Accellion

AN ACCELLION WHITE PAPER

Building Enterprise Secure File Transfer Processes that Improve Your Security and Compliance

COMPLIANT, EASY TO USE, AND EASY TO MANAGE

Accellion, Inc.
1900 Embarcadero Road
Suite 207
Palo Alto, CA 94303

Tel +1 650 739-0095
Fax +1 650 739-0561
www.accellion.com
info@accellion.com

Executive Summary

Virtually all businesses today have work processes that dictate the need to share critical business information with people outside as well as inside the organization. The information may be highly confidential intellectual property, patient health records, sensitive customer data, financial information or the like. This presents a challenge: How to transfer data from one person or company to another in a secure, auditable, reliable, compliant and easy to use manner?

Information can be at risk of loss or exposure when it is being sent from one person to another, depending on the file transfer process that is used. Email is the easiest and most common method used, but unfortunately, it is inherently insecure. FTP also is common, and not only is it insecure, but itôs hard for the average person to use. Some people choose to put unencrypted information on CD-ROMs and send them via courier. All three of these common file transfer processes ï email, FTP and CD-ROMs ï are risky, normally non-auditable and ñnon-compliantòwith legislative mandates that dictate appropriate information handling procedures.

Protecting data is a matter of observing how and when the data is at risk, and finding appropriate methods to mitigate those risks. Mandates such as the Sarbanes-Oxley Act (SOX), the Health Insurance Portability and Accountability Act (HIPAA), the Graham-Leach-Bliley Act (GLBA), and others provide guidelines on what companies can or must do with the information they handle. Where electronic business records are concerned, it is incumbent on the IT department to take those guidelines and implement appropriate business and technology measures to ensure compliance with the legislative mandates as well as corporate policies.

In the case of a secure file transfer solution, the IT department needs to provide workers with the file transfer technology that addresses security and compliance needs without putting an unreasonable burden on normal work processes and the ways people prefer to work.

This whitepaper discusses the issues important in selecting a solution for user-to-user secure file transfer that ensures your methods for handling private information adhere to your security and privacy policies and government mandates for data handling. The secure file transfer process discussed in this whitepaper is based on Accellionôs secure file transfer solution, which is currently deployed in more than 20 countries, supporting the exchange of business information between internal and external users. This solution has been chosen by numerous companies in industries that are regulated by SOX, HIPAA, GLBA and other legislation in order to increase their compliance and security posture.

Security and compliance considerations

Government regulations such as HIPAA, the Food and Drug Administration (FDA) 21 CFR Part 11, GLBA and, most notably, the Sarbanes-Oxley Act, place significant requirements on companies regarding who was sent what information, and when. For example:

- HIPAA requires that companies **prove that only the intended information was shared or exchanged**.
- The FDA requires that **administrative controls are in place** when electronic systems and records are used in place of paper or manual systems.
- GLBA requires that financial services organizations **ensure the security and confidentiality of customer records and information**.
- SOX requires that **business processes are auditable**.
- The Federal Rules of Civil Procedure (FRCP) Rule 37(f) requires that companies can **prove how electronic records are stored, what mechanisms are in place to retrieve them, and when and how they are deleted**.
- The U.S. Department of Defense Electronic Records Management Software Applications Design Criteria Standard (DoD 5015.02-STD) requires that an agency **provide documentation of transfer activities in an electronic format that can be saved as a record**.

"As with many recent initiatives, including HIPAA and the Sarbanes-Oxley Act, internal and external mandates are calling for every process to be documented, auditable, and accountable—including those business processes that incorporate or leverage traditional communications protocols. The result is that, in the immediate future, most companies, regardless of industry, need to consider how they are managing their file transfers."

Research Director
Gartner, Inc.

These criteria are examples and are by no means an exhaustive list of regulations governing the handling of information. You can see, however, that they are merely guidelines that are open to interpretation for how they can or should be implemented.

Even if an organization is not bound by any of these legislative requirements, adhering to the procedures above makes good business sense. Ignoring these procedures puts any organization at too great a risk for a data breach.

Requirements for secure file transfer

In order to adhere to these compliance mandates and protect critical business information, a secure file transfer solution must:

- √ Transmit files only via secure channels and protocols.
- √ Allow for (or enforce) encryption of especially sensitive data.
- √ Secure the information so that it is received only by the intended recipient.
- √ Provide accountability (i.e., an audit trail) for who sent and received the files, and when.

- √ Ensure complete delivery of the information, even in the event of a disruption during transmission (i.e., checkpoint/restart capabilities).
- √ Control the life cycle of files (i.e., automatic deletion).
- √ Validate the identity and authenticate the authority of users of the file transfer process.
- √ Ensure the integrity of the information, so that it can be confirmed that what was sent is what was received.
- √ Ensure that audit trails and files can be archived and easily retrieved as part of a routine records retention policy.

File transfer solutions that meet the above criteria can help ensure compliance with regulatory mandates. At the same time, it is possible to adopt a secure solution that supports business process agility. A solution that meets these requirements doesn't have to be difficult to use.

The Accellion secure file transfer system is an enterprise-class solution that addresses the need for security/compliance

Accellion's secure file transfer system is architected to address the critical functional and technical requirements for enterprise secure file transfer that meets organizational compliance needs. The Accellion system is comprised of a selection of components that in combination create a robust ï yet easy to use ï system for securely sending and receiving large files and folders up to 20 gigabytes in size.

The key components of the system include:

- √ a secure file transfer appliance
- √ a web user interface
- √ an email plug-in for Microsoft Outlook and Lotus Notes
- √ an IT administrator interface
- √ business process automation agents

The total solution helps maintain a posture of compliance to both legislative mandates and corporate policy.

Security/compliance: The Accellion solution secures your critical information assets

The protection of an organization's information assets is a top-of-mind issue for business and IT management. A data breach that reveals private information can be costly and perhaps even devastating to a business and its reputation. That being said, there are ways to improve the ability to secure private email attachments and other file transfers, and help meet the regulatory compliance

requirements under which a business must operate. Here are a few examples based on specific features within the Accellion secure file transfer system.

(Note: The words in **bold** relate directly to specifications of the legislative mandates we've been talking about.)

End to end file security

Files are **encrypted**, uploaded, stored, and downloaded through **secure links** and **recipients are authenticated** ensuring only the intended recipients can access the file. Optionally, files can be scanned for viruses on upload/download.

File management

An Osterman Research survey revealed that a majority of businesses are concerned that they aren't doing enough to secure their private data when it is "in motion" and to meet the compliancy requirements of government regulations. This is especially true for businesses that are under government mandate to manage the control of all data.

Workers can review and **track files sent and their download status**, and can **manage the lifecycle of a file** (for automatic deletion).

Directory services authentication

The Accellion solution **uses LDAP and Microsoft Active Directory for authentication** and to minimize setup efforts.

File transfer auditing and tracking

The Accellion system provides **auditable records detailing when recipients download attachments that can be summarized by individual recipient, file name, time and date**.

Automated download receipt

When a recipient downloads the file, ***a* return receipt is generated to the sender**. The file recipient is unaware of the return receipt and cannot turn it off.

Optional integration with enterprise storage infrastructure

Administrators can set up **rules to centrally manage the lifecycle of files per corporate retention policies**. Multiple copies are identified and removed based on set demand levels or after a period of time and **can be archived to long-term storage over time**.

File security is less complicated when approached holistically as an automatic and integrated part of the IT system and not left up to end users to initiate. That's why the Accellion secure file transfer system includes standard features such as encryption, audit trails, sender and recipient authentication, and secure links, to name a few. And because it's what the government wants/tells you to do, compliance is a non-issue.

Ease of use: The Accellion solution works the way people work

It's important for any IT solution to take in account the way workers prefer to work. If a business process is too cumbersome, is too hard to learn or master, and requires intervention from someone else, the workers will simply find a workaround to the official process. For example, if workers are required to ask an IT administrator to post a file to an SFTP server and then give permission and instructions for others to access that file, the workers are likely to simply send files via email. Workers will do whatever is easiest to get a job done.

Accellion has designed a secure file transfer system that *works the way people prefer to work*:

A familiar easy-to-use email interface

Embracing the email paradigm, Accellion provides a **web interface** as well as an **optional email plug-in** that is very intuitive. The **familiar email-like interface** removes a major obstacle to adopting the new technology.

Workers have control over the file transfer process

Workers require little to **no training** and **no assistance** from the IT department to send files at any time. There is **no need to ask for permission, passwords or help to send, retrieve or manage files**. For remote users, and those organizations not utilizing the email plug-in, the web interface allows authorized users to **send or retrieve files from anywhere, at anytime**.

More importantly, Accellion puts **file transfer control within the users' hands** while minimizing IT involvement in the process. Yet, IT retains the ability to control, safeguard and track critical information assets by setting group and individual policies and assembling the audit trails.

Colleagues outside the company can use the same system

The Accellion file transfer solution allows authorized employees to **invite outside guests to use the solution**, too. Provisioning (setting up) a guest can be handled in mere minutes without intervention from a system administrator, allowing for **true ad hoc file transfer** when the business process calls for it. Or if company policy requires centralized authorization, a system administrator can grant the access. Either way, the Accellion process helps assure that the file transfer system is not misused or hijacked (as so often is the case with FTP servers). For external users, there is **nothing to install or configure** on their PCs.

There is virtually no size limit for files and folders

While email administrators often restrict the size of file attachments to 10 megabytes or less ï which barely allows you to send a PowerPoint presentation these days ï the Accellion secure file transfer solution can **handle 20+ *gigabytes* in file/folder size with a single procedure**. The system can handle large digital files such as architectural drawings, medical images, engineering blueprints, photographs and videos, large databases, and so much more.

Workers know when their files have been received

Once a file or folder is sent and retrieved by the specified recipient, the **sender receives a confirmation** that the action is complete. The receipt also is logged in the system records. This does two things. First, this closes the loop on the process by providing an ñaudit trailòof who received what and when, and second, it relieves the sender of the burden of calling to make sure the file was received.

Examples: How Accellion customers use their secure file transfer systems

The Accellion secure file transfer solution fits into any industry or business market. Where there is a requirement to exchange files promptly and securely, Accellion addresses the need, as with these customers.

Wyckoff Heights Medical Center

Wyckoff Heights Medical Center (WHMC) is a 350-bed teaching hospital located on the border of northern Brooklyn and western Queens boroughs in New York City. To ensure the confidentiality of its patients and meet HIPAA regulations, WHMC needed a secure way to exchange electronic files with affiliates outside of its network.

The Accellion secure file transfer solution allows the hospital to quickly and easily send and receive files using a process that meets the strict security and privacy requirements. WHMC has the ability to authenticate the recipient to ensure there is no unauthorized access to sensitive and confidential data. The hospital automatically manages each file and account lifecycle to protect confidential information from exposure. Audit trails document compliance with the HIPAA mandate. Most importantly, patient care is improved because the medical records can be transferred from one healthcare provider to another without delay.

The IMA Financial Group

The IMA Financial Group specializes in identifying, analyzing, and solving clientsômost challenging risk management problems ï including property, casualty, surety and employee benefits solutions, especially addressing customersôinsurance needs. Through an extensive global network, IMAôs team helps protect and add value to their customersôbusinesses. But IMA is much more than insurance. Their clients benefit from a seamless delivery of products and services that helps to ensure their companyôs ï and their employeesôï continued health and prosperity.

In this business, IMA works with thousands of documents of all types sent to the company by clients. The content of the documents is often of a very sensitive nature, and must be kept confidential and secured at all times and comply with regulations, including HIPAA and Sarbanes-Oxley, even when documents are ñin motionòduring file transfer.

IMA has deployed the Accellion Secure File Transfer System in order to send and receive large files while simultaneously ensuring that the documents are

secure and meet the regulatory requirements faced by both IMA and its many clients.

Conclusion

Whether mandated by legislation or dictated by company policy, every organization has an obligation to ensure the security and integrity of the information it handles. That obligation doesn't stop during the process when information is transferred from one party to another. A secure file transfer solution is no longer a luxury, but rather a necessity. The IT department has a responsibility to select and provide a solution that meets the security and compliance requirements and fits into the regular workflow of business.

The Accellion secure file transfer system is the preferred solution for easily and securely transferring files and folders from person to person. By choosing this solution, your organization can be assured that it is:

- √ controlling access to private information,
- √ maintaining the security and integrity of the information, and
- √ improving your security and compliance

About Accellion

Founded in 1999, Accellion, Inc. is the premier provider of on-demand secure file transfer solutions with an extensive customer base covering industries such as advertising/media production, legal, manufacturing, healthcare, consumer goods, higher education, and more.

Accellion provides an enterprise file transfer solution that is secure, economical and easy to use for both end users and IT management. Unlike email and FTP that can no longer meet the evolving security and business requirements, Accellion enables enterprises to eliminate FTP servers, create Sarbanes-Oxley compliant business processes, improve email infrastructure performance, and reduce IT management footprint requirements.

The Accellion secure file transfer solution allows internal and external users to send and receive files bi-directionally on the same platform without adding administrative overhead or infrastructure burden. Accellion offers an intuitive web interface with end-to-end file security and policy-based file lifecycle management. Accellion also supports plug-in integration with Outlook and Lotus Notes email clients. For multi-site enterprises, Accellion offers clustering for multi-site load balancing, intelligent replication and failover.

Accellion is a privately held company headquartered in Palo Alto, California with offices in North America, Asia and Europe.

www.accellion.com **info@accellion.com**