



Compliance and Email

Compliance and email are difficult enough issues to address individually. Where they overlap, the complexity increases by an order of magnitude.

- *Brian Foster, Director of Legal Business Consulting at Access Sciences*

Autoclassification

Q: How does autoclassification work?

A: Autoclassification products scan messages to determine classification. They may simply compare the subject line to a chosen set of keywords, or conduct a more complex review of the message content. Autoclassification products can be configured to read and classify records, or to recommend a classification for the user to accept or correct. Autoclassification tools are only as successful as the policies established for their use. It is crucial to perform extensive testing and auditing to verify that both the software and configuration are functioning properly.

Q: Would autoclassification make inaccessible data accessible?

A: Because the autoclassification process aims to assist the user in classification, it should not have an impact on arguments supporting the accessibility of ESI. The content that has been classified into an ECRM system is accessible by definition.

Email Management

Q: Is it possible to separate business emails from personal emails? How can organizations determine and apply the correct retention period for each email? Some companies are automatically deleting emails after 90 to 120 days. Is this advisable?

A: Email management must be part of an overarching enterprise content and records management (ECRM) program that establishes how information is managed in the organization, regardless of media.

An email in itself is not part of a record series any more than a piece of paper is part of a record series. It is the content of the email that determines whether the email is a record, business information, ephemeral information, or information that is non-business related.

If a scanned image of a signed contract is sent to a company representative via email, that contract is a corporate record and should be placed in a designated location. An organization that automatically deletes email messages without regard to the content and without a system in place to store records is certainly increasing its risk. Deletion of



information based on format (e.g., email sweeping) is comparable to setting forth a policy that states, “Shred all paper documents after 90- to 120-days.”

Software products are available that have the capability to scan the content of a mailbox and select email messages meeting defined search criteria. These emails are moved into a holding area for classification. The user is allowed a set period of time to conduct a final review and declare records before the messages are deleted. Assessment of the costs, benefits, and of the level of risk should provide the framework for decisions related to the ECRM solution. Any systems created to support email management should be aligned with the corporate ECRM strategy.

FRCP

Q: Do regulations governing e-discovery vary between private and publicly traded companies?

A: Discovery rules pertain to any individual or organization involved in civil litigation. Other than the vast amount of information resources belonging to large corporations, there is no variance in the discovery responsibilities of companies, regardless of size. Additionally, the FRCP (Federal Rules of Civil Procedure) only applies to cases filed in Federal Court. Each state has specific rules that must be followed (see <http://www.ncsconline.org/> for more information).

Q: Does e-discovery include text messages delivered to PDAs and cell phones?

A: E-discovery spans any place that ESI (electronically stored information) could exist. This includes but is not limited to PDAs, smartphones, instant messages, text messages, voice mail messages, home computers, digital cameras, phone logs, VoIP calls, Web browser cache files, vehicle data capture devices or black boxes, YouTube, Facebook, blogs, and—as seen in recent case law—system RAM.

Legal holds apply to any potential evidence that may be relevant to the matter in contest. All documents (electronic and paper), database records, reports, email messages, etc.—regardless of whether the items are declared as records or are merely information of temporary value—are subject to legal holds.

Q: If more than one copy of an email exists, is it necessary or advisable to preserve all copies?

A: If an individual has two identical, exactly identical, copies of an email, they are not required to store both copies. If a user has printed an email and made hand-written notes on it, that document is unique and must be retained as a record. If a user has forwarded an email, that email must be kept as well as the forwarded copy. However, if a corporation has the same email stored by two different users, both copies must be preserved. If during normal course of business a user stores a copy of an email using email archiving software, only one copy of the message will be stored. In this case, the sender and each recipient will be able to access the single copy by selecting a link provided by the software.



--Brian Foster is the director of Legal Business Consulting at Access Sciences (www.accesssciences.com) and has over twenty years experience in IT, project management, and litigation support. Prior to joining Access Sciences he was the director of e-discovery for a Fortune 25 Energy Company where he managed e-discovery events and led improvement projects.

***Reprinted with Permission from AIIM Infonomics
May/June 2008***