# CONCORD TECHNOLOGIES COMPLIANCE WHITE PAPER

*An overview of Concord's Cloud Fax Security and Compliance Adherence*

CONCORD
TECHNOLOGIES

## Introduction

In industries where sensitive documents are sent and received, protecting data housed in those files is crucial at every stage, including while in transit. Industries such as healthcare, legal, government, and finance are held to rigorous security and compliance standards to protect sensitive documents and data. However, navigating those standards is complex and can be overwhelming when evaluating potential partners.

For over 25 years, Concord Technologies has been a trusted partner to organizations operating within tightly-regulated industries. Concord's Cloud Fax network supports thousands of businesses and hundreds of thousands of employees who send and receive millions of documents each business day. However, it is not just the technology that sets Concord apart as a partner but also the commitment to serving customers. In this white paper, the reader will gain insight into Concord's holistic approach to compliance and security to address the needs of their customers and those they serve.

## Making the switch to cloud fax

Fax technology remains a valuable tool for many organizations and industries operating within rigorous security and compliance standards due to its status as an easily accessible and universal communication method. However, fax, as it exists today, looks very different than the traditional fax machine. Cloud fax technology has grown and adapted to meet the evolving needs of healthcare, legal, government, and finance, bridging interoperability gaps to provide trusted and reliable communication.

Cloud fax technology maintains the convenience of fax and provides a solution that's much more user-friendly and fosters tighter security and adherence to compliance standards. The combined ease-of-use and improved security of cloud fax have caused organizations within healthcare and other regulated industries to migrate en masse from their outdated on-premises fax servers and other legacy hardware to cloud fax technologies.

Organizations looking to eliminate outdated, difficult-to-manage, and equally difficult-to-secure fax machines and servers find that choosing a cloud fax partner that prioritizes security from the ground up is vital to a successful fax technology displacement project and long-term partnership.

## Concord’s holistic approach to security

Each element of Concord's Cloud Fax service facilitates the security measures required for a range of compliance standards, with particular attention to HIPAA. The design of Concord's policies, procedures, and network architecture focus on compliance-driven organizations' needs. In addition, Concord partners with its customers to support their security objectives and help them meet their obligations under a variety of standards, including HIPAA, PCI, and others. Concord takes a holistic approach to security, believing that security is something to be considered with every business decision and at the forefront of all services offered.

# Concord Cloud Fax Security

Concord is committed to providing data security that meets or exceeds rigorous regulatory and industry standards. It aligns physical, network, and application security in its multi-faceted approach for data protection. Physical security protects the actual brick and mortar component of the business against physical access to systems holding sensitive data; network security safeguards cloud and internal networks from potential cyberattacks or threats; and application security protects against unauthorized access to customer data processed by Concord's services. Together, these three prongs of security work to keep data safe.

## Concord Physical Security

Physical security is in place to restrict entry to buildings where information is stored, accessed, and processed. For cloud fax companies, data breaches can occur through more than compromised network security or hacking attempts; a physical security breach can have equally damaging effects. Concord's facilities utilize security measures that include guards, key cards for entry, and security cameras. Tight physical security is in place to protect Concord's facilities from unwanted—and even unintentional—visitors.

- Secure datacenters are located in Seattle, WA and Chicago, IL
- Secure building access requires photo ID and access card
- Additional access card use is required at Concord suite entrance and exit, which is logged and audited.
- Datacenter access is tightly controlled, only those with a justifiable business need and senior management authorization are granted access to Concord datacenters.
- Third-party access, for parties such a electricians, plumbers, HVAC and equipment vendors, is strictly controlled, logged and audited. Work is scheduled in advance and third parties are escorted by Concord staff while in the datacenter.
- CCTV video surveillance of facilities is stored for 90 days.

## Concord Network Security

Network security is in place to help prevent hackers from gaining access to personal information and to protect data from the various types of network breach that might occur, whether intentionally or by mistake. Concord's Fax network is designed to protect the sensitive data being transmitted via its Cloud Fax services every day.

- Next generation firewalls are deployed and kept up-to-date.
- Logical network segmentation – Demilitarized Zone (DMZ,) Management Zone (MZ,), Internal Zone (IZ,), Development Zone (DEV).
- Intrusion detection and logging.
- Frequent security and vulnerability scans are performed.
- Regular penetration tests are performed on internal and Cloud Fax networks.
- Ongoing process of updating and patching with Critical and High items to be addressed within 30 days.
- Systematic auditing and review of logged data including, but not limited to:
  - Invalid access attempts
  - Access attempts to the database
  - All successful and unsuccessful logins
- Formal alerting and response process are used in the event the Intrusion Detection System detects a suspicious event or exceeds normal thresholds for our environment.

## Concord Application Security

Application security is in place to secure data within Concord production systems. When the privacy of personal information and compliance concerns are involved, thwarting unauthorized access is essential. Whether by intentional hacking or by accidental access of a system, if Protected Health Information (PHI) or other sensitive information is viewed by someone without permission to do so, compliance issues may arise. Concord takes care to make sure that information in the production system is properly secured at all times.

- All data provided for processing by and through the services and fax content is encrypted both in transit and is also encrypted while at rest.
- Utilization of Secure Sockets Layer/Transport Layer Security (SSL/TLS) or email communications (opportunistic or enforced).
- Access to databases is strictly controlled with Role-Based Access Control (RBAC) principles.
- Multi-factor authentication requirement for privileged system access.
- Customer-configurable minimum password standards for length, complexity, and characters.
- Multiple options are available to fax customers to specify where their data will be stored.
- Multiple options are available for customer to specify the duration of fax document storage including zero image retention.
- Security engineering principles embedded into the System/Software Development Lifecycle (SDLC) to achieve the goal of “secure by design” when designing, building, and updating systems.

# SOC 2 Audit Information

Developed by the American Institute of CPAs (AICPA), SOC 2 (Systems and Organizations Controls 2) is a voluntary compliance standard, which is based on the Trust Services Criteria: security, availability, processing integrity, confidentiality, privacy. SOC audits can only be performed by independent CPAs (Certified Public Accountants) or accounting firms.

The purpose of SOC 2 is to assist a service organization report on its internal controls for protecting customer data in relation to the trust services categories. A SOC 2 audit typically covers a combination of the trust services categories, as not all categories are applicable to all service organizations due to the nature of the operations and regulatory requirements. The audit is a test for the suitability and effectiveness of the service organization's controls. The audit report demonstrates that controls are in place to secure the service provided.

There are two types of SOC 2 audits. A Type I audit tests the design of a service organization's controls but not the operating effectiveness. A Type II audit covers a certain period (usually 12 months), testing the design and operational effectiveness of key internal controls over that time. A SOC 2 report is an independent attestation demonstrating that a service provider has the appropriate information, security policies, and procedures in place to protect customer data. It provides an evaluation of controls adequacy and operational effectiveness over time. It also identifies any deficiencies with recommended changes.

Every year, Concord undergoes a SOC 2 Type II audit, testing the trust services categories applicable to its operations and regulatory requirements. The latest SOC 2 Type II audit report is available for review after executing a signed non-disclosure agreement.

# PCI Compliance Information

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements that governs the processing of credit card data. It was launched on September 7, 2006, to improve security throughout the transaction process. An independent body created by Visa, MasterCard, American Express, Discover, and JCB, the PCI Security Standards Council (PCI SSC) administers and manages the PCI DSS. The payment brands and acquirers themselves are responsible for enforcing compliance rather than the PCI SSC.

PCI DSS compliance is essential to an enterprise cloud fax provider because customers may use its service to transmit or store credit card information. PCI DSS provides a baseline of security requirements intended to reduce the risk of a data breach, and its controls help in the continual identification of threats and vulnerabilities. In an organization's being PCI-compliant, it means that there is constant maintenance and assessment of security posture, and that the technical and operational standards set out by the PCI SSC are implemented and maintained.

Concord is a PCI-compliant Service Provider. Concord's PCI Professional (PCIP)™ certified internal auditor oversees the continuous monitoring of controls and the PCI program. Concord completes an Annual Self-Assessment Questionnaire (SAQ) D and submits to quarterly vulnerability scans as part of the PCI DSS process. An Attestation of Compliance (AOC) is available for our customers' review. The following is a summary of the Concord Cloud Fax Platform's security highlights with PCI DSS goals:

| PCI DSS Goal | Compliance on Cloud Fax Platform |
|---|---|
| Build and Maintain Secure Networkand Systems | ▪ Standardized firewall, router, and system configurations<br>▪ All vendors' supplied password removed, default accounts disabled where applicable |
| Protect Cardholder Data | ▪ Data encrypted in transit and at rest<br>▪ Encryption key management process and procedure fully documented |
| Maintain a Vulnerability Management Program | ▪ Anti-virus installed in systems<br>▪ Security patches deployed on a risk-based vulnerability management program<br>▪ Change Management enforced for changes to system<br>▪ Secure coding guidelines in place |

| | |
|---|---|
| Implement Strong Access Control Measures | ▪ Least privileged methodology used with default deny-all for access control<br>▪ VPN/MFA required for production network access<br>▪ Physical access for non-employee requires pre-approval and employee escort |
| Regularly Monitor and Test Networks | ▪ Intrusion detection system in place<br>▪ 12 months' retention of system audit trail entries (logs)<br>▪ Other Controls:<br>o Daily log reviews<br>o Quarterly wireless scan<br>o Quarterly vulnerability network scan<br>o Annual penetration test |
| Maintain an Information Security Policy | ▪ Security policies reviewed once per annum<br>▪ User acceptance policy reviewed and accepted by all personnel once per annum<br>▪ Background checks carried out before hiring<br>▪ Continuous security training mandatory for all personnel<br>▪ Incident response plan tested once per annum<br>▪ Customer-Concord Shared-responsibility matrix available for current customers |

# HIPAA Compliance Information

Concord's Cloud Fax services help support our customers' compliance with HIPAA.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a law enacted by Congress to improve efficiency in the healthcare industry, to improve the portability of health insurance, to protect the privacy of patients and health plan members, and to ensure that health information is kept secure. Together with the implementing regulations issued by the Department of Health and Human Services (HHS), HIPAA created national privacy and security standards through the HIPAA Privacy Rule, the HIPAA Security Rule, and the HIPAA Breach Notification Rule. The intent is to protect sensitive patient health information, Protected Health Information (PHI), from being disclosed without the patient's consent or knowledge. The HIPAA regulations are found at 45 C.F.R. Parts 160, 162, 164.

HIPAA imposes rigorous obligations on Covered Entities in the healthcare industry, namely insurance plans, healthcare clearinghouses, and healthcare providers, in the handling of, among other things, electronically transmitted PHI. Under HIPAA, Business Associates–those who provide certain services to Covered Entities and other Business Associates involving the access, use or disclosure of PHI–are required to comply with the terms of their Business Associate Agreements (BAAs) with those they are providing the services to. BAA terms generally require the Business Associate to comply with the Covered Entity's obligations under HIPAA that are applicable to the services provided. Cloud fax providers delivering services to a Covered Entity may be acting as a Business Associate.

The HIPAA Security Rule requires Covered Entities to have Administrative, Physical, and Technical Safeguards that protect PHI from unauthorized use or disclosure. The HIPAA Privacy Rule establishes how PHI may be used and disclosed, and the HIPAA Breach Notification Rule requires that appropriate processes are in place to notify patients if a security incident or breach compromises the privacy and security of their PHI.

Sharing PHI between Covered Entities via fax is a common practice in the healthcare industry. Covered Entities relying on cloud fax providers to transmit their PHI want to know that they have a trusted and reliable partner when it comes to meeting their HIPAA compliance obligations. They want to know that the security and privacy of the PHI they transmit will be protected by a provider who knows and meets the standards set by HIPAA.

## Concord's Secure Services Enable Customer Compliance

### The Security Rule

Concord's Cloud Fax services are designed to address HIPAA's Administrative, Physical, and Technical Safeguards required under the Security Rule, enhancing its already rigorous security protocols by exceeding HIPAA's regulatory requirements. By implementing the following policies and procedures, Concord enables its customers' compliance with the statutory obligations they have under HIPAA.

| Requirement | C.F.R. Citation | Concord's Policies & Procedures |
|---|---|---|
| Administrative Safeguards | 45 C.F.R. §164.308 | Concord's comprehensive policies and procedures cover the management, implementation, and maintenance of the controls used to safeguard PHI, and a disaster recovery/business continuity plan in case of emergency, including, but not limited to:<br>• Business Associate Agreements with its customer<br>• Documented access control policy<br>• Documented security management process<br>• Documented risk assessment and risk management process<br>• Documented and tested incident response plan<br>• Documented and tested disaster recovery plan<br>• Appointed security and compliance officer<br>• Security training and awareness for Concord employees |

| | | |
|---|---|---|
| Physical Safeguards | 45 C.F.R. §164.310 | Concord's policies and procedures to restrict access to facilities and system include, but are not limited to:<br>• Strictly controlled and audited access to all data center facilities and office locations |
| Technical Safeguards | 45 C.F.R. §164.312 | Concord's policies and procedures guard against unauthorized access with least privileged access control methodology, multifactor authentication, data encryption and continuous system monitoring to:<br>• Strictly controled and audited user access to network systems<br>• Strictly controled event auditing policies<br>• Enforce transmission security |
| Organizational Requirements | 45 C.F.R. §164.314 | Concord Business Associate Agreements are available for customers. |
| Documentation and Retention Requirements | 45 C.F.R. §164.316 | Concord's policies and procedures address its obligations regarding the implementation and documentation of policies and procedures, including, but not limited to:<br>• Documented policies and procedures with structured review process<br>• All required documentation with minimum retention period of six years |

## The Privacy Rule

The Privacy Rule sets out how PHI may be used or disclosed. Acting as a Business Associate, Concord may only use or disclose PHI as permitted or required by its BAA or as required by law. Concord has no relationship with, independent knowledge of, or information about any individuals whose PHI is being transmitted, and all access to, use of, and disclosure of PHI is at the end-user's direction and control. Because of this, compliance with the Privacy Rule is primarily the customer's responsibility. Concord does have policies and procedures that restrict access to PHI to authorized individuals for the purpose of providing the services.

| Requirement | C.F.R. Citation | Concord's Policies & Procedures |
|---|---|---|
| Rules Regarding Use and Disclosure of PHI | 45 C.F.R. §164.502-514 | Use and disclosure of PHI by Concord complies with rules for Business Associates. |
| Notices of Privacy Practices | 45 C.F.R. §164.520 | Responsibility of the Covered Entity. |
| Right to Request Restrictions on PHI | 45 C.F.R. §164.522 | Responsibility of the Covered Entity. |
| Right to Access and Amend PHI | 45 C.F.R. §164.524-26 | Not Applicable – Concord does not maintain Designated Record Sets. |
| Right to Accounting of Disclosures | 45 C.F.R. §164.528 | Concord's policies and procedures address its obligations to document and store this information as applicable under the rule. |

## The Breach Notification Rule

This narrow rule addresses notification obligations in the event of a security breach of unsecured protected health information. Concord has a comprehensive policy for investigating potential security breaches and notification of customers whose data may have been disclosed.

| Requirement | C.F.R. Citation | Concord's Policies & Procedures |
|---|---|---|
| Notification by Business Associate | 45 C.F.R. §164.410 | Concord's policies and procedures provide for the investigation of breaches and required notification of customers. |
| Notification to Individuals, the Media and HHS | 45 C.F.R. §164.410 | Responsibility of the Covered Entity. |

## Conclusion

For organizations seeking a cloud fax provider that will afford them not merely a service vendor, but a partner in security and compliance, Concord is a clear industry leader. Concord has been meeting and exceeding the needs of customers for over two decades and is committed to being their preferred partner well into the future. Concord's commitment to making the exchange of information simpler and more secure is present throughout every service offered, from their Cloud Fax service to data extraction and document handling. To learn more about any of Concord's product offerings, please contact us at sales@concord.net or schedule a demo online by visiting https://concord.net/contact-us/request-a-demo/.