

The HIPAA Electronic Signature Rule¹

Bill Pankey
Tunitas Group

Public Law 104-191 (HIPAA) requires the Secretary of HHS to promulgate standards for the “electronic transmission and authentication of signatures with respect to the [HIPAA] transactions”. The effect of that adopted signature standard would be to satisfy any Federal or state statutory requirement for signatures in the listed transactions. However, since there are very few, if any, laws or regulations that require signature on the industry’s administrative transactions, HHS has apparently given the electronic signature rule little attention². Such inattention may prove to be a mistake, as the lack of an effective signature standard will significantly retard achieving benefits of administrative simplification. This paper will detail the importance of signature to healthcare transactions and the inadequacy of various HIPAA proposals relative to support of the needed electronic signatures. The paper will then analyze the logical alternatives for electronic signature support and offer recommendations for the HIPAA electronic signature standard.

Summary of this Paper’s Conclusions

1. Without appropriate electronic signature support, the proposed HIPAA Standard for Health Claims Attachments will generally be ineffective in responding to many of the purposes for which health plan’s request attachments.
2. Without appropriate electronic signature support, HIPAA’s ‘must accept’ rules will lead to *less* accountability for healthcare claims than currently possible with paper based attachments.
3. HL7’s lack of support for electronic signature transmission limits its utility for healthcare claims attachments. To maximize the utility of the electronic claims attachment and to avoid causing further deterioration of claims accountability, HL7 must support definition of data elements for signature transmission.
4. The business purposes of signature in the healthcare reimbursement processes create functional and non-functional requirements for electronic signature solutions.
5. Requirements analysis recommends a digital signature standard for the signatures needed in healthcare reimbursement transactions.
6. Digital signatures in support of healthcare reimbursement transactions can be cost effectively implemented on an industry scale.

The Importance of Signature in the Reimbursement Process

Currently, more than 20% of all healthcare claims are rejected pending examination of the billed treatments’ appropriateness, compliance with plan protocol, or medical necessity. Primary input to such examinations are the patient records supplied by claim submitters. Patient records transmitted to plans include, for example, admission sheets, H&P, progress notes, operative reports, treatment plans, consultative reports, discharge summaries and certifications of medical necessity. These sorts of patient records constitute the bulk of what is generally known as healthcare claim ‘attachments’. The electronic transmission of these from provider to plan is subject to standardization under HIPAA.

¹ A version of this paper will be published in the August, 2002 edition of e.healthrecord.news. The author welcomes questions and comments on the content of this paper. The author’s email address is bpankey@tunitas.com.

² The 1998 HIPAA “Security and Electronic Signature” NPRM did give desultory treatment of an electronic signature standard. HHS personnel have subsequently announced in public meetings and on public lists that signature will not be addressed concurrently with the HIPAA Security Final Rule. This should be read as a withdrawal of the NPRM’s statements vis a vis the signature rule. Subsequent to publication of the NPRM, NCVHS has heard testimony regarding electronic signature without finding a clear directive in that testimony.

Generally speaking, each of the attachments listed above is signed by a medical practitioner prior to transmission to the health plan. This use of signature arises not so much from an explicit requirement set by health plans as it does from historical industry practice. A collection of state laws and regulations, JCAHO information management standards, as well as Medicare Conditions of Participation support the general expectation that medical record entries and clinical orders need to be authenticated with the signature of the practitioners responsible for the care. Furthermore providers rely upon such signatures as a quality check on records; it is typical for institutions not to release any patient record until it has been signed by the responsible practitioners. Therefore, when imaged or paper copies of records are transmitted to plans, those copies, as a matter of course, include the signature of responsible practitioners. In this way, when plans receive patient records as 'attachments' today, they receive records that are authenticated with the signature of responsible practitioners.

It is fair to ask if plans actually require the currently available levels of patient record accountability. Is it only an unintended consequence of provider controls that practitioner signatures of patient records are communicated to plans and that plans do not rely upon such signatures? This is not likely to be the case.

Plan issued provider manuals (such as Medicare's Conditions of Participation) establish conditions for acceptable patient record practice which include authentication of entries using the author's signature (or initials or computer code). Plans' 'provider manuals' state with precision what constitutes an acceptable patient record including the need for authentication of record entries, but the manuals do not state the conditions under which plans would readily process and rely upon *unauthenticated* fragments of patient records. However, in our surveys of healthplan personnel, we encountered significant discomfort at the prospect of adjudicating claims exclusively on the basis of unauthenticated patient records. The impression left with our surveyors was that plans so expected patient records to be signed and that such records would be available to them, that few had explicit policy having to do with unsigned records.

The reason for such discomfort is apparent in various testimonies before the NCVHS on the topic of the HIPAA claims attachment standard³. There plan personnel testified that among the typical purposes for which attachments are requested are to "provide evidence of medical necessity", to "verify whether the service was actually performed", and to "verify that services were ordered by a physician". A dominant thread heard throughout NCVHS testimony was that attachments are collected for their *evidentiary* value in ensuring a plan's control over reimbursement and to reduce fraud and abuse. Without practitioner signature, the value of the attachments for such purposes is substantially reduced. For example, a provider institution can always *assert* to the healthplan that some procedure has been ordered by a physician. However, where the plan suspects fraud on the part of the institution, the institution's mere assertion of legitimacy obviously does not reduce suspicion. If a plan routinely accepts as authentic whatever the suspected institution submits to it, then, for many of the plan's purposes, it just as well not request the attachment. Clearly, reproduction of the physician's signed order goes further to reduce suspicion than does mere statements that such an order did exist. Attachments without signatures are mere assertions; attachments including the signatures of responsible individuals have greater weight.

The author of this paper understands that health plans routinely accept unauthenticated patient information and adjudicate many claims with such records. For example, a plan may accept the hemocrit reading from the provider's lab system without further authentication in approving payment for a dialysis treatment. It is this paper's position, though, that, in principle, at least some patient records need be signed to support the plan's purpose in requesting those records.

³ The National Committee of Vital and Health Statistics, NCVHS, collects industry input while preparing its recommendations to the Secretary of HHS on HIPAA and other matters. It has conducted several sessions devoted to 'healthcare claim attachments'; transcripts from these sessions can be found at <<http://www.ncvhs.hhs.gov/>>

For example, where the plan anticipates subsequent dispute over, say, denial of treatment authorization, the plan will certainly want the documentation on which it based the adverse decision to withstand a challenge to authenticity. To ensure as much, the plan would, at a minimum, collect and retain the practitioner signatures on authored reports.

The favored proposal⁴ for the HIPAA claims attachment standard *does not* ensure that signatures can be transmitted as part of the attachment. It does provide a mechanism to assert various signature aspects such as signing date and signer name, but such aspects themselves do not authenticate the patient information. Therefore, under the proposed standard, practitioner authentication of those records can, at best, only be assumed. Presumably, HIPAA's 'must accept' rules will prevent plans from seeking, in lieu of the standard X12.275 transaction, only paper or imaged records that include the practitioner's signature. Furthermore, since the HIPAA attachment standard will establish, *de jure*, what satisfies a plans' request for additional patient information, plans simply will not be allowed to delay adjudication until receipt and processing of other, possibly non electronic, information that the plan may require to authenticate the information in the claim attachment. Consequently, the proposed HIPAA scheme for attachments provides less accountability than does current paper based process. Since a significant purpose of the claim attachments is to ensure appropriate accountability for healthcare claims, it may well be the case that electronic claims attachments without signature will fail to satisfy plan needs in requesting them. While not all claim attachments need be signed, clearly some do and so its is the position of this paper that any attachment standard mandated thru HIPAA should support the 'transmission and authentication' of signatures associated with the attached documents.

The Electronic Signature Requirement

The "Electronic Signatures in Global and National Commerce Act" (US Public Law 106-229 aka E-SIGN), defines in law, an electronic signature as "any electronic sound, symbol, or process attached to or logically associated with a contract or record and executed or adopted by a person with the intent to sign the record". Further, the law ensures that electronic signatures, with only a few exceptions related to consumers, have full legal effect. E-SIGN is preemptive of contrary state law and E-SIGN directs all federal state regulators to rewrite their rules to support the use of electronic signature and record keeping. Although June 1, 2001 was the E-SIGN mandated deadline for the rewriting of rules, few federal or state agencies have to date fully complied. .

Following E-SIGN, the electronic signatures required by HIPAA must be supported by a security framework that allows the signature's attribution to a specific person (natural or not) and a binding of the signature with the particular document. While any number of technologies allegedly provide *the* framework sufficient for the industry's needs, consideration of various non functional requirements simplifies choice among them. In particular, the HIPAA Law is quite explicit⁵ that the promulgated electronic signature must have the effect of reducing the administrative cost of healthcare.

Signature acquisition and retention is a source of enormous cost to the industry. The reason for this is well understood. In healthcare, signatures are typically collected a significant time after the to be authenticated records are created. For example, clinical notes, reports and summaries are signed subsequent to transcription of the practitioner's dictation. Similarly, verbal orders are recorded by the dispensing nurse or unit secretary for subsequent authentication with ordering practitioner's signature. Since these sorts of documents are signed following treatment, practitioners tend to discount their importance and see record signing as an inconvenience.

⁴ HL7 and the X12N have jointly developed a recommendation that "claims attachments" be supported by enveloping standard HL7 messages inside of a BIN (binary) segment of a X12.275 "Patient Information" transaction. Although not yet the subject of an NPRM, it is generally acknowledged that HHS currently favors this proposal. For more information, see < <http://www.hl7.org/Library/Committees/ca/CATutRSNA.pdf> >.

⁵ sec 1172(b)

Frequently, HIM departments must engage in 'signature chases' which are accomplished always with significant expense and inconvenience but usually only with mixed success. Therefore rather than introduce requirements for additional signature acquisition, a cost effective HIPAA signature standard must support the use, for administrative purposes, of the signatures now collected for clinical purposes. This is accomplished in today's paper world as the practitioner's simple handwritten signature serves the multiple purposes. The challenge is to avoid a HIPAA standard that effectively requires implementation of distinct and duplicative electronic signature for reimbursement and clinical processes. The electronic signature technology used for attachments must be implementable in the clinical systems and processes that currently collect signatures for compliance purposes.

Unfortunately, the industry's current electronic signature practice does not well support the attachment transaction. The procedures explicitly endorsed in JCAHO's IM7 standards and multiple state law involves electronic 'signature' by entry of the practitioner's unique computer code. Assignment of the code is accompanied by an attestation whereby the practitioner promises to reserve the code to the practitioner's exclusive use and to accept responsibility for signatures created by that use. Unfortunately, this scheme does not create a signature representation that exists independent of the application implementing the scheme. This sort of "signature" is only implicit in the enforcement of the application's logic, e.g. 'record entries are committed only after entry of the user's computer code'. Current practice then provides 'nothing' that can be transmitted to third parties (e.g. plans) other than an assertion that the record was, in fact signed. As argued above, such assertions will not always satisfy the needs of plans in adjudicating claims. To support reimbursement documentation needs, current electronic signature practice simply must change. For a electronic signature technology to be useful for the attachment transaction, it must involve a signature representation that is independent of the implementation creating the signature.

Transmission of Signatures

The HIPAA Law calls for a standard vehicle for the transmission of electronic signatures. This is taken to mean some sort of common format by which any signature required by the standard transactions may be transmitted to any transaction recipient. For the sake of this discussion, our concern is with the transmission of the practitioner signatures that authenticate patient information in the healthcare claim attachment transaction. We assume that the attachment transaction will have the basic form of the X12N - HL7 proposal, to wit the encapsulation of HL7 encoded patient information in a BIN segment of an ANSI X12.275 transaction.

There are apparently three logical alternatives for the transmission of signatures in the above scheme: 1) signatures could be applied to the HL7 content and inserted in the BIN segment; 2) signatures could be applied to the BIN segment or relevant 275 transaction set; 3) signatures could be applied to the entire X12.275 message containing the attachment transaction.

Signatures and HL7. It is desirable that the applications that create the native HL7 messages also implement the technology that records the practitioner's signature. This approach is economical of the practitioner's time and effort as the practitioner is generally otherwise involved with those applications for record creation and / or access. Here the idea is that the practitioner could create the electronic signature as they make record entries or validate transcriptions and summaries. Such signatures would then become part of the HL7 data stream and transmitted to plans as part of the HL7 encoded data.

Unfortunately, HL7 currently does not support an HL7 field dedicated to 'signature'. Because of this deficiency, there is simply no standard place to insert the signature representation within HL7. The topic has been discussed within HL7 as recently as last April's HL7 meetings, but the effort to develop such support has not been assigned a high priority. To effectively accomplish signature transmission, there also need be definition of additional LOINC codes, such as for

'provider signature' to complement the existing LOINC code for 'provider signer'. Even as that is accomplished, it is also necessary to extend current HL7 data types to support of a general signature syntax(es) such as those using ASN.1 "Basic Encoding Rules"⁶ to represent digital signatures (e.g. PKCS#7⁷). For these purposes, the HL7 'encapsulated data' (ED) type holds promise. This data type allows for Base64 or HEX encoding which seems sufficient for signature representations. The appropriate 'type of data' would apparently be 'AP' (for 'other application data') which is typically arbitrary binary uninterrupted within HL7. While the subtype 'xml' works for some representations such as that found in xml-dsig, a subtype like 'ASN.1' probably should be added for PKCS#7 representations.

This being said, there is a current, but limited, capacity within HL7 to include practitioner signatures. Among other things the 'encapsulated data' type is intended to support 'image data', specifically in a 'TIFF' format as would be constructed in everyday faxing or scanning of documents. Using this type, a provider can transmit, using the HIPAA attachment standard, a scanned image of a practitioner signed report. While such an approach is likely to meet an immediate business need, it hardly advances the 'administrative simplification' agenda in that, among other things, it essentially requires acquisition of the practitioner signature on a *paper* report. While the enveloping of the scanned data inside the X12.275 message *might* provide some beneficial transmission control, the provider could just as well choose to fax the paper document to the payer and avoid the X12 cost and complexity.

In the absence of movement by the HL7, signatures could still be supported in the BIN segment. By X12 specification, the BIN segment encapsulates arbitrary (possibly binary) data. Therefore the attachment implementation guide, could be modified to include support for inclusion of a signature representation in addition to the HL7 encoded data. To do this, the guide would have to specify some internal structure to the BIN segment that allows parsing the signature and HL7 data out of the BIN.

Signatures and X12. X12 does support transmission of signature information in an X12.275 transaction with methods defined in the X12.58 "Security Structures". X12.58 describes a method of applying electronic signatures to X12 "Transaction Sets" (delimited by ST/SE segments) and "Functional Groups" of Transaction Sets (delimited by GS/GE segments). It does this by defining 'assurance' headers and trailers to envelope a targeted transaction set or functional group. The Assurance Header (S3A or S4A) identifies the business purposes of the assurance, algorithms, identifiers and optionally some signature parameters including certificate lookout information. The Assurance Trailer (S3E and S4E) contains the assurance information, specifically the encrypted hash of the X12 data set off by the security segments. Where the key material is identified with a specific person or process, the method provides the basis of an electronic signature. X12.58 and X12.42 collectively support conventional digital signatures using public key cryptography; but they also support signatures based on symmetric keys. Assurance segments can be nesting allowing for the application of multiple signatures.

While X12 provides this mechanism for a signature of the attachment transaction, it probably provides the 'wrong' signature for the current (attachment) purposes. The X12.58 signatures are defined for an EDI *transaction*, the clinical information for which practitioner attestation is sought is only a component of that transaction.. To confound the practitioner's attestation regarding the clinical data with one regarding a X12 transaction information is, to say the least, extremely inefficient and, as practical matter, un-implementable. Were it possible to define assurance segments narrowing enveloping the BIN segment of the X12.275 transaction, the approach might be more useful. Its would seems a simple matter to define the additional Assurance headers and trailers to envelope segments but X12.58 does not currently allow this.

⁶ ITU-T Rec. X.690. <http://asn1.elibel.tm.fr/en/standards/#encoding>

⁷ "Public Key Cryptography Standards #7 – Cryptographic Message Syntax Standard" provides the most familiar and robust mechanism for representing and communicating digital signatures. <http://www.rsasecurity.com/rsalabs/pkcs/pkcs-7/index.html>

Furthermore, the currently listed business purposes of the assurances do not include anything approximating 'practitioner authentication' as the current use of the assurance mechanism seems focused on the communication of transaction authorization. However, X12.58 does support specialized purposes for the assurance such as communication of EPA certification or tax preparer signature. Again it seems a simple matter to define an "Business Purpose of Assurance" code for 'practitioner's authentication' but X12.58 does not currently support this.

Signature and Message Transmission. Traditionally, EDI is transmitted as cleartext to 'mailboxes' across 'secure' channels where source and recipient are authenticated prior to mailbox access. To use 'open' networks for secure EDI transmission required the development of procedures to ensure that EDI messages were authentic, i.e. were sent by the transmitter identified in EDI headers (e.g. the X12 ISA header) and were not tampered with or corrupted during transmission. EDIINT⁸ has been developed within the IETF as a standards based mechanism to provide this assurance. EDIINT conforming messages are digitally signed using the transmitter's public key pair and the PKCS#7 format. The EDI messages, once labeled with appropriate s/MIME header's, can then be securely sent using ordinary Internet mail methods. EDIINT and s/MIME are particularly attractive technologies as they are well supported today with low cost, off the shelf, commercial software.

For much for the same reasons as with the X12.58 methods, neither EDIINT nor s/MIME is appropriate to the HIPAA electronic signature problem. Clearly, the practitioner's signature on the EDI message is inappropriate as the practitioner is typically not the transmitter of the EDI. The practitioner's role is limited to authenticating only some of the information in the X12.275 transaction, i.e. that inserted in the BIN segment. This is especially true when the underlying claim was submitted by an institution for which the practitioner has no direct responsibility or ownership.

In 2001, joint activity of several healthcare and other standards bodies⁹ sought to develop pilots and demonstrations of the use of healthcare electronic signature. This was an ANSI HISB sponsored activity and was intended to provide input to its recommendations to the NCVHS on the HIPAA electronic signature rule. This Joint SDO activity focused on the use of EDIINT from the outset, perhaps to the detriment of the activity. Furthermore, much of the Joint SDO activity is irrelevant to the current topic (of a HIPAA electronic signature standard) because few of its use cases involved the transactions subject to HIPAA regulation that require transmission of a signature.

Conclusions

By far the most practical method to transmit signatures authenticating patient information is to incorporate the signature into the transmitted patient record. Where HL7 is format for the transmitted patient information, then the signature should properly be part of the HL7 message. Unfortunately, HL7 is not yet ready to support this role.

Consequently, patient records requiring signatures are best sent as encapsulated image data in a TIFF format. Whether or not there is a benefit to using the X12.275 attachment transaction for this purpose, as opposed to faxing, remains to be seen. Certainly, the lack of HL7 signature support delays further implementation of electronic signature and will force the provider's continued reliance on paper documentation.

Authentication of Signatures

⁸ "EDI – Internet Integration" <http://www.ietf.org/html.charters/ediint-charter.html>

⁹ <http://hl7.org/special/Committees/multiSDO/index.htm>

The HIPAA Law calls for standard procedures for the authentication of electronic signatures used with the HIPAA transactions. “Authentication of signatures” involves developing some sort of assurance that the document was signed by the purported signer and that the document has not been modified subsequent to signature so as to call into question the signer’s intent. The HIPAA Law, then, asks the regulators to accomplish two tasks: 1) determine the level of assurance required for signatures associated with the HIPAA transactions. 2) specify a signature technology that when implemented in a standard way provides this assurance.

It is important to recognize that ‘authentication’ can be accomplished with more or less certainty. To be cost effective, the HIPAA signature standard should be grounded in risk analysis that associates acceptance of a fraudulent or otherwise inauthentic signature with the economic consequences to the party unwisely accepting that signature. Where healthcare claims attachments are concerned, the economic consequence is presumably limited to the dollar value of the claim supported by that attachment. While these dollar values obviously vary, they would be generally known at the time of signature acceptance, and so can be used to calibrate the level of certainty required in the signature authentication. If the HIPAA standard procedures are to be cost effective, it may be that the HIPAA developed standard procedures do not provide a level of assurance appropriate to some very high valued claims. The legislative mandate for the HIPAA standards is that they are to have the effect of reducing costs but this is unlikely to occur if the least valued claims must be supported by security infrastructure appropriate to the highest valued claims. In developing the standard authentication procedures, the regulators may well have to support some sort of ‘opting out’ for the highest valued transactions.

What is incorrect is the approach taken in the HIPAA Security and Electronic Signature NPRM¹⁰. Here the regulators propose, without justification, that the standard electronic signature mechanism support a property known as ‘non-repudiation’. By intent, systems supporting ‘non-repudiation’ ascribe near certainty to signature authentication as they attempt to effectively preclude the purported signer from disputing the signature’s authenticity. While it is likely that such systems can only be created with legislative and judicial support¹¹ and therefore beyond the scope of mere regulators, it is also likely that such systems will be very expensive to implement. Since such systems seek to limit the dispute resolution opportunities of participating individuals, in order to acquire the participation of those individuals, the signature systems must provide and demonstrate substantial protections of individual interests. What is lacking in the NPRM is any economic foundation that would cost justify the expense of a proposed system of ‘non-reputable’ signatures. Electronic commerce can and does readily occur without such ‘non-repudiation’.

The status of HIPAA’s mandate for standard ‘procedures’ is uncertain following the enactment of the E-SIGN Law in 2000. Preemptive provisions of E-SIGN generally require that state and federal regulation of signature and record retention, among other things, be ‘technology neutral’. It is unclear how HIPAA’s ‘standards specifying *procedures*’ can be technological neutral as procedural language obviously constrains implementation. However, E-SIGN does allow a federal agency to specify the use of specific technology where there is a showing that the

¹⁰ In 1998, HHS Regulators published a “Notice of Proposed Rulemaking” that addressed the security standards mandated by Sec 1173(d) and the Electronic Signature standards mandated by Section 1173(e). Since publication of this NPRM, HHS personnel have advised that the electronic signature rule will be ‘de-coupled’ from the security standards and addressed by a separate rule. The NPRM can be found at:
<http://aspe.os.dhhs.gov/admsimp/bannerps.htm#security>

¹¹ Whether or not a signature mechanism provides “non-repudiation” is clearly dependent upon how signature disputes are resolved. For disputes regarding healthcare claims, disputes are typically resolved either in civil courts or in the administrative hearings of state health insurance regulators. Some states have created, as a matter of law, presumptions of validity for specially constructed digital signatures that borders on ‘non-repudiation’. For example, the Washington State Electronic Authentication Act <http://www.secstate.wa.gov/ea/> Such presumptions, though, do not exist as a matter of preemptive federal law such as E-SIGN

technology mandate is 'substantially' related to an 'important' government objective. The Federal government's interest in 'administrative simplification' of healthcare reimbursement most likely provides the HIPAA regulators the basis for a very specific signature technology mandate.

The component processes required for any sort standard signature authentication procedure seems clear: 1) There must be a *registration* process by which credentials are associated with persons; 2) There must be a *signature creation* process where, following the action of a person, some aspect of a person's credential is bound to a document. 3) There must be a *verification* process that allows confirmation of a correspondence between signature and signer's credential.

Registration of Signer Credentials

The concept of credential is broad and includes any data that is used to corroborate the identity of a signer. Currently, three sorts of credentials are used for electronic signature purposes: PINs (personal identification numbers), biometrics and public key (digital) certificates.

PINs are represented in the currently typical electronic signature practice. Thru a registration process, a unique PIN is issued to a practitioner who attests to its ownership and responsibility for subsequent use. Subsequent to registration, the practitioner enters the PIN when prompted to 'sign' an record entry or document. There is a difficulty in using PIN based systems in that a PIN is a simple secret shared between the signer and the verifier of signature. A signature system based on PINs would necessarily need to disclose the PIN to all verifiers of a signature; in general, this would involve both the institution maintaining the patient record system and the payer(s) requesting the additional patient information. Therefore, while perhaps acceptable within an enterprise, such a system would require a very elaborate security infrastructure to work on an industry scale. In particular, it is most likely that some sort of 3rd party verification would be needed to ensure adequate control over inappropriate disclosure and use of a given practitioners' PIN. While there are some models for this approach¹², inter-mediation, by definition, introduces more 'steps' and added security vulnerability to signature implementations as well as added complexity to associated business agreements. The 3rd Party service would necessarily be responsible for its diligence in identifying practitioners and securely issuing PINs to them.

From a security perspective, a more robust solution is possible with the use of some sort of biometric capture. Although the idea of a 'biometric signature' has not been fully fleshed, such a signature would involve associating a biometric capture with a signing event. For example, the practitioner may be prompted to place a digit on a fingerprint reader to commit or approve and thereby 'sign' a clinical order. The registration process for this kind of signature involves constructing a 'biometric template' from a sample of readings and associating that template with an person. A principal difficulty with using such templates on an industry scale is that there are few standards for template construction. Vendors of biometric readers use different algorithms and measures to construct templates for, nominally, an identical biometric, say fingerprints. Complicating standardization effort is the fact that the vendor specific procedures are the intellectual property that differentiates vendors product¹³. Since any registration of biometric templates must be qualified by the product that used to capture the biometric, it is difficult to understand how 'biometrics' can, in the near term, be the basis for an industry 'standard procedure'.

¹² The "TIE (Trust Infrastructure for Europe)" has persons authenticating to a trusted / disinterested proxy service using conventional PIN / password which creates / records the document signature on behalf of the signer. Document recipients rely upon the proxy's assertions of authenticity. <http://www.tie-project.org/>

¹³ For example, this problem is so severe that interagency-law enforcement agency transfers of fingerprint data is based on distribution of images of fingerprints rather than computer coding of fingerprint minutiae. This is one reason why there is such a backlog on finger print checks.

The most familiar and mature mechanism for a signer credential is a public key (digital) certificate. The issuance of digital certificates to persons has been a subject of considerable study and standardization¹⁴. The particular advantage of a digital certificate is that they can be issued and maintained independently of parties seeking to verify signatures created with them. This allows practitioners to acquire a single certificate which, in principle, could be used to verify any signature created by that practitioner. This sort of scalability is a practical requirement of a HIPAA electronic signature standard. It is frequently the case that, at the time of treatment and medical record creation, all payers may not be known while any of them may seek additional patient information (attachments) prior to payment.

It is a frequent mistake to assume that the industry standard use of digital signatures (i.e. signatures using digital certificates) must await the deployment of a formal industry scale PKI¹⁵. To the large extent, the patient information in attachments is created and authenticated by practitioners with whom the requesting plan has an established business relationship. For such practitioners, it is a simple matter to distribute certificates to healthplan at the time either of credentialing or of negotiating business contacts. The details of where and how the practitioner received the digital certificate are made largely irrelevant by the plan's reliance on the representations made directly to the plan by the practitioner. Plans could readily associate the practitioner's chosen certificate with the practitioner's profile in plan databases for subsequent use in signature verification. This is not to say that economies cannot be obtained thru reliance on 3rd party assertions in a PKI, but merely that such reliance is not essential to industry wide implementation of digital signatures under HIPAA.

Signature Creation

By E-SIGN definition, electronic signatures result from the *intentional* 'act of a person'. However, the electronic signature itself is not a recording of the 'act' but rather a computation or other computer event that is triggered the person's action. There is, then, a significant interest on the part of both practitioner and plan that the signature not be triggered by an unintentional act or other spurious event. Almost certainly, this means that electronic signature has to be 'obtrusive' and the signature act explicit. Signers must know, in fact, that they are about to sign an electronic record.

Although not necessarily so, the explicit signature act is often confounded with the signer authenticating self to the signature system. This is possible since authentication involves presentation of something unique to the party being authenticated. So once choosing to 'sign', practitioners are prompted to enter a secret PIN, place a digit on a biometric capture device, swipe a smart card, present some other security information, or some combination of the preceding. The extent to which such acts do not occur 'coincidentally' is taken as an indication that a signature act did in fact occur. To a degree, the required level of 'obtrusiveness' can be standardized in the 'performance criteria' for suitable signature systems. The DEA, for example, in its promised 'electronic prescription for narcotics' rule, apparently will require that the practitioner both to present a hardware token containing a personal signature key and have a fingerprint or other biometric be captured as part of the signature process. While the DEA 'multi-factor' authentication requirement is not a good example of a "performance standard"¹⁶, it does illustrate how regulators can manipulate a required level of 'intentionality' in the signature action.

¹⁴ The ASTM e31.20 Committee on Data Security has just completed successful balloting of a healthcare specific Certificate Policy. This Certificate Policy provides guidance for issuance of certificates that would be appropriate for healthcare transactions and provides a basis for interoperability of healthcare oriented CA.

¹⁵ "Public Key Infrastructure"

¹⁶ With respect to authentication, performance standards are properly stated in terms of the likelihood of various kinds of authentication errors not in terms of methods that *may* insure compliance.

What constitutes the 'signature action' is ultimately an question of user interface design. Since modern approaches to software design (e.g. the model-view-controller pattern), abstracts the user interface from application logic, it is unlikely that health plan recipients of a transmitted signature can ever know the exact user conditions under which the signature 'act' takes place. The HIPAA regulators can however specify various interface requirements and then mandate 'certification' of the applications that implement the required electronic signature functionality. This is an approach taken by some states in their regulation of medical record signature.

Even when practitioner's signatory intent is clear, the purpose of that signature may be questioned. The ASTM e1762 "Standard Guide for Electronic Authentication of Health Care Information" details 17 distinct purposes for signature on a health record. For example a practitioner typically signs as the author of an operative report and thus to indicate responsibility for the report's accuracy. However, the practitioner may also sign the operative report as a participant in the procedures in order to indicate responsibility for the procedures that the practitioner conducted. Practitioners can also sign as witnesses to procedures or to the signatures of others; they can sign documents to indicate their review and approval of document or to indicate their oversight of the underlying treatment. Industry practice even supports the curious phenomena of an 'administrative signature' where the signer has neither read the document or accepts any responsibility for the events detailed within it.¹⁷ It may be important, then, to clarify signer's purpose beyond just 'signature'. This can be done in a standard way by referencing e1762's signature taxonomy.

Electronic signatures have the net effect of 'binding' the signer's credential to the signed document. The significant issues here have to do with whether such binding is persistent or transient and with the 'strength' of that binding.

The binding is 'persistent' when the representation of the electronic signature, once created, is not dependent upon the application creating the signature. A singular advantage of persistent signatures is that they allow implementing organizations flexibility to modify and replace the applications which implement the signature method. Digital signatures are examples of persistent signatures. Transient signatures, on the other hand, must be maintained by the system that created them. For example, if the 'fact' of signature is represented as a database entry, say containing the name of signer as well as date and time of signature, signature availability depends on the maintenance of the database application constructing the signature. A corruption, loss of database tables, or security breach effectively destroys or diminishes the assurance provided by the signature.

Regardless of persistence, signature bindings can be, in a security sense, strong or weak. Signatures only weakly binding credentials to the authenticated record are at least somewhat insensitive to modification of that record, i.e. the some change in the record can be made without affecting the signature. Although most would say that this is generally not desirable, some record changes may not impact the semantics of the record and therefore probably should not impact signature validity. Signatures that are strongly bound to the record are invalidated with slight modifications of the record. Digital signatures, for example, are invalidated by even the slightest change in record syntax or coding.

Signature binding is generally provided by one of two mechanisms. Today's clinical systems rely upon a collection of 'audit trails' and 'record locking' procedures to secure signature bindings. The idea is that a series of checks on data integrity will detect modification of a record subsequent to signature. Such mechanisms are generally inefficient in that the audit trails and other logs that are used to provide assurance of record integrity must themselves be secured. The assurances providing by this sort of signature binding then is vulnerable to an indefinite regress of challenges. These mechanisms are inexpensive to implement but generally expensive

¹⁷ Such signatures are apparently used to satisfy regulatory or accreditation demands for 'signature' that cannot otherwise be satisfied, say where an report's author is not available. .

to maintain as they require active management. Security bindings based on audit trails should be considered weak. The assurance provided by such systems erode catastrophically as *any* failure of the management controls is effectively a failure of the signature *system* which calls into question the assurance of *any* given signature created within it

A second mechanism for signature binding involves the use of cryptographic methods, in particular, where a secure hash of the signed record is encrypted by the signature system. The encrypted hash provides the signature binding. If the document is changed, the hash value will change; encryption prevents modification of the binding by other than the holders of the encryption keys. Where the encryption keys are private signature keys in a public key system, the signature binding is known as a digital signature. Digital signature binding is efficient in that, once constructed, the binding requires no active management. As a practical matter, the assurance provided by digital signatures erodes only gradually as increased computer resources allow for more effective key space searches. Furthermore, cryptographic bindings are robust in that a failure with respect to control over individual signature keys impact only signatures involving those keys. In public key systems, this means that compromise of one person's signature does not negatively impact the assurances provided by other persons' signatures.

Signature Verification

Obviously, signatures can only provide assurance if their authenticity is verifiable. Furthermore, for signatures of health claim attachments, that authenticity need be verifiable by means that are independent of the applications or implementations creating the signature. There are a couple of reasons for this. First, the practitioner's signature is relevant primarily because the attachment provides the health plan with the *practitioner's* statements regarding conditions of care. Plans rely upon such statements particularly in cases where they are concerned about the integrity of institutional controls over admissions, treatment and billing. Where there are such suspicions, it would be illogical for the health plan to rely heavily upon the institution's controls over the creation and *maintenance* of the practitioner's electronic signature. In principle, the institution that can bill improperly, if permitted, could improperly record, maintain and transmit practitioner signatures. Second, the providers (and their vendors) need for implementation *flexibility* conflicts with the health plan need for implementation *simplification*. If any signature verification required an ongoing interface with the application creating the signature, then plans, with their large provider networks, would rapidly find verification of electronic signature intractable. The cost of maintaining communication protocols with the variety of signature implementations would be cost prohibitive. Although it may be the case that context might dictate whether an electronic signature needed to be verified and therefore not all electronic signatures needed to be verified, in principle, electronic signatures are only useful if *any* signature can be verified.

The recognizable signature technology currently providing for such independent verifiability is digital signatures using public key technology. Once plans have acquired the certificates of practitioners, signature verification is a simple and entirely technical matter. Plans only bear the risk that practitioner's may have failed to adequately control use of their signature keys. This risk can be mitigated by the use of signature applications certified to conform to appropriate standards, private key implementations certified to provide appropriate key protections, and procedures by which practitioner may notify plans of potential key compromise¹⁸.

Conclusions

¹⁸ The timeliness of such 'certificate status information' is not critical. Health claim attachments are processed as part of a claim adjudication workflow as opposed to an automated real time process. The latencies intrinsic in the processes associated with the decision to request the patient information, the provider's review and fulfillment of the request, the plan's receipt and processing the attachment ensure substantial time for the posting of changes in certificate status.

The HIPAA electronic signature standard procedures should incorporate use of digital signatures. Digital signatures are supported by a high degree of standardization from a variety of sources including the X9, IETF, W3C, ASTM and a host of other bodies. Development of digital signature capability is well supported by commercial toolkits and so the capability can readily be included in clinical applications. The benefits of industry standard digital signature procedures does not have to involve infrastructure development on an industry scale as signature verifiers can obtain certificates directly from practitioners at the time of credentialing or contract negotiation.

For the standard procedures to be effective, the HIPAA regulators should specify (human) interface standards for applications invoking signatures keys and develop accompanying certification requirements. The regulators should also select among potential digital signature formats (e.g. PKCS #7, xml-dsig) and identify requirements to support various signature attributes (e.g. 'signature purpose').