ARCMAIL

www.arcmail.com | 888-790-9252

EMAIL COMPLIANCE RULES FOR GOVERNMENT AND EDUCATION:

E-Discovery, Records Retention, and Email Management Policies & Best Practices

Authored by Nancy Flynn
Founder & Executive Director, The ePolicy Institute
Author, *Handbook of Social Media (2011), The e-Policy Handbook, Email Rules, Instant Messaging Rules, Blog Rules, Writing Effective Email, and Email Management*

OVERVIEW

ArcMail Technology, www.arcmail.com, and The ePolicy Institute™, www.epolicyinstitute.com, have created **Email Compliance Rules for Government and Education:** *E-Discovery, Records Retention, and Email Management Policies & Best Practices* as a best practices guide for public sector decision-makers—including CIOs, legal/compliance officers, records managers, school administrators, and agency directors—who play a role in email management, e-discovery, email retention, and email compliance.

Through the implementation of a strategic email management program that incorporates the "3-Es" of email compliance management—establishment of email policy and email retention policy; education of employees; and enforcement via proven-effective email archiving—government entities and educational institutions can successfully manage legal, security, and regulatory compliance risks.

Email Compliance Rules for Government and Education: *E-Discovery, Records Retention, and Email Management Policies & Best Practices* is produced as a general best-practices guide with the understanding that neither the author, ePolicy Institute Founder & Executive Director Nancy Flynn, nor the publisher, ArcMail Technology, is engaged in rendering advice on legal, regulatory, records management, security, or other issues. Before acting on any practice, policy, or procedure addressed in this whitepaper, you should consult with legal counsel or other professionals competent to review the relevant issue.

TABLE OF CONTENTS

LEGAL RISKS AND RULES:
EMAIL CREATES DISCOVERABLE EVIDENCE

Email creates the electronic equivalent of DNA, which may be subpoenaed and used as evidence for (or against) local municipalities, state agencies, publicly funded educational institutions, and other public entities in the event of litigation. During the e-discovery (evidence-gathering) phase of litigation, the court orders each party to produce all documents relevant to the case, including email. The ability to quickly locate and promptly produce legally valid email messages, attachments, and other electronic stored information (ESI) is essential. Fail to meet your electronic discovery obligations, and your public entity could suffer costly court sanctions—paid for with taxpayer dollars that might be needed (or better spent) elsewhere.

SELF-ASSESSMENT:
WHERE DO YOU STAND WHEN IT COMES TO EMAIL MANAGEMENT, E-DISCOVERY, EMAIL RETENTION, AND EMAIL COMPLIANCE?

1. Do you have in place an email policy that is clear, comprehensive, and current? In other words, has your email policy been reviewed and updated within the past 12 months?

____Yes ____No ____Don't Know

2. Have you created an email retention policy to govern the retention and disposition of electronic business records and help ensure legal and regulatory compliance?

____Yes ____No ____Don't Know

3. Have you provided all users (employees, executives, faculty, students, and others) with a formal definition of "business record"?

____Yes ____No ____Don't Know

4. Do your users know the difference between business-critical email that must be retained and archived for legal and regulatory compliance vs. personal and otherwise insignificant messages that may be deleted in the ordinary course of business?

____Yes ____No ____Don't Know

5. Do you support email retention policy with email archiving?

____Yes ____No ____Don't Know

6. Does your email policy incorporate clear rules governing written content and personal use?

____Yes ____No ____Don't Know

7. Is your organization's email archive a potentially dangerous mix of rules-based professional correspondence and off-the-cuff personal conversations that could potentially embarrass your users and sabotage your legal position?

____Yes ____No ____Don't Know

SELF-ASSESSMENT: continued

8. Could you quickly search, locate, and produce legally compliant email messages and attachments in response to a subpoena or public records request?

____Yes ____No ____Don't Know

9. Do you know, understand, and adhere to the amended Federal Rules of Civil Procedure, as well as the e-discovery laws of all the states in which you operate or litigate lawsuits?

____Yes ____No ____Don't Know

10. Is legal and regulatory compliance a priority for your public entity? In other words, have you established a strategic email compliance program that combines email policy and email retention policy with employee education supported by email archiving?

____Yes ____No ____Don't Know

BEST PRACTICE RECOMMENDATION: If you answered ***no*** to any of the 10 self-assessment questions, then you must get to work—***immediately***—on the development and implementation of a strategic email management program for your local municipality, state agency, school district, college/university, or other public entity. The ability to formally define, effectively retain, successfully archive, and promptly produce email and other forms of ESI is one of the most important jobs a public entity can undertake.

You cannot afford to leave email compliance management to chance. If your organization becomes embroiled in litigation or a regulatory investigation, the production of subpoenaed email and other electronic business records is mandatory, not an option. Nearly a quarter of U.S. employers (24%) had employee email subpoenaed by courts or regulatory bodies in 2009, according to the *Electronic Business Communication Policies & Procedures Survey* from American Management Association and The ePolicy Institute. Take a proactive approach to email compliance management. Follow the lead of 51% of organizations that have implemented email retention policies, according to American Management Association/ePolicy Institute research. Combine email policy and email retention policy with employee education, supported by email archiving to maximize compliance with the ever-increasing e-discovery guidelines set forth by federal and state courts and government and industry regulators.

FEDERAL RULES OF CIVIL PROCEDURE

At the heart of e-discovery are the Amended Federal Rules of Civil Procedure (FRCP). The United States Federal Court System raised the bar on email compliance management in 2006, when long-anticipated amendments to the Federal Rules of Civil Procedure were announced. The FRCP make clear the following:

1. Electronically stored information—including email messages, attachments, and other data—is discoverable and may be used as evidence—*for or against any organization (including government entities and publicly funded educational institutions)*—in litigation.
2. Business record email and other ESI that is related to current, pending, or potential litigation must be retained, archived, and produced in a timely and legally compliant fashion during e-discovery, the evidence-gathering phase of litigation.
3. Employers are allowed to routinely purge electronic archives of data that is not relevant to ongoing litigation or pending cases.
4. Writing over backup tape once litigation is underway may constitute *virtual shredding* and lead to allegations of spoliation, or the illegal destruction of electronic evidence.
5. Not all email is equal in the eyes of the law. To be accepted as legal evidence, email must be preserved and produced in a trustworthy, authentic, and tamperproof manner. Unfortunately, email can easily be changed—and rendered legally invalid—just by clicking *edit and change*. Even all-important business records can be forged when sent or received via email. Unless properly managed and securely archived, email opens your organization to a variety of claims ranging from *"I never received your message"* to *"That's not what the attachment said."* Organizations that are eager to protect email business records are advised to turn to archiving technology to ensure forensic compliance. For example, by instantly encrypting and archiving a copy of every internal and external email sent or received across your organization, ArcMail's Defender solution guarantees that your email is secure and tamperproof. Nothing in your archive can be deleted or altered. Everything in your archive is authentic and legally compliant.
6. FRCP's 99-Day Rule requires all parties to a lawsuit to meet and discuss the scope and accessibility of email and other ESI within 99 days of a claim's initiation. Compliance requires you to implement email retention policy and email archiving technology today—or face potentially costly federal court sanctions tomorrow.

BEST PRACTICE RECOMMENDATION: Unmanaged email can trigger financial, productivity, and legal nightmares should your government entity, school system, or university become embroiled in federal litigation. Workplace lawsuits, including harassment, discrimination, and hostile work environment claims, often are filed in federal court. Consider the potential cost and time required to produce subpoenaed email, retain legal counsel, secure expert witnesses, mount a legal battle, and cover jury awards and settlements. Best practices call for a proactive approach to email management. Coupling email retention policy with a proven-effective email archiving solution like ArcMail Defender helps ensure your ability to manage vast stores of email and successfully comply with FRCP's electronic discovery guidelines.

STATE RULES OF CIVIL PROCEDURE & STATE E-DISCOVERY RULES

In addition to complying with federal subpoenas and FRCP's e-discovery rules, government and educational entities also must adhere to e-discovery guidelines on the state level. State Rules of Civil Procedure and State E-Discovery Rules continue to evolve. Some states mirror the Federal Rules of Civil Procedure. Other states have yet to adopt rules based on FRCP. In general, however, state IT departments must comply with e-discovery requests within 30 days, according to the State of Alabama's Information Services Division.[1]

BEST PRACTICE RECOMMENDATION: Have your legal counsel or compliance officer research and monitor how each state in which you operate or litigate claims handles e-discovery, electronic evidence, and record retention requirements. Then, make sure you adhere completely and consistently to State Rules of Civil Procedure and State E-Discovery Guidelines. To help ensure legal compliance in the public sector, ArcMail Technology and The ePolicy Institute have created **ArcMail Compliance Management**, an up-to-date resource that provides information about and links to State Rules of Civil Procedure and E-Discovery Rules for all 50 states.

STATE SUNSHINE LAWS:
COMPLIANCE WITH PUBLIC RECORDS REQUESTS

Government agencies and municipalities, school systems and universities—all public entities are under pressure to maintain the transparency and availability of email and other electronic information. State Sunshine Laws (also known as Open Records or Open Meeting Laws), obligate public entities on the state, county, and local levels to preserve and protect email and other ESI, while ensuring that electronic evidence can be produced promptly in response to a public records request.

REAL-LIFE OPEN RECORDS DISASTER STORY. Government agencies, school systems, and other public entities are obligated to respond to records requests in a timely fashion. In 2010, an Ohio Appeals Court found the city of Cleveland to be in violation of Open Records Law when the city took more than a "reasonable period of time" to satisfy a public records request from the Municipal Construction Equipment Operators' Labor Council. The city's delayed response, coupled with its failure to communicate with the Union about the status of the request, led the 8th District Court of Appeals to award attorney's fees of $5,763.75 to the Union.[2]

When it comes to public entities, every private citizen has subpoena power. Do not allow unmanaged email to undermine legal compliance. Prepare today for tomorrow's records requests by reviewing and (as necessary) updating email policy and email retention policy. Support written policy with an email archiving solution like ArcMail Defender to guarantee your ability to search, locate, and produce email and other electronic records in compliance with State Sunshine Laws.

REGULATORS GROW INCREASINGLY WATCHFUL

Over the years, government and industry regulators have turned an increasingly watchful eye to the content created and business records generated by email messages and attachments. Don't take chances with regulatory compliance and email management. Consult with legal counsel to ensure that your publicly funded organization is in compliance with regulators' email-related rules and guidelines. The regulatory compliance risks and rules with which government entities and educational institutions must concern themselves include:

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA):

If your organization provides health care products, services, or insurance to taxpayers, employees, students, faculty, or other parties, then you are legally required by HIPAA to protect the privacy of patient information. HIPAA requires the safeguarding of email messages and attachments that contain electronic protected health information (EPHI) related to a patient's health status, medical care, treatment plans, and payment issues. Failure to do so can result in regulatory fines, civil litigation, criminal charges, and jail time. Be sure to combine email policy and email retention policy with employee training, supported by email archiving to help keep HIPAA email compliant.

GRAMM-LEACH-BLILEY ACT (GLBA):

GLBA is to the financial industry what HIPAA is to health care. If your government entity or agency, school system or university handles social security numbers, credit card data, debit card numbers, and other personal financial data belonging to consumers, employees, students, faculty, and others, then you must take steps to ensure regulatory compliance. GLBA requires the safeguarding of email messages and attachments that contain personal financial information. To that end, employee education is essential to regulatory compliance. You cannot expect untrained employees to be familiar with regulatory rules, appreciate the importance of email compliance, or understand their individual roles in the compliance process. Support the organization's email policy and compliance management program with formal employee training. Be sure to stress the fact that regulatory compliance is not an option; it is 100% mandatory.

GLBA and HIPAA aren't the only regulations that government agencies, school systems, and other public sector organizations need to worry about. Thousands of federal and state agencies regularly request access to email for audit or review. If you're unsure which government or industry regulations govern email, now is the time to find out. Assign a team of legal, compliance, records management, and IT professionals to determine where email fits into your organization's regulatory puzzle. Then establish a formal email management program, complete with a written retention policy. Support email retention with proven-effective email archiving, such as ArcMail Defender, to automate the process of locating and producing email records in a timely and compliant fashion—exactly when regulators request them and precisely in the manner they are requested.

WHAT CONSTITUTES AN ELECTRONIC BUSINESS RECORD?

Unfortunately, there is no one-size-fits-all definition of a business record. Every organization must determine for itself what type of email and other ESI rises to the level of a business record. In general, however, a business record, electronic or otherwise, provides evidence of an organization's business-related activities, events, and transactions. Business records are retained according to their ongoing business, legal, regulatory, operational, and historic value to the organization.

Not every message that enters or leaves your email system is a business record. Not every electronic conversation you conduct rises to the level of a business record. Your organization's welfare depends on your users' ability to distinguish business records from insignificant non-record messages. From a legal perspective, the process of formally defining, properly identifying, and effectively retaining electronic business records is one of the most important email management activities your organization can undertake.

BEST PRACTICE RECOMMENDATION:

When it comes to email business records, best practices call for the following:

1. Establish a clear definition of "business record" on an organization-wide or department-by-department basis.
2. Know—and adhere to—the courts' and regulators' record retention and production rules governing email and other electronically stored information.
3. Know—and comply with—the Open Records Laws governing all of the states in which you operate.
4. Communicate the organization's "business record" definition clearly and consistently to all email users. Make sure all users know the difference between business records and non-records—and understand their individual roles (if any) in the preservation of email records and the purging of non-records.
5. Establish written email retention policy and procedures governing the preservation of business records and the purging of non-records.

HOW LONG SHOULD EMAIL BE RETAINED?

If you're struggling with this question, you're not alone. There are different schools of thought on email retention periods. For some organizations, the retention and disposition of business records is governed by laws or regulations. In the financial sector, for example, the SEC requires regulated broker-dealers to preserve and produce three years' worth of electronic records immediately upon request. The Employee Retirement Income Security Act (ERISA), on the other hand, requires the indefinite retention of email and other documents related to employee benefits. The IRS, EPA, HIPAA, and other regulatory bodies all impose rules dictating email retention schedules.

That said, unless your organization's email and other electronic business records are governed by law or regulations, you are free to determine your own retention policies and deletion schedules. While the courts typically don't punish organizations for deleting email in the "ordinary course of business," many unregulated entities are opting to keep email for increasingly long periods of time. E-discovery rules and declining storage costs have motivated more organizations to choose long-term archiving over quick-fix deletion.

DESTRUCTIVE RETENTION OFFERS A FALSE SENSE OF SECURITY

In spite of email's ever-expanding evidentiary role, many organizations continue to engage in "destructive retention." Destructive retention calls for the preservation of email for a limited time, followed by its permanent deletion, manually or automatically, from the network. When it comes to destructive retention, preservation periods range from months to years. The most commonly applied retention period is seven years, according to ArcMail Technology.

If you opt for destructive retention, bear in mind that email never disappears completely. Your users (employees, executives, students, faculty, and staff) are likely to file, print, copy, forward, and otherwise hold onto internal and external email. Email recipients also may retain incoming messages from your users. At the end of the day, a retention policy that calls for the purging of email at regular intervals may render you the only party to a lawsuit who is unable to produce copies of your organization's own email. That's a position you never want to be in!

BEST PRACTICE RECOMMENDATION: BE STRATEGIC ABOUT EMAIL RETENTION & DELETION
The management of electronic business records is challenging for all organizations, large and small, public and private, regulated and unregulated. You simply cannot afford to play fast and loose with email and other electronic business records. Retention policies, deletion schedules, and archiving procedures should be driven by legal and compliance experts and supported by IT and archiving professionals who really understand the nature of business records and business record lifecycle management.

For growing numbers of organizations, the strategic retention and automatic archiving of all business-related email forever is the best way to manage electronic business records. In the course of e-discovery, everything is a potential business record. You have no idea what will—or won't—be valuable down the road. That's why archiving everything forever is a recommended best practice.

STATES PUT TEETH IN PRIVACY LAWS:
SECURITY BREACH NOTIFICATION LAWS

Forty-six states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands have enacted data breach notification laws, requiring organizations to notify affected parties in the event of a security breach involving personal identity and financial privacy information. The law takes data theft—and compliance with security laws and procedures—seriously. Comply with best practices and the law in all states in which you operate or have facilities. If your government agency or municipality, school system or university touches credit cards, Social Security numbers, protected health information, financial data, or other sensitive and private consumer information, then you must combine email policy and email retention policy with security tools and email archiving technology to ensure compliance with data breach notification laws.

REAL-LIFE EDUCATIONAL INSTITUTION SECURITY BREACH: When hackers breached The Ohio State University's computer system in 2010, personal information (Social Security numbers, birth dates, and addresses) of 760,000 current and former students and applicants, faculty and staff were in danger of identity theft. The largest security breach of the year, according to the Privacy Rights Clearinghouse, Ohio State's data breach put the university at legal and regulatory risk. In compliance with State Security Breach Notification Law, the university mailed notification letters to all 760,000 affected parties, established a dedicated website and toll-free hotline, and offered a free year of credit protection to everyone whose data was on the server.[3]

Summary:

10 EMAIL COMPLIANCE RULES FOR GOVERNMENT & EDUCATION

1. Define business record on an organization-wide or department-by-department basis. Make sure users can distinguish business-critical email messages from personal and otherwise insignificant email. Make clear what role, if any, individual users play when it comes to email record retention and deletion.
2. Form an email management team made up of your legal counsel, compliance officer, records manager, human resources manager, and IT director.
3. Know and adhere to the Amended Federal Rules of Civil Procedure.
4. Research and comply with the State Rules of Civil Procedure governing e-discovery and email retention in every state in which you operate or litigate lawsuits.
5. Know and comply with the Open Record Laws of every state in which you operate or have employees or facilities.
6. Establish a formal, written email retention policy.
7. Assign legal the task of forming a litigation hold policy to halt the routine destruction of email records and other ESI once litigation is underway or legal claims are anticipated.
8. Create an audit trail. Eliminate potential surprises by investigating your email system to determine exactly who has been doing precisely what on the system. Take steps, through written email policy, email retention policy, and ArcMail's Defender solution to demonstrate that your email records are authentic, reliable, and legally compliant. If you can demonstrate that your email archiving solution is reliable, and your email records are tamperproof, then your organization will be on more solid footing with courts and regulators.
9. Educate all of your email users. Don't expect users to understand business records—or their individual roles in email management—without formal training. Address, among other topics, legal, regulatory, and security risks facing the organization and individual users; content and usage rules; email monitoring realities vs. privacy expectations; laws and regulations governing email content and record retention; e-discovery risks and requirements; and disciplinary action—up to and including termination—awaiting users who violate email policy, email retention policy, federal and state laws, or regulatory rules.
10. Automate the archiving process with ArcMail Defender to enhance productivity; reduce search costs; enforce email retention policy compliance; ensure the legal validity of electronic evidence; meet e-discovery obligations; maximize legal and regulatory compliance; and minimize organizational risks.

ABOUT ARCMAIL TECHNOLOGY

ArcMail is a world-class trusted provider of scalable archiving solutions that address multiple business issues through best-in-class technologies and services. For more information, visit www.arcmail.com or call 888-790-9252.

ABOUT THE ePOLICY INSTITUTE™

www.epolicyinstitute.com

The ePolicy Institute is dedicated to helping employers limit email and Web risks, including litigation, through effective policies and training programs. The author of 11 books including *Handbook of Social Media* (2011 Pfeiffer) and *The e-Policy Handbook, 2nd Edition*, Founder and Executive Director Nancy Flynn is an in-demand trainer, consultant, and expert witness. Since 2001, ePolicy Institute has collaborated with American Management Association on annual surveys of workplace email/Internet policies, procedures, and best practices. A respected media source, Nancy Flynn has been interviewed by thousands of media outlets including *Fortune, Time, Newsweek, Wall Street Journal, US News & World Report, USA Today, New York Times*, NPR, CBS, CNBC, CNN, NBC, and ABC. For information about ePolicy Institute training programs and other products and services, contact 614-451-3200 or nancy@epolicyinstitute.com.