An Attempt to Clarify the Use of Electronic Signatures and Electronic Delivery for HIPAA-Required Patient and Beneficiary Authorizations, Notices and Acknowledgments

By Jon Neiditz

My friends in the e-commerce world tell me that they continually run into representatives of HIPAA-covered organizations – usually providers – who maintain that HIPAA simply does not permit them to get electronic agreements to HIPAA authorizations or electronic acknowledgements of HIPAA privacy notices. I am happy to state emphatically that their belief is both false and ironic, which distinguishes it from many of the unintended consequences of HIPAA, that are instead true and ironic. HIPAA's ironically titled "Administrative Simplification" provisions were intended to enable some electronic transactions between providers and health plans. However, by requiring some standard transactions that many providers had trouble implementing, a true and ironic consequence of HIPAA's attempt to encourage electronic transactions was to force those providers into using paper for those same transactions.

Of course, between 1996, when HIPAA was enacted, and December, 2000, when the Clinton Administration issued the first final HIPAA privacy rules, something happened that changed the focus of those Administrative Simplification provisions a bit - the Internet. The issue of maintaining privacy of health information had become a prominent issue, and the complexity of the resulting privacy rules made privacy and information security the most visible components of HIPAA for much of the world.

In the draft of the HIPAA security regulations published in August of 1998, the Department of Health and Human Services (DHHS) noted the importance of electronic signatures in standardizing electronic health care transactions by stating that although "HIPAA does not require the use of electronic signatures[,] [t]his particular capability…would be necessary for a completely paperless environment." However, in the final security regulations that were not released until February 20, 2003, the DHHS stated that the final rule only adopted security standards and did not contain any standards or recommendations relating to electronic signatures. Instead, the DHHS stated that it would publish a final rule for electronic signatures at a later date. That publication never occurred.

Where does that leave HIPAA-covered entities in dealing with the HIPAA-required documents that mandate a patient or beneficiary signature? In the United States, state and federal laws from outside of the health care world provide a clear answer that one may rely on electronic signatures on such documents freely, as long as they are obtained and maintained correctly. A state law that has been enacted in 46 states called the Uniform Electronic Transactions Act or UETA and the federal e-signature law, the Electronic Signatures in Global and National Commerce Act or ESIGN (which preempts inconsistent state law other than UETA), **together assure that electronic signatures obtained and maintained with the proper process controls will be effective for all HIPAA-required documents throughout the United States.**

Because neither HIPAA nor any of the regulations issued under it specifically address the use of electronic signatures and none of the HIPAA-required documents are among the document types excluded by ESIGN or UETA, UETA applies to electronic signatures on HIPAA documents for intrastate transactions in UETA states and ESIGN applies to electronic signatures on HIPAA documents for interstate transactions and in non-UETA states if the laws of those states are inconsistent with ESIGN. Section 7(a) of UETA and Section 101(a) of ESIGN both state that a

~

signature may not be denied legal effect or enforceability solely because it is in electronic form. Therefore, an electronic signature can be used when a signature is required by a document governed by HIPAA, and is as legally enforceable against the signing party as a "wet ink" signature. Any electronic signature process – clicks, typed names, check boxes, you name it – will work as long as it is "attached to or logically associated with" the electronic HIPAA record or tangible HIPAA document, and as long as the process is a solid one.

And speaking of solid processes, the HIPAA security rules do dovetail nicely with ESIGN and UETA requirements for process controls. The security rules strongly encourage covered entities to "[i]mplement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner," and to "[i]mplement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."

The security of electronic transmissions containing protected health information (PHI) was considered important by the DHHS. In the draft of the HIPAA Security Regulations published in August of 1998, the DHHS suggested requiring all such communications be encrypted when transmitted over "open networks" such as the Internet or dial-up lines. The encryption requirement was removed, however, after the DHHS received an "overwhelming majority" of public comments voicing strong objections to the financial and technological burdens associated with mandatory encryption when using any media other than the Internet. In the end, the DHHS appeared to see encryption as a technology not quite ripe:

> Thus, we agree that encryption should not be a mandatory requirement for transmission over dial-up lines. We also agree with commenters who mentioned the financial and technical burdens associated with the employment of encryption tools. Particularly when considering situations faced by small and rural providers, it became clear ***that there is not yet available a simple and interoperable solution to encrypting email communications with patients.*** As a result, we decided to make the use of encryption in the transmission process an addressable implementation specification. ***Covered entities are encouraged, however, to consider use of encryption technology for transmitting electronic protected health information, particularly over the internet.***
> As business practices and technology change, there may arise situations where electronic protected health information being transmitted from a covered entity would be at significant risk of being accessed by unauthorized entities. ***Where risk analysis showed such risk to be significant, we would expect covered entities to encrypt those transmissions, if appropriate, under the addressable implementation specification for encryption.***" (emphasis added)

Of course, a lot has happened since 2003. Encrypted messages can be sent more easily between entities that use different encryption platforms. One product, **RPost's Registered E-mail service**, offers the sender and recipient an automatically returned encrypted copy of the original message and all attachments as they were received originally by the recipient's server (and therefore delivered legally under UETA). That product also allows anyone in possession of this returned "Registered Receipt" e-mail to verify the authenticity of the data it contains by employing hash algorithms that can be unlocked and used to regenerate the original electronic correspondence. Further, where risk analysis shows data privacy risk to be significant, the RPost system permits a one-click e-mail

encryption option that delivers the encrypted information to the desktop of the recipient without any complexity, website visits, or decryption keys.

HIPAA is ironic enough already; don't let HIPAA confusion force you to deal with your patients and beneficiaries only on a paper basis while at the same time moving toward electronic health records. Inexpensive solutions on the market today that are simple to use and deploy can serve as catalysts to help you and those you serve move from paper to electronic while remaining in compliance with HIPAA. One such tool is **RPost (www.rpost.com).**

About the Author: Jon Neiditz is a partner in Nelson Mullins Riley & Scarborough's Atlanta office and co-leader of the Firm's Information Management Practice. Jon's practice is focused on assisting his clients in meeting the challenges of electronically stored and sent information.