Thomas M. Susman
Director
Governmental Affairs Office

Defending Liberty
Pursuing Justice

AMERICAN BAR ASSOCIATION
740 Fifteenth Street, NW
Washington, DC 20005-1022
(202) 662-1760
FAX: (202) 662-1762
SusmanT@staff.abanet.org

July 21, 2009

The Honorable Michael J. Astrue
Commissioner
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235-7703

Dear Mike:

As you requested, the ABA explored the issues related to the use by the Social Security Administration (SSA) of electronic signatures for applications and authorizations to disclose medical information. The ABA supports the use of electronic signatures by the government when appropriate security techniques, practices, and procedures have been adopted for the signatures, provided the government addresses in detail the manner in which the privacy and security of personal health information is to be protected.

The ABA formed a Subcommittee on SSA Disability and Electronic Signatures as part of the ABA's Medical Records Project to study the issue. Thomas Smedinghoff, Past-Chair of the Section of Science and Technology conducted extensive research on the subject and, based on a meeting and other exchanges with the ABA Governmental Affairs Staff and the Subcommittee, developed the enclosed list of issues that the ABA believes should be addressed if electronic signatures are to be used for applications and authorizations to disclose medical information. We hope that this list is helpful to you. A roster of the ABA's Medical Records Project Subcommittee on SSA Disability and Electronic Signatures is enclosed.

If we may be of further assistance please let me know. I know that the Subcommittee, and certainly GAO, would welcome the opportunity to discuss this issues list and potential next steps with you or your staff so that we can continue to move forward on this important issue.

Best regards,

Thomas M. Susman

Enclosures

Issues to Address:

The Privacy Concerns of Individuals

In utilizing electronic signatures, SSA should continue to ensure that it protects the confidentiality of personally identifiable health information from any source, including medical records, electronic data, and genetic material. It should address in detail the manner in which the privacy and security of personal health information is to be protected.

Process for Electronic Signatures on Form SSA-827

Note: The following list assumes that both federal law (e.g., the federal E-SIGN Act,[1] SSA regulations, HIPAA, etc.) and state law (e.g., the state enactments of the Uniform Electronic Transactions Act or UETA[2]) will be relevant to this analysis. This will need to be verified, as it may be that only federal law is applicable.

1. **Authorization:** Confirm that each element of the transaction can legally be done in all-electronic form. This is unlikely to be a concern, but it should be verified that each element of the proposed electronic SSA-827 authorization process is not prohibited by E-SIGN, a state enactment of UETA, or some other statute or regulation (e.g., SSA regulations).

2. **Signer Authentication:** The SSA must determine how the signer's identity will be authenticated. This is a critical issue, and is complicated where multiple signatures are required on the form.

   From an evidentiary perspective, authentication requirements will be implied with respect to each electronic SSA-827 authorization form coming from, or signed by, the signer. That is, SSA will need the ability to prove up "who" signed the applicable form. That proof may not necessarily come from the signature itself. Authentication may also be a regulatory requirement, e.g., under SSA or HIPAA regulations.

3. **Agreement:** If UETA applies, the SSA must require some evidence that the signers agree to execute the SSA-827 authorization form in electronic form (although such "agreement" may be implied from their conduct). UETA Sections 5(b) and 5(c).

---

[1] Electronic Signatures in Global and National Commerce Act (hereinafter "E-SIGN"), 15 U.S.C. 7001 et. seq., effective October 1, 2000. E-SIGN is available at www.ntia.doc.gov/ntiahome/frnotices/2002/esign/report2003/ElectronicSignaturesAct.pdf. E-SIGN preempts all inconsistent state legislation, other than state enactments of UETA in the form promulgated by NCCUSL.

[2] Uniform Electronic Transactions Act (hereinafter "UETA"), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999. A copy of UETA is available at www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm. As of May 2009, 46 states and the District of Columbia had enacted UETA.

UETA imposes a general consent requirement that applies to all parties to the transaction. Specifically, UETA is structured as an "opt-in" statute, such that the Act "applies only to transactions between parties each of which has agreed to conduct transactions by electronic means." In other words, if the parties have not agreed to conduct their transaction electronically, UETA will not apply. Thus, it may be necessary to ensure that the electronic transaction is structured so as to provide some evidence that the parties have agreed to execute the SSA-827 authorization form in electronic form.

4. **Signer Consent to Receive "In Writing" Information in Electronic Form.** If signing the SSA-827 form requires the delivery of information to the signer "in writing" and SSA wants to deliver that information electronically, it will be necessary to make certain disclosures to the signer, and get his or her electronic consent to delivering the required information electronically. E-SIGN 15 USC 7001(c). Is does not appear that this is an issue here, but it should be verified just in case.

5. **Opportunity to Review:** The complete electronic SSA-827 authorization form must be clearly displayed on the computer screen so that the signer has an adequate opportunity to review the document, print the form, and download a copy of the form, if so desired, before signing the form.

   Cases involving electronic contracts suggest that the SSA must provide the signer with an *opportunity to review* the terms of the SSA-827 authorization form before signing it. Courts consistently hold that, in order to enforce a standard form contract, the user must have the opportunity to review the terms. *Actual review* of the contract by the signer is not required for enforceability. Providing a signer with a reasonable opportunity to review the form requires that: (1) the form must be "made available in a manner that ought to call it to the attention of a reasonable person and permit review," and (2) the signer must also have the right to decline to sign the form.

6. **Design an Understandable Electronic Signing Process:** The SSA must design a signing process that appropriately conveys to the signer the significance of his/her actions. In particular, such process must:

   (a) make clear to the signer that he or she will be doing something with legal significance (i.e., affixing a legally binding signature);
   (b) clearly specify what it is that the signer is signing/agreeing to;
   (c) clearly specify what action or conduct constitutes the act of "signing;"
   (d) be sufficiently easy for the signer to use and create
   (e) clearly specify what the signature means (e.g., "I authorize disclosure," "I know the person signing this form, and witnessed his/her signature");
   (f) be readily understood by the signer; and
   (g) clearly give the signer a choice of proceeding or not proceeding.

7. **Use a Legally Compliant Form of Electronic Signature:** The electronic signature used to sign the SSA-827 authorization form must: (1) consist of a sound, symbol, or process, (2) be attached to or logically associated with the electronic SSA-827 record being signed, and (3) be executed or adopted by a person with the intent to sign the record. E-SIGN 15 USC 7006(5); UETA Section 2(8)

   (a) Sound, Symbol or Process: The SSA must select a form of signature that will be easy to execute yet reasonably recognizable by the signer as a signature (e.g., an "I Agree" button, a digitized handwritten signature executed on a signature pad, typing one's name, following appropriate instructions, etc.).

   (b) Attach Signature: The SSA must ensure that the system is programmed so that the signer's electronic signature, once executed, is attached to or logically associated with the electronic record being signed, is date and time stamped, and is recorded and/or saved in a tamper-evident format (or protected by other appropriate security procedures) designed to provide appropriate security for the authenticity and integrity of the form.

   (c) Evidence Intent: SSA must ensure that the signing process clearly sets forth the intent with which the signature is made (e.g., "I authorize disclosure," "I know the person signing this form, and witnessed his/her signature," etc.) so that there is clear evidence of the signer's intent when signing the record, and the signer clearly understands the legal significance of the signing act. Signers should not be able to later argue that they thought they were simply typing their name in a form or clicking on a "next" button to get to the next screen in the process.

8. **Record Accessibility:** Following signature, the signed copy of the SSA-827 authorization form should be available for downloading and/or printing by the signatory. E-SIGN 15 USC 7001(e); UETA Sections 8(a), 8(d)(1), and 8(c). This means that SSA cannot do anything to inhibit downloading or printing of the form by the signer.

9. **Posting, Display, and Formatting of Documents.** If any applicable substantive law requires the SSA-827 authorization form to be "posted or displayed in a certain manner" or "formatted in a certain manner," (i) it must be determined whether that can that be done electronically, and (ii) if so, those requirements must be satisfied. E-SIGN 15 USC 7001(f); UETA Sections 8(b)(1) and (b)(3). [This may be unlikely]

   This rule addresses additional requirements that might be imposed by some other substantive law that might affect the legal enforceability of an electronic record in a particular case. It is a savings provision for laws (e.g., paper-based regulations) that provide for the means of delivering, displaying, or formatting information and which are not affected by UETA or E-SIGN. Under this rule, paper-based display, delivery and formatting requirements will continue to be applicable to electronic records and signatures. If those legal requirements can be satisfied in an electronic medium, e.g., the information can be presented in the equivalent of 20 point bold type as required by some other applicable law, then UETA and E-

SIGN will validate the use of the electronic medium, leaving to the other applicable law the question of whether the particular electronic record meets the other legal requirements.

10. **Method of Delivery of Documents.** If any applicable substantive law requires the SSA-827 authorization form to be "sent, communicated, or transmitted by a specific method," (i) it must be determined whether that can that be done electronically, and (ii) if so, those requirements must be satisfied. UETA Section 8(b)(2). [This may be unlikely]

    This rule also addresses additional requirements imposed by other law which may affect the legal effect or enforceability of an electronic record in a particular case, and also operates as s a savings provision for laws that provide for the means of delivering information in a paper-based environment which are not affected by UETA. For example, if a law requires delivery of notice by first class US mail, that means of delivery would not be affected by UETA. The information to be delivered may be provided on a disk, i.e., in electronic form, but the particular means of delivery must still be via the US postal service. Delivery requirements will continue to be applicable to electronic records and signatures.

11. **Record Retention / Electronic Recordkeeping:** The signed electronic SSA-827 authorization form should be retained by SSA in a manner that complies with applicable electronic record keeping requirements, including applicable security procedures to ensure that the signed record accurately reflects the information set forth in the record at the time of signing and that it remains accessible to all persons who are entitled to access, in a form that is capable of being accurately reproduced for later reference. E-SIGN 15 USC 7001(d)(1); UETA Section 12(a).

    This rule requires that there exist reliable assurance that the electronic record accurately reproduces the information. This is consistent with Fed.R.Evid. 1001(3) and Unif.R.Evid. 1001(3) (1974). This rule assures that information stored electronically will remain effective for all audit, evidentiary, archival and similar purposes. The requirement of accuracy is derived from the Uniform and Federal Rules of Evidence. The requirement of continuing accessibility addresses the issue of technology obsolescence and the need to update and migrate information to developing systems.

12. **Transaction Information Disclosure:** To the extent that any applicable law governing e-transactions (e.g., via websites) requires the up-front disclosure of specific relevant transaction information to the signer, those requirements must be satisfied.

    California law, for example, requires vendors conducting business through the Internet to disclose their legal name, street address, and return and refund policy.[3] Such a disclosure can be in writing or by electronic means, but it must occur *before* the vendor accepts any payment or processes any credit card or funds transfer. While this law is likely not applicable here, it is this type of law that must be addressed if it exists.

[3] California Business & Professions Code, Section 17538(d).

13. **Information Security Requirements:** To the extent that applicable laws and regulations require that appropriate information security for the records and information comprising the electronic transaction, those requirements must be satisfied.

    The federal government (e.g., via FISMA) and several states have enacted laws imposing a general obligation to ensure the security of personal information. These laws generally require businesses to "implement and maintain reasonable security procedures and practices" to protect personal information about residents from unauthorized access, destruction, use, modification, or disclosure.

14. **SSN Security Requirements:** Several federal and state laws and regulations also provide special rules requiring certain information security (e.g., encryption) be provided when SSNs are communicated or stored in certain cases. Since the SSA-827 form includes SSN this will likely be an issue. For example, when the signed SSA-827 form is communicated over the Internet (from the signer to the SSA, from the SSA to a healthcare provider or to a court, etc.), these laws often require that the data be encrypted.

15. **Website Privacy Policy Requirements:** To the extent that the SSA-827 form will be delivered via an SSA website, and to the extent applicable laws and regulations require that websites post privacy policies for the personal information collected via the website, those requirements must be satisfied.

    For example, California Civil Code § 22575 requires an operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual signers residing in California to conspicuously post its privacy policy on its Web site. While that law likely does not apply here, as I assume this is not commercial, that is the issue.

16. **Data Destruction Rules:** To the extent that applicable laws and regulations govern the destruction of any SSA-827 records, those requirements must be satisfied. At present, HIPAA includes such requirements, as well as at least 19 state laws. SSA and/or FISMA may also impose such requirements.

    Data destruction laws typically do not require the destruction of data, but seek to regulate the manner of destruction when businesses decide to do so. They generally require companies to properly dispose of personal information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. With respect to electronic information, such regulations typically require implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing signer personal information so that the information cannot practicably be read or reconstructed.

17. **Transaction-Specific and/or Industry-Specific Electronic Transaction Requirements:** There may also be electronic requirements in substantive healthcare laws, SSA regulations,

or evidentiary requirements that must be satisfied, in which case SSA must design / review the proposed processes to ensure that those requirements are met. (Note: These requirements appear in laws governing substantive transactions, and are often unique to the type of transaction involved).

One example, is the laws regulating collection, use, communication, and storage of SSN numbers. Several states have enacted laws that prohibit requiring an individual to transmit his or her Social Security number over the Internet unless the connection is secure or the individual's Social Security number is encrypted. The law in Maryland and Nevada goes further, and prohibits initiating any transmission of an individual's Social Security number over the Internet unless the connection is secure or the Social Security number is encrypted.