URPERA Security and eRecording Metadata
By John Messing, (Attorney at law and Member, Science and Technology Council, American Bar Association)

I spoke as a panel member during the PRIA Annual Conference in Charlotte, NC, in July 2007 about URPERA Section 5(b)(5) security requirements. I have since become aware that despite the very best intentions, my comments may have sown some confusion. The statement which follows was prepared by myself with the help of others to clarify a view of the relationship between URPERA security requirements in Section 5(b)(5) and eRecording metadata retention policies. I can be reached at jmessing@law-on-line.com with questions or comments.

Beginning with modern imaging technologies of microfilm and computers, constructive notice of a recorded document has been provided by a recorder's office through making available an image of the submitted document itself onto which was imprinted the date and time of recording. In the pre-microfilm and computer age, recorders manually transcribed or abstracted the contents of the submitted document into the paper copy records of the recorder's office. The modern imaging technology convention seems based upon the commonsense supposition that notice of something is best given by presenting the thing itself, and not just someone's description about it.

In eRecording, a recorded document is composed of computer codes that when presented with the proper software produce a human-readable view of the submitted document. In addition, the recorded document has recording information imprinted on it (or logically associated with it) and it is maintained in an archivable medium and format. Technology people tend to call this human readable view "document content." Submitted documents are often accompanied by metadata, which is other information that describes a submitted document’s content, such as the identity of provider companies and the times and identity of the computer servers a document passed through on its way to the recorder's office. Retaining this metadata information in the recorder’s official records after the recording function has been completed seems unnecessary and burdensome, with one very narrow and limited exception.

URPERA Section 5(b)(5) imposes security requirements that in turn may be met by a limited class of security metadata. An example of such metadata that is generated for URPERA security purposes is an encrypted hash of the submitted document (we’ll call this SubmittedEncryptedHash) that, through technology, can determine whether the submitted document content was changed after an event or process, such as the time when the document was created and signed, and/or recorded, and it may also reveal the identity of a signer. It is my opinion that the SubmittedEncryptedHash is a type of metadata that can fulfill the security requirements and purposes of URPERA Section 5(b)(5). Thus, under this view, a SubmittedEncryptedHash should always be captured and retained by the recorders’ office as metadata preserved pursuant to URPERA Section 5(b)(5).

In the event that a document is converted (e.g., to a TIFF image) during the recording process, a second encrypted hash (we’ll call this RecordedEncryptedHash) can also be generated and stored with the first. The RecordedEncryptedHash could cover the composite of the converted document and the recording information. Together with the document content, the two...
encrypted hashes (SubmittedEncryptedHash and RecordedEncryptedHash) enable an easily verifiable method to determine whether the converted document content differs in any material way from the original, in a way that renders it as a practical, commercial, and legal matter indistinguishable from the submitted version. Additionally, the second encrypted hash would have the salutary effect of revealing alteration to the recorded document after it was initially converted, since the RecordedEncryptedHash would be available beginning immediately after the recorded document was created. With a way of both proving a document was authentic and unchanged since it was submitted for recording and actually recorded, the security purposes of URPERA Section 5(b)(5) can be easily achieved.

The encrypted hashes are relatively short strings of computerized characters that require a relatively insignificant amount of additional storage space in the recorders’ back office systems. Thus, I do not believe that retaining the encrypted hashes would be burdensome or expensive for the recorders’ offices.

Except for the purposes of establishing the security and authenticity of the recorded documents by means of such metadata, URPERA Section 5(b)(5) otherwise seems to be irrelevant to the preservation or destruction of metadata relating to an eRecording.
For purposes of this document, “submitted document” means that document which has been submitted to the recorder’s office for recording, and “recorded document” means that document as it appears in the official records maintained by the recorder.

Traditionally, information in paper form utilizes a document as its container. In electronic form, information may be broken down and stored piecemeal in databases, or alternatively, other media formats that do not lend themselves well to the concept or definition of a paper document.

As the methods and types of electronic transmission and storage evolve, new types of information containers may arise. Hence, a flexible definition that includes all information that can be stored electronically, regardless of method of transmission, storage, retrieval, display and verification, becomes necessary.

The term "logically associated" recognizes that the term document may be unduly restrictive when applied to electronic data, although certain lawyers who deal in paper are primarily familiar with that format and may have difficulty with this newer concept. In fact, the 2006 federal amendments to eDiscovery rules recognize this very distinction. Instead of the traditional term "documents," the new term for discoverable information in the federal courts includes "electronically stored information" (ESI).