Are you playing by the rules?

Why email archiving and fax solutions are critical for meeting compliance

GFI®

Let's play a game: Imagine it's Tuesday morning after a long weekend. Three hundred unopened emails have arrived since Friday and you haven't finished your first cup of coffee. And let's face it, you are not at your best this morning anyway.

As you go through the list, you find an email marked "URGENT" from an ICO.org.uk address.

With growing concern, you read that a formal complaint has been lodged against your organization and department for sending customer records to the wrong fax address, revealing sensitive information about a dozen clients. Horrified, you immediately start to investigate how such a mistake could possibly happen. Pulling up your mail archiving solution and digital fax maker log, you quickly search through the dates and destinations identified in the complaint. With a long sigh of relief, you see that the faxes were sent to the correct address and that a confirmation email was received from the receiving party. Relaxing now, you prepare an email summary of the issue with your findings and forward it to legal.

You go back to your coffee and email sorting.

Unfortunately, that is not how the day went for North Staffordshire Combined Healthcare NHS rust when it received a notice of complaint from www.ICO.org.uk. Unable to defend itself with proof, it ended up paying a £55,000 fine because three sensitive faxes were sent to a member of the public instead of a health institution.

This scenario is playing out across the Globe, and forcing companies everywhere to take privacy issues more seriously. Due to the Health Insurance Portability and Accountability Act (HIPAA) in the United States, organizations dealing with medical information have similar requirements such as verifying the destination number before sending a fax and waiting at the fax machine for a response. Fines upon conviction for violation of rules can range from $100 per record to $50,000 per record.

Germany has similarly stringent regulations under the GDPdU for tax relevant documentation. These regulations stipulate

how documents must be preserved, who they are able to be accessed by, and the consequences for the improper storage or disclosure of those documents.[1]

The modern organization produces and consumes massive amounts of data. In email, fax and electronic documents, the flow of information can seem endless, and as the quantity grows, so too does the complexity of its management, storage, retrieval and retention. In addition, the connectivity of organizations and mobility of their data brings a new set of challenges. The importance of strong data retention and storage policies is greater than ever and in today's litigious and privacy-conscious society, the stakes have never been higher.

With the number of lawsuits and regulatory fines over the disclosure of customer or client information, it's tempting to want to destroy records as quickly as possible to protect them from falling into the wrong hands. However, that information may be the only way an organization can prove how a scenario transpired, and the only way to demonstrate proof of proper use and storage. Also, consider that just because your company didn't retain the data doesn't mean that a client or other party purged it too. Finally, the reality is that deleting the collective memory of an organization every few months is grossly impractical and in some situations, even illegal. There are many reasons to keep records and each has its own requirements. Record retention is important, regardless of jurisdiction, to deal with possible:

- Civil litigation
- Government inquiries
- Internal investigations

Civil litigation: The US has seen a surge of class-action lawsuits related to data breaches in recent years. With a mean plaintiff payout of $2,500 and a mean attorney fee of $1.2 million for cases that settle, it definitely appears that the class-action attorney fees are driving this bus. The situation is different in other jurisdictions, but the same potential exists, and trends show that the "lawsuit happy" culture traditionally found in the US is spreading. At the same time, it's not just class actions that are an issue. Any civil action brought against your company has data-retention implications. If your organization communicates with clients or other parties by fax or email, you will be required to disclose those communications, known as

[1] See GFI's white paper "Compliance with the requirements of GDPdU using GFI Archiver for Exchange" for an extensive analysis: http://www.slideshare.net/GFISoftware/son-whitepaper-engfigdpdujnv14e

"e-discovery," during litigation proceedings. While time limits for bringing a claim vary by jurisdiction, many lawsuits involve events that occurred years earlier.

During the legal process, it is important for a party to demonstrate strict controls and policies concerning any data it relies upon. The weight, or reliability, of evidence being put forward will be affected by the strength of data-retention policies already in place; if the data could be altered, who had access to the data, and if it can be shown that the retention policies were consistently followed. This will be particularly so if one party is unable to produce any pertinent material (such as an email conversation).

Government inquiries: When a breach is alleged, it is often a government department that responds to the incident, such as the UK's Information Commissioner's Office (ICO). Since 2010, the ICO has levied fines totaling more than £4.5 million. With the capacity to audit, fine and even criminally prosecute, the UK has established itself as a leader in the prevention of data breaches.

The following is a summary of the different penalties for privacy breaches in a variety of jurisdictions:

Germany
A maximum €300,000 fine for administrative offenses
Criminal sanctions (maximum of two years imprisonment or a fine)
Damaged reputation
Confiscation of profit and benefit derived from a violation
Civil liability and injunctive relief (under competition law)
See Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU) - Principles of Data Access and Verifiability of Digital Documents

United Kingdom
Fines up to £500,000 for serious breaches of the Data Protection Act or the Privacy and Electronic Communications (EC Directive) Regulations 2003
Enforcement notices requiring organizations to take (or refrain from taking) specified steps
Information notices requiring organizations to provide the ICO with specified information
Undertakings committing an organization to a particular course of action
Assessment notices to conduct compulsory audits to assess an organization's compliance
Prosecution for criminal offenses under the DPA

United States
A consumer's actual damages and attorney's fees; and injunctive relief
In 2011, it cost an organization the suffered a data breach an average of $5.5 million
Industry-specific fines (e.g., HIPAA: $50,000 maximum per violation; $1.5 million calendar year cap)

If a company falls under the purview of a particular governmental body (HSA, FCC, ISO) it is prudent to follow the published best practices and consult with that body on implementing effective policies and procedures. After all, what better way to avoid fines and levies than to use that agency's own rules and regulations to guide your efforts?

Internal company review

Internal reviews are conducted for a variety of reasons, including organizational purposes and assisting a government body in resolving a criminal or civil investigation. Ideally, an organization wants to provide appropriate information without having a full audit conducted. The cost of internal reviews can be staggering for large companies. For example, in 2011 Avon disclosed that it spent $93.3 million on an internal review, with the cumulative total

for three years being more than $140 million. Regardless of the size of the organization, being able to provide comprehensive information will be of critical importance.

Unfortunately, responding to a data breach in any of these situations can be costly, particularly if you are dealing with:

- Detection and escalation costs of breach;
- Notifying customers
- Lost business
- Post data breach costs.

These costs will vary based on a wide range of factors including jurisdiction. An extreme example of soaring post-data breach costs is TJX, an American clothing company, whose expenses for contacting affected customers and providing credit watch services alone over an 18-month-long data breach are estimated to be more than $1.24 billion.

On a different scale, the UK's ICO recently fined a small money-lending company after the owner's briefcase, containing an unencrypted portable hard drive, was stolen from his car through an open window while he was stopped at a red light. While the £5,000 fine (along with the £3,600 that was in the briefcase) was minor compared to the costs of the TJX example,no doubt it had a significant financial impact on the company.

Regardless of the context and the specific laws with which a company is obliged to comply, there are a few key points for any business to consider when looking at data storing and retention. Organizations need to:

- Maintain secure storage of company data
- Maintain restricted access to company data
- Maintain data for time limits as required by authorities in their jurisdiction
- Ensure data is properly disposed in a secure and orderly fashion after retention periods expire
- Ensure data is searchable, and easily accessed by authorized personnel

To support themselves in achieving these measures, organizations need to implement a set of IT solutions that allow for simple, secure data and electronic message management.

Automated faxing solutions offer organizations a secure, paper-free, way to send faxes, with a means of recording what was sent, where it was sent, and when it was sent. Automated faxing allows for trunking of faxes directly to the inbox of the intended employee, rather than relying on a manual process that poses a

risk to data security and is time-consuming. Robust messaging archiving solutions make sure that both those fax emails as well as all other emails are stored in a secure and tamper-free environment. (Secure storage should automatically include all faxes sent and stored, and provide a transmission report and transaction log.)

With an email archiving solution in place, organizations can set global policies for data retention so that documents are retained as required and destroyed at the proper time.

Safe and secure fax and email

With server systems and databases stored in secure locations and managed solely by authorized personnel, there is no risk that emails and faxes can be tampered with, deleted or accessed by third parties. This ensures that all patient information is secure at all times – prior to, during and after transmission.

No more paper waste or wrong numbers

Automated faxing enables users to quickly and easily send, receive and manage fax communications from their desktops. With faxes composed in a word processor (or other application) or created via email (commonly known as "email-to-fax"), numbers can be selected from the email client's address list or entered manually. As a result, your end-to-end fax communication process is shorter, more efficient and better organized.

No more waiting around the fax machine

Automatic inbound routing sends faxes directly to the recipient's desktop, eliminating the risk of being discarded or read by an unintended recipient.

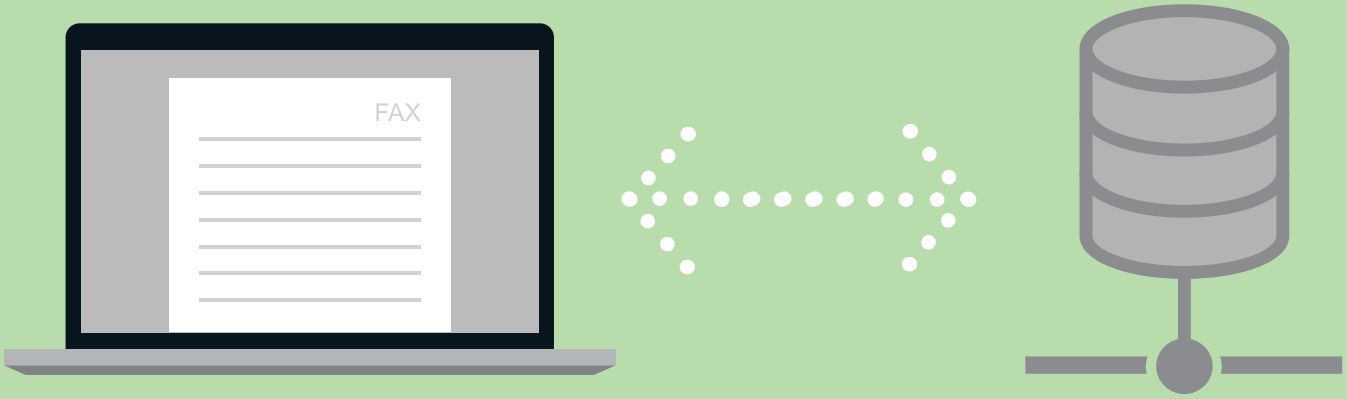
No need for secure fax machine location

Both outbound and incoming faxes can be sent and received using an email client

or, preferably, a third-party health records application. This eliminates the need for a manual fax machine and special security measures to safeguard the data or the equipment.

Email storage compliance at your fingertips

Legislation such as GDPdU demands you follow multiple requirements to meet compliance; basic storage of email (for example, in PST files on a local disk) is no longer acceptable. Under the GDPdU, emails and documents transmitted by email must be stored in a manner that provides for:



- Immediate read access
- Data storage in a tamper-proof environment
- Auditor access for third-party evaluations and verifications
- Retention of documents for specified time periods
- Ability to export data in commonly readable formats.

With an email archiving solution, these features are standard.

Whether you are operating locally, nationally, or globally, privacy and data protection legislation will impact how you do business.

The rules of the privacy game are continually changing as legislators and policymakers play catch up. When a breach is alleged or a complaint is filed, an e-discovery process or audit will be required to meet requests of a government regulatory body or for civil litigation. This process is time-consuming, complicated and challenging, but will be more so if data is not properly retained and stored. This can result in increased fines, higher settlement fees or court judgments against the business, not to mention the incalculable cost of your clients, customers or stakeholders losing faith in your business simply because you were unable to demonstrate proper storage of their information and data.

GFI Software™ offers a range of solutions to enable companies to improve the security and efficiency of their email and messaging systems, while helping them meet the requirements for compliance with data protection and retention legislation. Software solutions such as GFI Archiver® and GFI FaxMaker® specifically offer the compliance-related features described above. ***For more information about GFI's email and messaging solutions, visit our website:*** *www.gfi.com*

Click here for a FREE GFI Archiver 30-day trial, or click here for a FREE GFI FaxMaker 30-day trial.

GFI 6012 oct13

www.gfi.com

For a full list of GFI offices/contact details worldwide,
please visit: www.gfi.com/contact-us