Electronic Business Records:

Compliance Rules for Financial Institutions

By

Nancy Flynn, Founder & Executive Director, The ePolicy Institute

Author*, The Social Media Handbook, The ePolicy Toolkit, The e-Policy Handbook*

The face of business communication is changing. It is anticipated that by the end of 2014, social networking will replace email as the number-one form of business communication for 20 percent of users.[1] In fact, among Fortune 100 companies in the United States, we've already seen rapid adoption of social media as a primary vehicle for business communication. As of 2010, 72 percent of Fortune 100 companies were using Twitter; 69 percent reported using Facebook; 59 percent had uploaded business-related videos to YouTube; and 34 percent were operating corporate blogs.[2]

Social media content, just like "good-old-fashioned" email messages and attachments, can create electronic business records that can place your financial institution in jeopardy of government and industry regulatory investigations or federal and state lawsuits. From defamation lawsuits and sexual harassment claims to the risks associated with mismanaged and misplaced business records, your organization faces a host of potentially costly and protracted risks triggered by the content that is posted and published on the social web by employees.

For regulated financial institutions that are governed by the Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Sarbanes Oxley Act (SOX), the Financial Industry Regulatory Authority (FINRA), or the Securities and Exchange Commission (SEC) among hundreds of other rules and regulators, the potential for risk is magnified. Any employee-generated content—whether written and posted at the office during work hours or at home after hours—has the potential to create an electronic business record that must be preserved, protected, and produced in the event of a subpoena.

To help minimize risks and maximize compliance with legal and regulatory rules, financial institutions are advised to adopt the "Three Es" of electronic risk management: (1) *Establish* effective policies; (2) *Educate* the workforce; and (3) *Enforce* policies through a combination of disciplinary action and best-in-class technology designed to monitor and manage content, use, and records in a legally compliant fashion.

Electronic Business Records: Best Practices Call for the Establishment of Record Retention Policies

In order to establish effective record retention policies, financial institutions must first determine what constitutes a business record, on either a company-wide or a department-by-department basis. While there is no one-size-fits-all definition of "business record," electronic business records typically record business-related events, activities, transactions, or discussions. Bear in mind that a personal conversation also may rise to the level of a business record if it takes place over the company network and is retained and archived alongside business-related content.

Electronic business records are generated by employees' online content, including but not limited to email messages, social media posts, blog comments, text messages, and web surfing. Any recorded online conversation has the potential to rise to the level of a business record. When it comes to business records, it is the content that counts. It doesn't matter whether you use a desktop, laptop, tablet PC, or smartphone to communicate. All of those technology tools can create business records that must be retained based on their ongoing legal, regulatory, or historic value to the company.

Once the definition of a business record has been established, the next step is to put together a document retention policy. An effective record retention policy should address all types of electronic content, from email and IM to text messages and tweets to blog posts and YouTube videos.

While an effective document retention policy and storage solution can effectively save a business from thousands–even millions—of dollars in potential lawsuits, many organizations are challenged when it comes to records management. According to American Management Association/ePolicy Institute research, 51 percent of companies lack an email retention policy. Thirty-four percent of records managers cannot distinguish business critical email from insignificant and personal messages. And another 33 percent of records professionals do not feeling confident about their organizations' ability to manage electronic business records in a compliant fashion.[3]

Failure to manage electronic business records can be costly. It's not uncommon for courts to sanction companies millions of dollars for their failure to turn over email in response to e-discovery requests. In a high-profile lawsuit several years ago, Morgan Stanley was slapped with a $1.6 billion judgment,[4] in part because of the company's failure to effectively preserve, protect, and produce email records.

Federal Rules of Civil Procedure Are at the Heart of Record Retention

There is no doubt that the evidentiary role of workplace email and other electronically stored information will continue to expand. The U.S. federal court made clear this fact in 2006, when the amended Federal Rules of Civil Procedure (FRCP) were announced, confirming the fact that all electronically stored information (ESI) is discoverable. That means that all ESI, including email messages and attachments, tweets and blog posts, text messages and instant messages is discoverable and may be used as evidence –either for or against your financial institution—in federal litigation. To be accepted as evidence, however, email and other forms of ESI must be preserved, protected, and produced in a trustworthy, tamperproof, and legally compliant manner.

Effective records management currently is trending toward permanent document preservation, rather than "destructive retention," where documents are destroyed according to an established schedule. That said, it is lawful to purge your system of electronic records in the ordinary course of business, as long as those records are not needed in connection with current, pending, or anticipated litigation.

Under Rule 26 of the FRCP, you are obligated to locate and be prepared to discuss all ESI related to a case, within 99 days of the time that a federal lawsuit is filed. Failure to comply with the "99-day rule" can result in significant financial penalties. In 2010, the court sanctioned Qualcomm $8.5 million for a "massive discovery failure."[5] The previous year, Onex Corp was ordered to pay over $1 million for what the court deemed to be a "textbook case" of discovery abuse.[6]

In addition to federal e-discovery rules, every state has its own rules of civil procedure and e-discovery. As a best practice, be sure to have your organization's legal counsel research and comply with the e-discovery rules of every state in which you do business or litigate lawsuits.

Don't Confuse Backup with Archiving

It is important to note that "backup" of email is not the same as "storage." If your financial institution relies solely on backup systems for record retention, then you are putting your email records—and your legal position—at risk. A backup system is no substitute for archiving, or storage, technology. Designed solely for the recovery of data in the event of a disaster, backup is nothing more than the mass gathering of ESI in a known location. Only with an effective storage solution will your business be able to ensure the preservation and production of legally compliant email in adherence with the requirements of the courts and regulatory bodies.

A few best practices for establishing an effective records management policy include:

- Review the retention guidelines and e-discovery rules of the federal court system, relevant state court systems, the FDIC, NCUA, SEC, IRS, and any other government or industry regulatory agencies that oversee your business.
- Establish a written retention policy.
- Educate users about the company's retention policy and their respective roles, if any, in the retention and disposition of email and other ESI.
- Establish lifecycles for every type of record created or transmitted by the business. Clearly spell out how long records must be retained, and when and how records may be purged.
- Assign your lawyer or compliance officer the task of establishing a litigation hold policy to ensure that relevant records are retained and purging stops once a lawsuit is filed (or if you sense litigation is headed your way).
- Support your organization's record retention policy and compliance program with secure archiving technology.

Educating the Workforce

After establishing your organization's formal retention policy, the next step is to educate the workforce. Make training mandatory for everyone, from the summer intern to the CEO. Training should also include independent contractors, freelancers, consultants, and anyone else who works on behalf of the company and could put it at risk of litigation.

A good way to gain employee buy-in is to conduct live training. If this is not possible, consider conducting a webinar or another interactive training forum. Conclude training with a test to ensure that your users fully understand the organization's electronic risks and rules, policies and procedures. Repeat training annually.

At the conclusion of training, require employees to sign an acknowledgment form, attesting that they have read the policy and will adhere to it, or they will accept the consequences, up to and including their termination. Retain copies of all policy-related training materials to demonstrate your commitment to compliance in the event of a lawsuit.

Enforcing the Rules

Take advantage of laws and technology tools designed to help enforce electronic rules and policies. The Electronic Communications Privacy Act (ECPA) is the federal law that gives U.S. employers the legal right to monitor all computer transmissions, activity, and records inside the organization's system. Along with giving employers the legal right to monitor email and other computer activity, the ECPA makes clear the fact that employees have no reasonable expectation of privacy when using the company's computer system.

While best practices and the law support monitoring, not all organizations take advantage of their legal right to monitor employees' online activity. As of 2007, only 66 percent of organizations were monitoring their Internet systems, with only 10 percent monitoring social media and another 12 percent monitoring the blogosphere. Further, only 43 percent of organizations were monitoring email, and of that group, 96 percent reported that they strictly monitored external email (incoming and outgoing messages), with only 58 percent monitoring internal email messages transmitted among employees, according to the *2007 Electronic Monitoring & Surveillance Survey* from American Management Association and The ePolicy Institute.[7]

Protect Your Records and Your Business

Thanks to social media, the potential for costly and protracted electronic risks is greater than ever. To help minimize risks and maximize compliance, best practices call for the establishment of clear and consistent policies, supported by employee education, and enforced by best-in-class technology tools.

As part of your comprehensive e-policy program, establish a formal records retention policy. Enforce your policy through a combination of disciplinary action and technology.

Best Practices for Effective Records Management:

1) **Conduct a risk and policy compliance audit.** Completed once a year, this survey includes a review of all the federal and state laws and industry and government regulations impacting the privacy, security, and e-discovery risks and obligations of your financial institution.
2) **Review potential data security risks.** As part of your annual audit, be sure to analyze how the company currently is using technology. For example, is the business providing employees with smartphones? If so, you'll want to establish policy governing mobile device use, content, and records.
3) **Review all acceptable use policies (AUPs).** Your annual audit is a good time to review all of the organization's AUPs including email policy, record retention policy, litigation hold policy, and records lifecycle and deletion schedules. Use this opportunity to update old policies and create rules for new and emerging tools.
4) **Have the IT director or chief information officer assess your technology solution on a yearly basis.** Use the annual audit process to determine risks. Then, investigate whether or not you have the right technology solutions in place to effectively keep information secure. Use this yearly opportunity to update or replace old technology solutions.

ABOUT THE AUTHOR

Nancy Flynn is founder & executive director of The ePolicy Institute™. An internationally recognized expert on workplace email, social media, and Internet policy, compliance, and communications, she helps employers limit electronic risks, including litigation and regulatory investigations, through the development and implementation of policy, training, and compliance management programs. The ePolicy Institute has nearly 10,000 worldwide members who turn to Nancy Flynn for help implementing strategic, best practices-based policies governing email, social media, and Internet use, content, and compliance.

Nancy Flynn is the author of 13 books including *The Social Media Handbook; The ePolicy Toolkit; The e-Policy Handbook; E-Mail Rules*; *Blog Rules*; *Instant Messaging Rules*; *E-Mail Management;* and *Writing Effective E-Mail*. Her books are published in six languages: English, German, Spanish, Russian, Vietnamese, and Chinese.

An in-demand speaker and seminar leader, Nancy Flynn provides onsite and online training to corporations, associations, and government entities worldwide. Nancy Flynn serves as an expert witness for the federal government and law firms engaged in Internet-related litigation. Since 2001, Nancy Flynn's ePolicy Institute and American Management Association have cosponsored surveys of electronic policies & procedures, monitoring & surveillance.

Nancy Flynn is a go-to media source. Among the media outlets that have featured the ePolicy Institute are *Fortune*, *Time*, *Newsweek*, *BusinessWeek*, *Forbes*, *Wall Street Journal*, *US News & World Report*, *Readers' Digest, Financial Times*, *USA Today*, *Entrepreneur*, *InformationWeek*, *Kiplinger's*, *Federal Lawyer*, *New York Times*, *Los Angeles Times*, *Chicago Tribune*, *Washington Post*, *Irish Examiner*, NPR, BBC, ABC World News with Diane Sawyer, NBC, CBS Early Show, CNBC, CNN Headline News, CNN Anderson Cooper 360, Fox & Friends, and Fox Business News among others.

Nancy@ePolicyInstitute.com 614-451-3200 www.epolicyinstitute.com

[1] T. Henneman, "Companies Making Friends with Social Media," Oct. 2010. http://www.workforce.com/section/software-technology/feature/companies-making-friends.
[2] "DataBank: Social Gauge," SC Magazine, Nov. 2010, p. 6.
[3] American Management Association and The ePolicy Institute, "2009 Electronic Business Communication Policies and Procedures Survey," July 2009. http://www.epolicyinstitute.com.
[4] Kim S. Nash, "E-Mail Retention: The High Cost of Digging Up Data," *Baseline*, August 2, 2006.
[5] *Qualcomm Inc. v. Broadcom Corp*., No. 05cv1958-B (BLM) (S.D. Cal. Apr. 2 2010).
[6] *Kipperman v. Onex Corp*., 411 BR 805, (Dist. Court, ND Georgia, May 2009).
[7] American Management Association and The ePolicy Institute, "2007 Electronic Monitoring & Surveillance Survey," June 2007. http://www.epolicyinstitute.com