



JATHEON
DATA | KNOWLEDGE | INSIGHT

Why You Have to Use Archiving for Complete Compliance

White Paper



CONTENTS

INTRODUCTION	3
WHAT DO THESE REGULATIONS STIPULATE?	4
MAIN COMPLIANCE CHALLENGES	4
KEY REGULATIONS IN TOP INDUSTRIES	5
WHO NEEDS TO ARCHIVE?	6
WHY IS BACKING UP NOT ENOUGH?	7
WHAT DO COMPANIES NEED TO DO?	8
THE ADVANTAGES OF AN IN-HOUSE ARCHIVE	9
ABOUT JATHEON	10



INTRODUCTION

MOST BUSINESSES AND ORGANIZATIONS TODAY ARE AWARE OF CERTAIN RESPONSIBILITIES THEY HAVE WHEN IT COMES TO THE ARCHIVING OF EMAIL AND OTHER TYPES OF INTERNAL COMMUNICATIONS UNDER COMPLIANCE LEGISLATION, BUT AREN'T SURE WHAT THE PURPOSE OF REGULATORY COMPLIANCE IS OR HOW TO IMPLEMENT IT.

Simply put, compliance legislation is a set of legal rules governing the protection and preservation of data. This means that communication data, among other types of information, must be protected from unauthorized access and stored for a certain period of time before it can be legally disposed of. This legislation is intended to increase transparency and maintain relevant information (such as email data) available in case it is required for any kind of legal purposes.

As a result, companies are taking email archiving and record keeping more and more seriously, in part also due to recent shake-ups across different industries. Organizations of all sizes from industries all over the spectrum face the need to comply with extensive rules and regulations when it comes to the retention of emails, instant messages and social media information. Those who fail to comply are increasingly at risk for audits, government investigations and lawsuits, and can face fines or even, in severe cases, imprisonment, as dictated by regulatory bodies.



WHAT DO THESE REGULATIONS STIPULATE?

When it comes to communication data archiving, many regulations have things in common. Simply put, email and other types of digital communications are considered important records which must be retained and produced when requested by a regulator.



Every industry has its own retention period, that is, the length of time that records should be stored securely for. While email archiving is the basic requirement across most industries, other types of communication data, such as instant messages, also need to be archived. In fact, according to regulatory notice 10-06 published by Financial Industry Regulatory Authority (FINRA), the largest independent securities regulatory body, emails, instant messaging, chats and social media activity are all included under compliance regulations.

MAIN COMPLIANCE CHALLENGES

Here are some of the most common compliance challenges faced by numerous industries. Some of these apply across the board, while others are industry-specific:

- **Records management** – companies are required to retain all communications like email, instant messages, and others based on timescale, as well as dispose of them appropriately and in compliance with industry-specific regulations.
- **Data leak protection** – organizations that deal with sensitive information, such as financial firms, are obliged to protect it and prevent data leaks.
- **eDiscovery** – organizations can be obliged to provide communications as evidence in legal inquiries, while they can also use them in company disciplinary procedures.
- **Internal retention policies** – in addition to regulatory requirements, or rather in anticipation of them, companies might want to implement their own messaging retention policies internally.



KEY REGULATIONS IN TOP INDUSTRIES

The following table summarizes some of the key regulations concerning the storage and management of electronic data which companies in virtually all industries are subjected to at some level:

Industry	Key Regulators	Overview of Requirements
Financial Services	<ul style="list-style-type: none"> • Basel II Accord (EU) • Securities and Exchange Commission (SEC) • National Association of Securities Dealers (NASD) • New York Stock Exchange 	<ul style="list-style-type: none"> • Schedules for records maintenance • How records are maintained • How client communication records are maintained and supervised • How financial information privacy is protected internationally
Healthcare and Life Sciences	<ul style="list-style-type: none"> • Health Insurance Portability and Accountability Act (HIPAA) • Medicare Conditions of Participation • Food and Drug Administration 	<ul style="list-style-type: none"> • Schedules for records maintenance • Disposition of records • Standards for records storage
Government Agencies	<ul style="list-style-type: none"> • General Records Schedules from the National Archives and Records Administration • Various other statutes and requirements 	<ul style="list-style-type: none"> • Schedules for records maintenance • How records are maintained • How client communication records are maintained and supervised • How financial information privacy is protected internationally
All Commercial	<ul style="list-style-type: none"> • Sarbanes-Oxley Act (SOX or Sarbox) 	<ul style="list-style-type: none"> • Schedules for records maintenance
Enterprises	<ul style="list-style-type: none"> • Gramm-Leach-Bliley Act • Personal Information Protection and Electronic Documents Act (PIPEDA) (Canada) • Internal Revenue Service Fair Labor Standards Act • Americans with Disabilities Act • Occupational Health and Safety Act • Various other statutes and requirements 	<ul style="list-style-type: none"> • How records are maintained • How personal information is gathered, stored and protected



WHO NEEDS TO ARCHIVE?



While every industry can benefit significantly from investing in email archiving, most organizations in the following industries are required to have an email archiving system due to different laws and regulatory requirements:

- Financial Services
- Healthcare
- Government
- Police
- Education
- Legal Services
- Construction
- Defense

However, according to some sources, as much as 53% of businesses in the United States do not include emails in their records management, and a further 39% don't employ any sort of email retention policy.

Unfortunately, not being aware of regulations is not an excuse for non-compliance. While decision makers and managers have also avoided archiving their emails and other communication data due to costs associated with it, they should consider the substantial cost they are likely to face as a result of non-compliance.



WHY IS BACKING UP NOT ENOUGH?

What is it that makes archiving necessary under these circumstances? Why is it not enough to simply back up data, as most companies and organizations already do?

Archiving is necessary because most regulations require the retention of emails and other communications in a read-only format, including their metadata (date of creation, last modification, etc.), for a certain amount of time. Additionally, companies are not only required to store internal communications, but are also required to be able to produce them when needed.

While a backup is mostly meant to restore files after disk failure or server issues, archiving stores documents as well as their metadata, and usually involves a much more complex indexing system, allowing for advanced search.

Archived emails and messages, unlike backed up ones, can be searched thoroughly and found quickly and easily. Email archiving allows eDiscovery to take place extremely efficiently, saving companies both time and money.



Finally, having an archiving system means having an automated process, rather than leaving this task to the (probably already burdened) IT department, thus freeing up IT time and minimizing the risk of human error.





WHAT DO COMPANIES NEED TO DO?

There are both administrative and technological steps that need to be taken set up an email archiving system in order to reach a level of compliance that will stand up to legal scrutiny.

Internally, companies should establish a thorough electronic communication and data retention policy that will specify employee expectations when it comes to all types of electronic communications initiated at the workplace (email, instant messaging, social media interactions, etc.). It should be made clear to employees that no communication initiated from a workplace platform (including even company-issued smartphones) is privileged or private.

Internal retention policies for saving, purging and managing email should also be implemented. This will promote email management best practices alongside archiving and prior to audits.

Finally, when it comes to setting up an archiving system, organizations just need to choose and implement an archiving solution. Choosing from the myriad options available out there could seem daunting, but various factors make an in-house archive the most compelling solution.



Employees should also be aware of how long electronic communication is archived and retained on the company network, as well as know the potential legal ramifications.



THE ADVANTAGES OF AN IN-HOUSE ARCHIVE

There are several advantages of establishing an in-house archiving solution:

- **It Provides Information Security**

Due to the highly confidential nature of many emails and file attachments, company leaders are often uncomfortable having their data archived off-site by a third party – especially since email archiving is currently an unregulated industry. In fact, the National Association of Securities Dealers (NASD) said in a Member Notice that “outsourcing an activity or function to a third party does not relieve members of their ultimate responsibility for compliance.” In other words, if a company doesn’t thoroughly investigate the service provider, and it’s later realized that company emails haven’t been properly archived, it is the company that gets fined, and not the vendor.

An in-house archiving solution avoids this situation altogether.

- **It Is Quick and Simple**

An in-house archiving appliance (no larger than an average router) can be set up and functioning in a matter of hours.

Additionally, managing the appliance after setup (which is usually completed with the appliance vendor or integration partner) is fairly simple, and requires little or no IT experience.

- **In Lets Servers Breathe**

In high-volume periods, server performance can be compromised when messages must share the same bandwidth. An in-house archive, on the other hand, captures copies of all incoming and outgoing messages after or before they make contact with the outside world, with no impact on bandwidth or server performance.

- **It Is Cost-Effective**

The appeal of an outsourced solution may be its apparent cheaper price tag. While it’s true that there are fewer start-up costs when outsourcing an archive to a third party, over time the cost analysis favors in-house solutions, as they are paid for once, in the beginning, while the costs of third party solutions go on indefinitely.



Taking into consideration the potentially high costs of non-compliance and the threat of non-compliance lawsuits, companies from industries across the board need to think about the archiving of email and other types of communication data. By establishing a good in-house archiving solution following a few simple steps, companies can not only ensure their future compliance, but can also gain significant strategic advantage.

Find out how Jatheon can help you implement an in-house archiving solution for complete compliance by [contacting us](#) or by [requesting a demo](#).

ABOUT JATHEON

Founded in 2004, Jatheon Technologies Inc. designed the world's first non-intrusive network appliance.

Today, Jatheon continues to raise the bar throughout the industry with its latest enterprise grade **cCore** appliance line, and **ergo**, its powerful email archiving, indexing, retrieval and dynamic monitoring software solution, and best-in-class technical support, **The Jatheon Guarantee**.

Jatheon is headquartered in Toronto, Canada and serves clients worldwide through its network of global business partners. For more information, please visit www.jatheon.com.