**Nelson Mullins**

**Nelson Mullins Riley & Scarborough LLP**
Attorneys and Counselors at Law
Atlantic Station / 201 17th Street, NW / Suite 1700 / Atlanta, GA 30363
Tel: 404.322.6000 Fax: 404.322.6050
www.nelsonmullins.com

# Memorandum

To: Zafar Khan and Frank Maguire

From: Jon Neiditz and Amanda Witt

Date: July 17, 2008

Re: Effective Electronic Delivery and Execution of Documents Required under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

---

## SUMMARY OF CONCLUSIONS

Based on our analysis below, we conclude:

(1) An RPost electronic signature can be used when a signature is required by a document governed by HIPAA , and is as legally enforceable and legally effective as a "wet ink' signature;

(2) RPost can be used to deliver documents electronically in conformity with the technical safeguard standards of HIPAA relating to the security of electronic communications of electronic PHI; and

(3) Where notification is required by HIPAA and in the great majority of U.S. jurisdictions in which UETA applies, RPost's core Registered E-mail service does provide the sender with legally valid evidence that notice has been accomplished under HIPAA,as long as RPost's resulting Registered Receipt e-mail reports at least successful delivery to the recipient's mail server.

## BACKGROUND & ANALYSIS

RPost (the "Company") offers the Registered E-mail® core service that provides the sender with legal proof of delivery, content and official time stamp. Additional service features include electronic signature, electronic contracting (eSignOff™), and end-to-end e-mail encryption. The RPost® services deliver a Registered E-mail® message to the recipient and automatically returns verifiable evidence in the form of a Registered Receipt e-mail containing a digital snap-shot of the content (message body and all attachments) and the official time the e-mail was sent and received by each recipient. The eSignOff™ feature incorporates a valid electronic signature of the recipient into the process. As a means of providing secure electronic communication, the Company's technology (a) does not store information on a central server; (b) maintains the integrity of electronic communications and the security of the transmission using cryptography; (c) provides the sender proof of delivery to the recipient; and (d) provides an encrypted, tamper-proof record of the

transaction that may include verifiable proof of both the delivery and acknowledgement or execution of any document.

The Company has asked us whether all documents governed by the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (1) may be signed, authorized or acknowledged using RPost's electronic signature when a signature is required and (2) may be delivered electronically by the RPost service. The documents required by HIPAA that involve notice to patients or beneficiaries or their agreement or acknowledgement include authorizations pursuant to 45 CFR Section 164.508, that must be executed by the patient or beneficiary and meet more standards evidencing intent than a mere consent, and notices of privacy practices for protected health information ("PHI") pursuant to 45 CFR Section 164.520, the receipt of which must be acknowledged by patients. Patients and beneficiaries also submit many types of requests under HIPAA, such as requests for special privacy protections, access to PHI, amendment of PHI and accounting of disclosures of PHI, pursuant to 45 CFR Sections 164.522 through 528. HIPAA also requires executed agreements or addenda between covered entities and their business associates, and between business associates and their subcontractors that process PHI.

Based on our analysis below, we conclude that (1) all of the documents required by HIPAA may be effectively executed and delivered electronically using the RPost service, (2) RPost's form of electronic signatures are as legally enforceable against the signing party as are "wet ink" signatures and are legally effective under HIPAA; and (3) RPost's electronic delivery is permitted under HIPAA in the context of a compliant information security program.

In reaching our conclusions, we have examined the federal electronic signature law, the uniform state law on electronic signatures and HIPAA. We have also relied upon our previous review of the Company's technology.

## A. Electronic Signature Laws

### 1. ESIGN vs. UETA

Except as otherwise noted in this Memorandum, the analysis under the Electronic Signatures in Global Commerce Act ("ESIGN")[1] (the federal statute) and the version of the Uniform Electronic Transactions Act, as published by the National Conference of Commissioners on Uniform State Laws ("UETA"), which forty-six states have adopted, is essentially the same for all relevant issues described herein.[2] For those states that have adopted electronic signature laws that are not consistent with ESIGN in areas relevant to the issues described in this Memorandum, such state laws will be preempted by ESIGN's broad preemption provisions if such state laws are inconsistent with ESIGN.[3] Specifically, ESIGN states that the general rule of ESIGN can be modified or limited by another law if (a) such law is an enactment or adoption of UETA and its exceptions to the scope of UETA are not inconsistent with ESIGN; or (b) such law specifies alternative procedures or requirements relating to the acceptance or use (or both) of electronic records or electronic signatures

[1] 15 U.S.C. Section 7001 (October 1, 2000).
[2] As of the date of this Memorandum, all but four (4) states (New York, Illinois, Washington and Georgia) have adopted a version of UETA, in one form or another. References to UETA that follow thus do not address the laws of those four (4) states.
[3] ESIGN Section 102(a).

if (i) such procedures are consistent with title I and title II of ESIGN; and (ii) such procedures are "technology neutral" such that they "do not require, or accord greater legal status or effect to, the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures."[4] Furthermore, with respect to electronic signature or electronic records laws other than UETA that modify or limit ESIGN, if such laws were enacted or adopted after the enactment of ESIGN, they must make a specific reference to ESIGN.[5]

Both ESIGN and UETA recognize that an electronic signature can be as legally effective as a signature applied manually on paper. Neither ESIGN nor UETA give electronic signatures an elevated or special status under the law or require a specific type of technology or electronic signature. Rather, ESIGN and UETA provide that a signature may not be denied legal effect *solely* because it is in electronic form. Consistent with UETA, the key provision of ESIGN acknowledging electronic signatures provides:

> (a) In General.--Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce-
>
> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
>
> (2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[6]

ESIGN, as does UETA,[7] gives equal recognition to electronic signatures, with the few exceptions mentioned below and which are not relevant to this Memorandum.

ESIGN and UETA will apply to the use of electronic signatures unless such signature is governed by a law excluded from the scope of the preemption provisions of ESIGN or UETA or if there is another governing, but consistent law that is "technology neutral" and specifically references ESIGN if such law was enacted after ESIGN. For example, following the effective date of ESIGN, certain federal governmental agencies, such as the Department of Labor and Securities and Exchange Commission, promulgated regulations relating to electronic signatures and electronic records. With an effective date of October 9, 2002, the Department of Labor's Pension Welfare Benefits Administration adopted Regulation 2520.140b-1, *Use of Electronic Communication and Recordkeeping Technologies by Employee Pension and Welfare Benefit Plans*. This regulation permits employee welfare benefit (including group health plans) employee pension plans and their plan sponsors and administrators to deliver in electronic form certain types of documents required under ERISA to plan participants if such participants have computer access and have agreed to receive such records electronically.

---

[4] ESIGN Section 102(a).
[5] ESIGN Section 102(a)(2)(B).
[6] ESIGN Section 101(a).
[7] UETA Section 7(a).

Section 101 of ESIGN, which permits the use of electronic records or signatures, will not apply to the following: (a) a contract or other record if it is governed by a law relating to the creation and execution of wills, codicils or testamentary trust, (b) certain areas of family law; and (c) the Uniform Commercial Code other than Sections 1-107 and 1-206 and Articles 2 and 2A.[8] Furthermore, the general permissibility of use of electronic signatures and records is, however, limited by ESIGN Section 103, which does not permit the use of electronic notices in the following circumstances: (a) court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings, (b) any notice of cancellation or termination of utility services (including heat, water and power), (c) notice of default, acceleration, repossession, forfeiture, or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of an individual, (d) notice of the cancellation or termination of health insurance or benefits (excluding annuities), (e) notice of recall of a product, or material failure of a product, that risks endangering health or safety, or (f) any document required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

UETA was designed "to facilitate electronic transactions consistent with other applicable law"[9] by simplifying, clarifying and modernizing "the law governing commerce and governmental transactions through the use of electronic means."[10] The following areas of law are excluded from the scope of UETA: (a) laws governing wills, codicils and testamentary trusts, (b) the Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2, and Article 2A, (c) the Uniform Computer Information Transactions Act, and (d) other areas of law that are specified by a particular state's law.[11]

None of the excluded areas above are relevant to the conclusions contained in this Memorandum.

2. Key definitions

If a signature is provided using an "electronic process" that is "attached to or logically associated with" the electronic record or tangible document comprising the application by a person intending to sign the application, such signature will be legally effective.[12] ESIGN defines an "electronic signature" as:

---

[8] ESIGN Section 103(a).
[9] UETA Section 6(1). All references herein to UETA shall be deemed references to the model UETA and its commentary published by the National Conference of Commissioners on Uniform State Laws in 1999.
[10] Commentary No. 1(c) to UETA Section 6(1).
[11] UETA Section 3. The Uniform Commercial Code ("UCC") is a model law adopted in all 50 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands that provides default rules for sales and other commercial transactions involving personal (i.e., moveable) property (not real property). The sections of the UCC excluded from ESIGN and UETA, although perhaps not as pervasive as the sales and leasing of goods, are quite pervasive, and particularly important in financial services: Negotiable Instruments (including banknotes and drafts (commercial paper)); Bank Deposits (including check collection); Funds Transfers (between institutions); Letters of Credit; Bulk Transfers and Bulk Sales (including auctions and liquidations of assets); Warehouse Receipts, Bills of Lading and Other Documents of Title (including storage and bailment of goods); Investment Securities (including assets in addition to securities); and Secured Transactions (transactions secured by a security interest).
[12] For ease of reading this Memorandum, the phrase "legally effective" is used, rather than the more technically correct phrase, "not be denied legal effect solely because such signature is an electronic signature."

> (5) Electronic signature.--The term "electronic signature" means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.[13]

ESIGN defines "record" as:

> (9) Record.--The term "record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.[14]

The same definitions used under UETA are consistent with those used in ESIGN. Thus, under both ESIGN and UETA, an electronic signature could consist of an electronic sound or symbol, such as an individual saying "I agree," typing "I agree" or following some other process, such as clicking "I agree," which is attached to or logically associated with information inscribed: (i) on a tangible medium, such as the tangible, hard copy of an authorization to disclose PHI to third parties under HIPAA; or (ii) stored in an electronic medium retrievable in a perceivable form, such as the electronic record containing identical information contained in the tangible hard copy that is delivered to an individual in a wet ink process.

To more fully understand the concept of "logically associated", the similarities between UETA and ESIGN are useful because of the official commentary included within UETA. UETA defines an electronic signature:

> (8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.[15]

UETA's official commentary relating to the "attached to or logically associated with" phrase in the definition acknowledges that an electronic signature, unlike a "wet ink" signature, may not be affixed to the actual document being signed:

> Another important aspect of this definition lies in the necessity that the electronic signature be linked or logically associated with the record. In the paper world, it is assumed that the symbol adopted by a party is attached to or located somewhere in the same paper that is intended to be authenticated, e.g., an allonge firmly attached to a promissory note, or the classic signature at the end of a long contract. These tangible manifestations do not exist in the electronic environment, and accordingly, this definition expressly provides that the symbol must in some way be linked to, or connected with, the electronic record being signed. This linkage is consistent with the regulations promulgated by the Food and Drug Administration. 21 CFR Part 11 (March 20, 1997).[16]

[13] ESIGN Section 106(5).
[14] ESIGN Section 106(9).
[15] UETA Section 2(8).
[16] UETA Section 2, Official Comment 7. The referenced FDA Regulation is not relevant to this analysis.

As with a signature applied in "wet ink", evidence of a person's intent to sign the record (which would be required if the person signed in blue ink on a piece of paper) may be inferred from words in close proximity to the place of the signature where such words indicate in clear and conspicuous terms the person's intent to sign and be bound thereby.

## B. The Absence of Electronic Signature Requirements or Prohibitions under HIPAA

As of the date of this Memorandum, neither the Administrative Simplification provisions of HIPAA nor any of the regulations promulgated under those provisions contain any prohibition or requirement of use of electronic signatures, nor are any HIPAA-required documents, which include executed authorizations, notices, etc.) specifically excluded from the scope of ESIGN, UETA or the non-UETA states.

When developing the final security regulations that were released on February 20, 2003 ("HIPAA Security Regulations")[17], the Department of Health and Human Services ("DHHS") contemplated requiring the use of digital signatures by covered entities. Digital signatures are a type of electronic signature that employ encryption through mathematical algorithms to secure the signature. In the draft of the HIPAA Security Regulations published in August of 1998, the 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."[18] However, in the final version of the HIPAA Security Regulations, 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.[19] As of the date of this Memorandum, no rule on electronic signatures has been issued by the DHHS.

Because HIPAA is not specifically excluded from ESIGN or UETA and neither HIPAA nor any of the regulations promulgated under it specifically address, require or prohibit the use of electronic signatures, the applicable electronic signature law, either ESIGN or UETA[20], would apply to permit the use of an electronic signature when a signature is required by a document governed by HIPAA. Specifically, Section 101(a) of ESIGN and Section 7(a) of UETA 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 legally enforceable against the signing party as would a "wet ink" signature and legally effective under HIPAA.

Although its technology was developed in other contexts, RPost's technology appears to be particularly well positioned to satisfy any sender signature or recipient signoff requirement of forms, waivers, or documents required under HIPAA. RPost's form of electronic signature and eSignOff are valid forms of signature for documents governed by HIPAA.

---

[17] Subchapter C of Title 45 of CFR, Parts 160, 162 and 164. For an electronic copy, see http://www.cms.hhs.gov/SecurityStandard/ .
[18] Fed. Reg., Vol. 63, No. 155 at 43260 (Aug. 12, 1998).
[19] Fed. Reg., Vol. 68, No. 34 at 8335 (February 20, 2003).
[20] ESIGN would apply to electronic signatures used in interstate transactions and in non-UETA states if the laws of those states were inconsistent with ESIGN and UETA would apply to electronic signatures used in intrastate transactions in UETA states.

## C. Secure Electronic Communication and Transmission Requirements under HIPAA

Although the HIPAA Security Regulations specifically contemplate the secure transmission of electronic protected health information ("PHI"), neither the Administrative Simplification provisions of HIPAA nor any of the regulations promulgated under those provisions as of the date of this Memorandum contain any prohibition or requirement of use of electronic delivery of documents governed by HIPAA. The HIPAA Security Regulations strongly encourage covered entities[21] to "[i]mplement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."[22] Furthermore, such regulations also encourage covered entities 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."[23]

The security of electronic transmissions containing 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 to be encrypted when transmitted over "open networks" such as the Internet or dial-up lines. The encryption requirement was removed 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. Unfortunately, as noted below in the DHHS commentary, the requisite technology for secure electronic communications was not yet widely available when the final HIPAA Security Regulations were released in 2003. The DHHS noted as follows:

> 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.***[24] (emphasis added)

---

[21] A "covered entity" is one or more of the following types of entities: (a) a health care provider that transmits any health information in electronic form in connection with a transaction covered by HIPAA; (b) a health care clearinghouse; or (c) a health plan. 45 CFR § 160.103.

[22] 45 CFR § 164.312(c)(2).

[23] 45 CFR § 164.312(e)(1).

[24] Fed. Reg., Vol. 68, No. 34 at 8357 (February 20, 2003).

Although its technology was developed in other contexts, RPost's technology appears to be particularly well positioned to satisfy HIPAA's technical safeguard provisions regarding the preservation and secure transmission of electronic PHI. RPost's Registered E-mail® messages may be sent using RPost's end-to-end encryption service, and such PHI is not stored on a central server controlled by the Company. The Company's Registered Receipt™ e-mail includes an encrypted copy of a sender's original message and all attachments as they were received by the recipient's server. Anyone in possession of that receipt, as attested by the Company, is able to verify the authenticity of the data it contains by sending a copy of the receipt to an e-mail address controlled by the Company where the Company's cryptographic methods are used to determine if information in the receipt has been altered, employing hash algorithms and RSA/PKI signatures. Once verified as authentic, RPost regenerates the validated electronic original e-mail and all attachments and returns a copy to the sender (or recipient, or both as an option).

## D. Conclusion

Because neither HIPAA nor any of the regulations promulgated under it specifically address the use of electronic signatures and HIPAA is not specifically excluded from ESIGN or UETA, UETA would apply to electronic signatures used in intrastate transactions in UETA states and the provisions of ESIGN would apply to electronic signatures used in interstate transactions and in non-UETA states if the laws of those states were inconsistent with ESIGN. Specifically, Section 7(a) of UETA and Section 101(a) of ESIGN state that a signature may not be denied legal effect or enforceability solely because it is in electronic form. Therefore, an RPost electronic signature can be used when a signature is required by a document governed by HIPAA, can be as legally enforceable against the signing party as would a "wet ink" signature and can be legally effective under HIPAA.

With respect to the electronic delivery of documents governed by HIPAA, the HIPAA Security Regulations specifically contemplate the secure transmission of electronic PHI, but neither the Administrative Simplification provisions of HIPAA nor any of the regulations promulgated under those provisions as of the date of this Memorandum contain any prohibition or requirement of use of electronic delivery of such documents. Accordingly, the RPost's technology can be used to deliver such documents electronically in conformity with the technical safeguard requirements of the HIPAA Security Regulations relating to the integrity and security of electronic communications of electronic PHI. Finally, where notification is required by HIPAA and in the great majority of U.S. jurisdictions in which UETA applies, RPost's core Registered E-mail service does provide the sender with legally valid evidence that notice has been accomplished under HIPAA, as long as RPost's resulting Registered Receipt e-mail reports at least successful delivery to mail server.

* * * *

This Memorandum contains a summary of complex regulatory issues, and we recommend that each reader seek the advice of independent legal counsel with respect to any matter discussed herein.