eFax Corporate®

White Paper

Compliance in a World of Digital Documentation

TABLE OF CONTENTS

Executive Summary

In a digital world, businesses of all sizes cannot function without the ability to share information. There is an increasing expectation for speed, ease of access, and to be able to find anything at the click of a button or a quick search.

Meanwhile, with 60% of IT decision-makers responding to an eFax survey saying they are accelerating the speed of their digital transformation projects as a direct result of the current pandemic, businesses are only going to be more digital.[1] Being able to share information securely is critical to that.

Then there's the cost of dealing with paper – Gartner has previously estimated that the cost of filing, storing and retrieving paper for US businesses was between $25 billion and $35 billion.[2]

This all points to the fact that all information and data, needs to be digitised in one form or another, whether it's a social media post, table in a spreadsheet or a vital document. These documents — whether they are faxes, email attachments, digitally shared, or processed in another digital format, have now become a critical component of business communication.

Yet for all the ease of sharing and accessing, they are still bound by compliance and other regulations that are designed to protect personal information and data. This means that businesses must be responsible for the safe and secure management of digital documents, yet how many organisations are educated on the appropriate dissemination of information via approved technologies?

Knowing the who, what, when and where of electronic document transmission is now a critical element of e-document control that should be used to prevent policy and compliance violations and, most importantly, assign accountability to the information transmitted or received. Unfortunately, those control methodologies often come at the cost of productivity, where controls, rules and policies prevent employees from sharing the information needed to accomplish projects or meet their daily work objectives.

This paper explores some of the challenges businesses face when wrestling with the compliance of digital documents, what it means for heavily regulated sectors, and also outlines some of the steps organisations can take, to ensure they remain compliant without hampering productivity or information sharing.

The Need for Compliance in Digital Documentation

The sharing of data, in any form, has long been a legislative, regulatory and ethical minefield. As individuals, businesses and legislators have become more knowledgeable of the power of data and the implications of data sharing, so too have the calls for better protection and accountability become louder. General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) have solidified both what protection individuals should expect, and what businesses are obligated to do. Critically, they have also made clear what punishments those that fail to comply can expect.

This all creates additional responsibilities for organisations who would hold any sort of data. Perhaps unsurprisingly, many struggle to find solutions that will counter compliance violations without impacting productivity.

Yet the current pandemic demonstrates exactly why we should all find better ways to share information quickly. Whether businesses looked to move their workforces remote in days and hours, or healthcare providers needed to share patient information rapidly, across multiple industries the sharing of data and documentation has been critical to how successfully organisations have continued to operate.

The pandemic was a black swan event where the usual processes and rules were temporarily suspended. Yet it demonstrates what could happen when the right focus was applied.

Fundamentally, there are a number of core problems when it comes to sharing and managing digital documentation.

1. Ensuring Equal Yet Secure Access: One of the biggest challenges associated with managing electronic documents is offering equal access to the intended recipients while still incorporating security controls. For example, many businesses have turned to canned services that focus on file sharing for the delivery of electronic documents. However, those services often lack the ability to fax, email or otherwise transmit electronic documents in a secure and auditable fashion. Also, many of those file-sharing services lack the ability to save electronic documents for the long-term and offer no transmission controls or management capabilities.

2. Sharing with Both Internal and External Users: The limitations of file-sharing services have forced businesses to consider other options, including deploying their own internal fax servers, document servers or other transmission platforms. Nevertheless, those internally deployed document transmission systems are often closed systems, ill-equipped to deliver documents or extend access to external parties. This often introduces incompatibilities, creating user administration management headaches which can add stress to overburdened IT departments with frequent requests and security changes.

3. Supporting Flexible Relationships: Another strike against both filesharing services and internal systems are that they tend to be designed for long-term relationships and are often ill-equipped to deal with infrequent or singular requests, such as forms, instructions, guides, or generic statements. Businesses want to be able to share documentation quickly, with a simple click-and-go approach, not have to get every party to sign contracts and receive a password before accessing a document once.

A Digital Platform for Digital Business

File sharing and internal systems are, in many ways, relics of a more analogue approach to technology. If, as we've seen, businesses want to become more digital, then their ambition has to cover every aspect of operations, including documentation.

To deliver on this ambition, requires platforms that are affordable, interoperable and secure. This is why we are seeing more companies move to the cloud – much hyped over the years, but only now becoming the default infrastructure for many organisations.

The right cloud environment gives companies ready and fast access to services that can be deployed in hours and days, rather than weeks and months, yet still offers the security and auditing capabilities needed to securely transmit documents, and the effective control of the information contained within those documents.

Cloud-based solutions are able to accomplish this by abstracting the management of digital documents from closed, internal systems and unifying access across a multitude of browsers, infrastructures and operating systems. That makes a cloud-based service immune to the incompatibilities often encountered by extending closed internal systems across multiple domains to external users. In other words, a cloud-based service becomes the great equaliser between different platforms, users and applications.

Furthermore, a properly executed digital cloud service incorporates security, encryption and auditing controls that can become the foundation of a digital document transmission system, allowing businesses to retire internal servers.

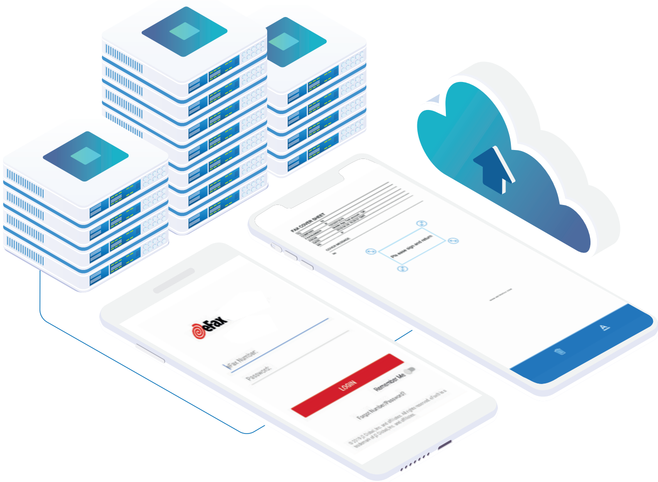
Securing the Digital Cloud

One of the reasons cloud adoption was initially slow was due to concerns around security. By outsourcing the physical hardware involved in hosting servers and data, how could businesses be sure it was secure?

Granted, the increasing digital footprint or connectedness of life today does increase the potential surface area that needs to be protected against cyber-attacks. Yet businesses are still more at risk from the human factor within their own organisation than they are from a failing of a digital cloud provider, as a Verizon report noted when it said 30% of breaches came from internal sources.[3]

But the fact is that we are all more connected. The eFax book ‘Extending Cybersecurity to Faxing’ highlighted instances where some had suggested that going analogue was a solution; however, as it went on to note, “for the majority of organisations, [not being connected] simply is not practical.” [4]

The answer then has to be to recognise security concerns and address them. Attacks may be coming more sophisticated; as such, the countermeasures need to be equally advanced.



First, however, it is necessary to identify those potential gaps in defences. When it comes to the transmission of digital documentation, that includes maintaining portability while ensuring security. With different types of sending documents available, businesses need to ensure they have appropriate security policies in place, with different controls needed for those sent via a fax service versus those shared over email or via file-sharing services. Maintaining security means that the management of transmission services must be unified, so that the same policy rules and accountability requirements can be applied to e-documents, regardless of the transmission services used. However, adopting those methodologies usually results in a closed platform that makes it difficult to share e-documents and can impact productivity as well.

Success in securing e-documents requires combining policies with open-platform technologies, which leverage cloud services. Those services should provide:

- Encrypted transmission of documents
- Easily retrievable audit data and access logs
- Integrated faxing, email and document transmission capabilities
- Policy-driven security controls to allow/deny transmission of documents
- Easy-to-use interfaces that work across multiple browsers and operating systems

Ultimately, it’s about balance – of complete security which does not hamper productivity, of the ability to share information as required without compromising security. End-user tools associated with a cloud-based document platform should be simple to use and work across multiple platforms and operating systems, enabling users, whether onsite, remote or external parties, to send and receive e-documents at will, without violating company policy or compliance requirements.

Industry Focus – Delivering Digital Documents in Healthcare

If one industry captures the challenges of transitioning to paperless operations while ensuring the fast yet completely secure exchange of documentation, it is healthcare. With many providers digitalising operations where possible, any innovation that promises to cut costs while contributing to improving service levels will be of interest to the industry.

Secure document transmission is one such area, in particular faxing. Yet faxing and healthcare has a complicated relationship – notably in the UK. In 2018 the technology was dismissed as “archaic” by health secretary Matt Hancock MP, with the Minister for Health and Social Care mistakenly declaring that “everyone else got rid of them years ago.”[5] The solution was email, with Hancock saying it was more secure and effective than fax, and going so far as to set a deadline for the removal of all fax machines from the NHS.

However, as ‘Extending Cybersecurity to Faxing’ states, “the suggestion that email is a like-for-like replacement is undermined by the fact that if that were the case, the sectors that rely on fax for certain communications would have migrated over a long time ago.”[6]

Any alternative to faxing needs to meet stringent standards for protecting patient privacy. In the UK, that means meeting NHS Digital Information Governance standards. For example, there are 12 requirements for digital fax providers to meet in order to comply with standards in that area. These range from having an IT management framework based on ITIL, to implementing a Performance Monitoring System and having

appropriate Disaster Recovery provisions in place to maintain continuity of service.

For third party technology providers, needing to be compliant with public sector standards is a common occurrence. What many may not realise is that needing to meet compliance extends to other suppliers.

Neighbourhood Midwives is a case in point. An independent midwifery service set up in 2013, it provides both private and NHS services. With ambitious plans to expand across the UK, it needed to ensure that its IT systems could scale to accommodate growth targets. As part of this, these systems are audited on an annual basis in accordance with NHS Digital's Data Security and Protection Toolkit (on top of regular inspections through the Care Quality Commission and NHS England). This means records must be accessible for inspection at any time. No wonder that founder and IT Manager, Eleanor May-Johnson says that the company's "IT systems are as important as the care we provide to our clients".

With many of its referrals coming via fax, it needed to deploy a solution that met the needs of both the business and NHS standards. With a dispersed team, having physical fax machines was not an option, so it deployed a digital fax service, based in the cloud, which gave it the ability to receive and send faxes, no matter where its employees were, from smart phones, laptops or tablets. As well as being easy to set up and secure, using digital faxing meant that Neighbourhood Midwives also complied with the relevant NHS regulations on storing and sharing patient data, while the cloud-based storage meant that files could be easily sorted and accessed when it came to audits.

Six Steps to Digital Document Compliance

Ultimately, as organisations in all sectors consider what the future looks like, they are seeking ways to be able to create, share and access digital documentation in a compliant-friendly way. While all businesses have unique issues that they alone can deal with, there are some consistent themes that they should consider when looking to implement digital document transmissions securely.

- **Ensure Reliable Document Capture:** Use technologies that can transform paper documents into digital files that can be transmitted, as well as tagged and stored in an electronic document repository for quick and easy retrieval, retransmission, and archiving.
- **Secure Access to Sensitive Documents:** Compliance dictates that some documents containing personally identifiable information have restricted access and secure sharing. Adopt a document transmission methodology that can incorporate authentication and password protection, allowing electronic documents to be only transmitted (or received) by those with the correct authorisation.
- **Consider Alternatives:** Investigate digital cloud services that incorporate document capture and transmission, allowing for a distributed methodology to work with electronic documents that must be secured, tracked and meet compliance regulations.
- **Accountability:** Deploy management techniques that combine digital document transmission controls with policy-based accountability to ensure that compliance and legal requirements are met, while enabling workflow and document movement auditing.
- **Workflows:** Improved business efficiency is at the heart of digital transformation. Cloud repositories can be used to organise electronic documents and even enable self-service delivery, where a recipient can request documents via a website and have those electronic documents faxed, emailed or delivered electronically using automation technology. Automated tasks and email notifications can help keep employees informed of requests and on track to follow up with other electronic documents.

Additional Information

Further Reading

Digital Acceleration in the Pandemic; How organisations can adapt to the New Normal

The need for digital transformation is not new. As a recent Harvard Business Review article noted: “technological advancements were already changing the world over the past two decades, from living standards to the very nature of our work.”[7]

This paper looks at how digital transformation can actually bring intangible benefits. Drawing on exclusive new eFax research, it highlights what businesses in different industries see as the key drivers in their digital journey, where they think they would be had the pandemic not prompted action, and what the lasting impact of digital transformation will be.

Extending Cybersecurity to Faxing

When it comes to the security conversation, much is made of how existing systems and approaches are ill-suited to tackle modern threats. With many organisations wrestling with ongoing digital transformation journeys, most are caught in a dangerous no-man’s land. As they digitise their operations, they also increase their risk, but their security processes have yet to evolve at the same rate.

This paper looks at how organisations are handling different security threats and the role cloud faxing has in helping securing the enterprise.

[1] https://www.efax.co.uk/docs/default-source/efax-corporate/digital-transformation-ebook_LSCAPE_SMB_.pdf
[2] https://www.telegraph.co.uk/business/ready-and-enabled/backing-up-work-in-paperless-world/
[3] https://enterprise.verizon.com/en-gb/resources/reports/dbir/
[4] https://www.efax.co.uk/docs/default-source/efax-corporate/cybersecurity_LSCAPE.pdf
[5] https://www.gov.uk/government/news/health-and-social-care-secretary-bans-fax-machines-in-nhs
[6] https://www.efax.co.uk/docs/default-source/efax-corporate/cybersecurity_LSCAPE.pdf
[7] https://hbr.org/2020/09/how-to-harness-the-digital-transformation-of-the-covid-era

About eFax

eFax launched its digital cloud fax service with the goal of using the convenience of email and the speed of the internet to make it easier for people to send and receive faxes. eFax lets users and our 11 million customers receive, review, edit, sign, send and store faxes by email or through a web interface. Our appeal and success are built around three key features: the widest selection of phone numbers; an easy way to send and receive faxes and voicemail by email; and a fast, reliable and secure communications network.

To learn more about outsourcing to a digital cloud fax model with eFax, visit us at: eFaxCorporate.com

European Headquarters

eFax
European Headquarters
Unit 3, Woodford Business Park
Santry, Dublin 17, Ireland

Contact Sales:
UK 0800 689 0588
Rest of Europe +353 (1) 656 4950

Web:
eFaxCorporate.com

Follow Us