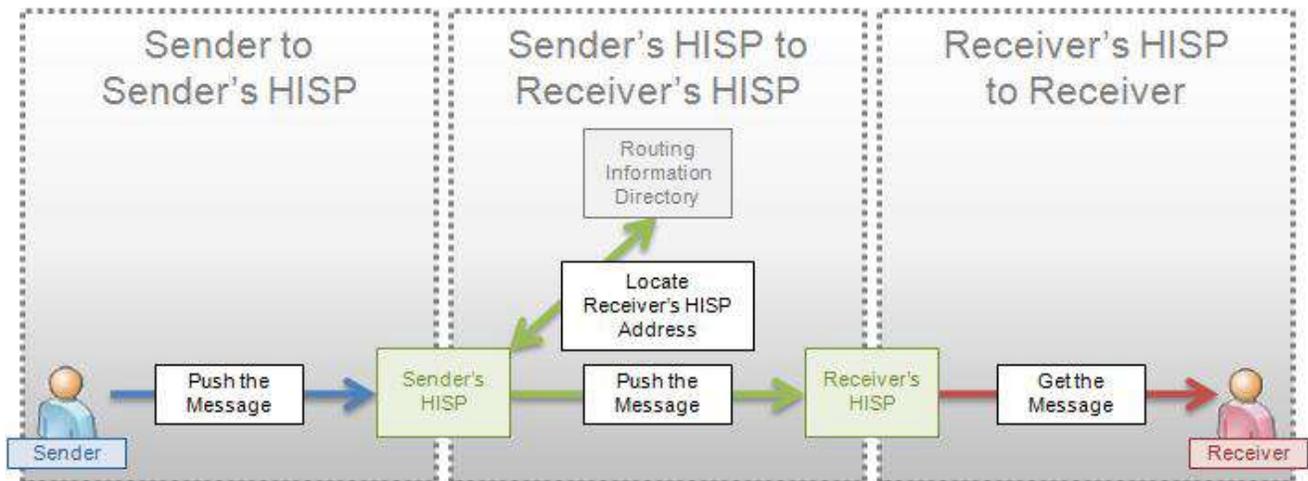
In practice, however, individuals are finding that health care providers are not leveraging their EHR technology to provide them access to their protected health information as required by HIPAA. We ask for your assistance in reducing this obstacle through clarification of HIPAA.

### **What is Direct Messaging?**

To understand the issue, some background on the Direct Project is helpful. Direct is a technical standard for exchanging health information between health care entities in a trusted

network.<sup>1</sup> For Stage 2 Meaningful Use, 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.<sup>2</sup> Additionally, the HHS Office of the National Coordinator’s (“ONC’s”) Blue Button+ initiative relies on Direct as the means for patients to securely receive Blue Button data (a patient record) in an automated fashion (this automated receipt of Blue Button patient data is known as Blue Button+).

To oversimplify Direct 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 following is a graphical representation:



Credit: Direct Project, *The Direct Project Overview*, <http://wiki.directproject.org/file/view/DirectProjectOverview.pdf>.

As illustrated above, 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](mailto:PhysicianName@direct.EHRvendor.com)). On the other end, a PHR vendor offers PHRs to patients. Each patient is assigned a unique Direct address (e.g., [ellen.ross@somephr.org](mailto:ellen.ross@somephr.org)). The PHR vendor 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 PHR application that supports Direct Messaging (there are many from which to choose) and securely obtain a copy of his or her medical record summary from any health care provider who has implemented certified EHR

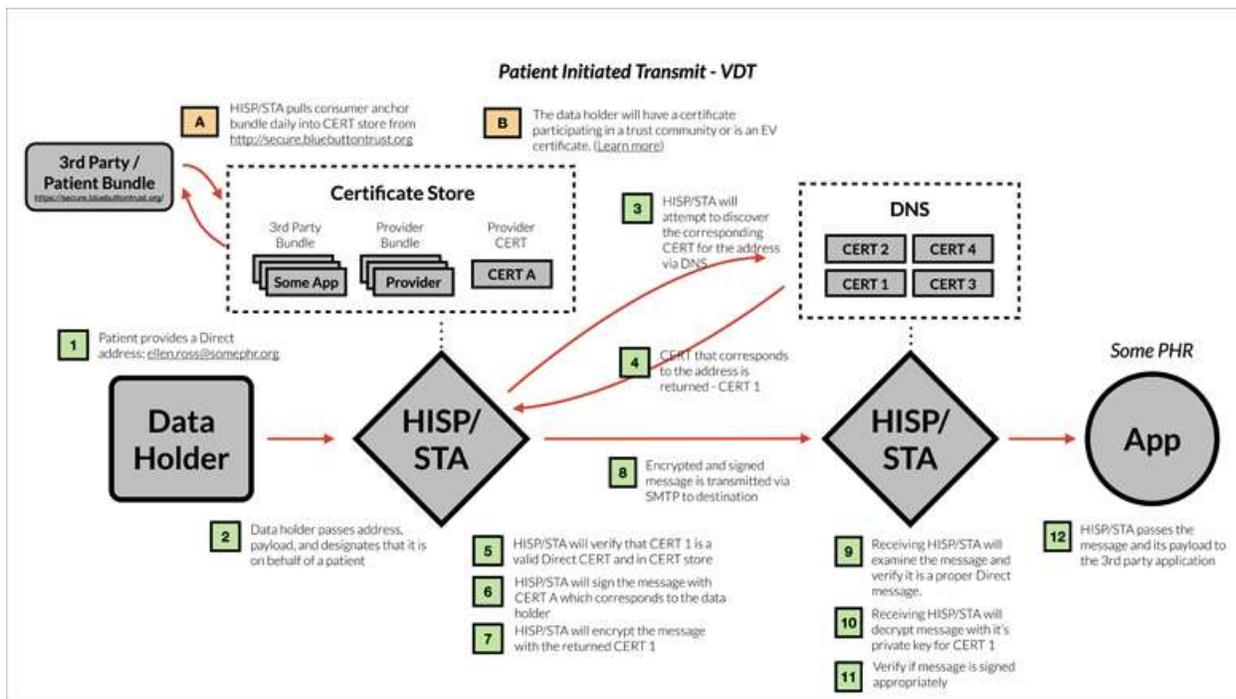
<sup>1</sup> U.S. Department of Health and Human Services, *Direct Basics: Q&A for Providers* (May 2014), [http://www.healthit.gov/sites/default/files/directbasicsforprovidersqa\\_05092014.pdf](http://www.healthit.gov/sites/default/files/directbasicsforprovidersqa_05092014.pdf).

<sup>2</sup> *Id.*

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.<sup>3</sup>

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

As referenced above, a fundamental part of Direct 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. The following is a schematic of how the complex exchange of certificates works during Direct Messaging.



Credit: Blue Button+ Implementation Guide, <http://bluebuttonplus.org/transmit-using-direct.html#certificates>

For example, a hypothetical patient (“Ellen Ross” in the above example) requests that her health care provider send her a copy of her medical record through Direct Messaging to [ellen.ross@somephr.org](mailto:ellen.ross@somephr.org). If the health care provider seeks to send the Direct message, then the health care provider’s certified EHR technology will send the message containing the medical record to the EHR’s HISP. The HISP maintains a “certificate store” where a number of Trust Anchors (digital certificates) are maintained. The health care 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 (“CERT 1”). If the recipient’s Trust Anchor (in this case, CERT 1) is loaded into the HISP’s certificate store, then the transaction will proceed. If the recipient’s Trust Anchor is not in the HISP’s certificate store, then the HISP will reject the health care provider’s attempt to send the medical record to the patient’s PHR.

<sup>3</sup> The Direct Project, *Direct Project Security Overview*, <http://wiki.directproject.org/Direct+Project+Security+Overview>.

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.<sup>4</sup> Organizations such as DirectTrust and the National Association for Trusted Exchange (“NATE”) create and maintain Trust Communities. 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.

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 health care provider may choose to only accept Trust Bundles for Trust Communities that address compliance with both federal and state privacy and security laws. ONC supported the creation of a Blue Button+ Patient Trust Bundle, now administered by NATE, which includes the trust anchors of all the undersigned PHR companies. 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 Trust Anchors concept currently is the stumbling block for widespread exchange with individuals’ PHRs, although it does not need to be. If the physician does not instruct its EHR vendor and/or HISP to include the patient’s PHR vendor in the HISP’s certificate 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 health care 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.

---

<sup>4</sup> DirectTrust, *Trust Bundle News and Announcements* (Oct. 25, 2014), <http://www.directtrust.org/trust-bundles/>.

- 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.<sup>5</sup>

The problem is that, in practice, health care providers are not asking their EHR vendors or HISPs to be able to communicate with patients through PHRs. Accordingly, when a patient with a PHR-vendor-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 health care provider may be confused and not know the step it needs to take. The health care provider may mistakenly believe that HIPAA does not permit it to exchange protected health information directly with a PHR at the individual's request. The health care provider may believe that it is inappropriate to exchange protected health information with an entity, such as a PHR vendor, that is not subject to HIPAA. The health care provider may interpret that the requested form and format is not "readily producible" since the health care provider would need to take some action (e.g., contacting the EHR vendor or HISP) to enable the exchange. Or the health care 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 is denied.

The NATE Blue Button Trust Bundle includes minimum privacy and security requirements for participating PHR vendors. Accordingly, a health care provider need not initiate trust relationships with PHR vendors 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 NATE Blue Button Patient Trust Bundle. This will immediately facilitate the health care 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. Nevertheless, health care providers and their HISPs are not taking this one step and instead are denying patients access to their electronic medical records through Direct 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.

---

<sup>5</sup> *Id.*

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.<sup>6</sup> 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.<sup>7</sup> 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.<sup>8</sup> 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 health care provider that has implemented certified EHR technology transmit protected health information in a designated record set to the patient's PHR via Direct Messaging, the health care provider is required to do so.<sup>9</sup> The health care provider must verify the patient's identity.<sup>10</sup> But the health care provider may not claim that the requested form or format is not feasible, since the certified EHR technology readily allows for the exchange. The health care provider may not refuse to contact the EHR vendor or HISP and request that the PHR vendor's Trust Anchor be added. The health care provider may not claim that it does not have a sufficient basis for trusting the PHR vendor, because it is not the health care 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 PHR vendors. The undersigned firmly believe that PHR vendors 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 purposes unrelated to the PHR. But it falls to the patient to decide whether he/she wants to trust his or her health information to a particular PHR vendor. No health care provider should be permitted to deny an individual's request for access based on the provider's unwillingness to request the upload of a PHR vendor's Trust Anchor to the HISP's certificate store.

### **Suggested Guidance**

To address health care providers' confusion and refusal to provide patients with access to their protected health information through Direct Messaging, we request that the Office for Civil Rights issue guidance clarifying that individuals have a right to receive their designated record set information in a PHR through Direct Messaging when a health care provider has certified

---

<sup>6</sup> 45 C.F.R. §§ 164.502(a)(2)(i) and 164.524.

<sup>7</sup> 42 U.S.C. § 17935(e); 45 C.F.R. § 164.524(c)(3)(ii).

<sup>8</sup> 45 C.F.R. § 164.524(c)(2)(i).

<sup>9</sup> An exception would be if a health care 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.

<sup>10</sup> 45 C.F.R. § 164.514(h).

EHR technology or other technology that readily supports such access. The following is potential guidance for your consideration:

### **Is an Individual Entitled to Have a Copy of Protected Health Information Sent to a Personal Health Record through Direct Messaging?**

#### **Answer**

Yes, when the covered entity has certified electronic health record (EHR) technology or other technology that readily permits the sending of designated record set information through Direct messages. Direct is a technical standard for exchanging health information between health care entities in a trusted network. 2014 Edition certified EHR technology is required to include the ability to send certain patient summaries using Direct Messaging. Many other health information technologies include the ability to send and receive Direct messages, including some personal health record (PHR) technologies.

Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's designated record set. See 45 CFR 164.524. Covered entities must provide the copy in the form and format requested by the individual, if readily producible. If an individual's request for access directs the covered entity to transmit the copy of protected health information directly to another person designated by the individual, the covered entity must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of protected health information.

If an individual provides a signed, written request that designated record set information be sent to a Direct address and the covered entity has the ability to send such information as a Direct message, then the covered entity is required to transmit the requested information to the Direct address that the individual provided. A Direct address may include "direct." in the e-mail address, such as [PatientName@direct.PHRvendor.com](mailto:PatientName@direct.PHRvendor.com). The covered entity may only deny the individual's request based on a reviewable or non-reviewable ground for denial set forth in 45 CFR 164.524(a).

Because Direct uses strong security to protect communications, the covered entity may need to take certain steps to start exchanging information with the individual's PHR vendor. For example, the covered entity may need to notify its EHR vendor or Health Information Service Provider ("HISP") that it wishes to send Direct messages to the individual's PHR vendor. The EHR vendor or HISP may need to upload the PHR's "trust anchor" (a digital certificate) to its systems in order to facilitate the exchange. To avoid having to make separate requests for each PHR vendor, the covered entity can request that its EHR vendor or HISP permit exchange with all members of the NATE Blue Button Patient Trust Bundle. This Trust Bundle (a collection of digital certificates), supported by the

HHS Office of the National Coordinator for Health Information Technology, includes a number of PHR vendors who have agreed to certain minimum privacy and security requirements.

Thank you for your consideration of our request. If you have any questions, please do not hesitate to contact Adam Greene at (202) 973-4213 or [AdamGreene@dwt.com](mailto:AdamGreene@dwt.com). We would be happy to have a meeting to further discuss this important issue.



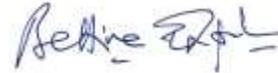
Max Wallace  
Chief Executive Officer  
Accelerate Brain Cancer Cure



Mark Heaney  
Chief Executive Officer  
Get Real Health



Nora Jean Levin  
Executive Director  
Caring From a Distance



Bettina Experton, M.D., M.P.H.  
President & CEO  
Humetrix



Gordon Raup  
Chief Technology Officer  
Datuit, LLC



Aaron Seib  
Chief Executive Officer  
National Association for Trusted Exchange



*Charles Ingoglia*

Charles Ingoglia  
Senior Vice President, Public Policy and  
Practice Improvement  
National Council for Behavioral Health



*Jeff Donnell*

Jeff Donnell  
President  
NoMoreClipboard

