

# WHITEPAPER

XMEDIUSFAX<sup>®</sup> CLOUD  
FOR HEALTHCARE AND  
HIPAA COMPLIANCE



## INTRODUCTION

The healthcare industry is driven by many specialized documents. Each day, volumes of critical information are sent to and from doctors, patients, pharmacies, laboratories, healthcare providers and insurance companies. These documents are often urgent and confidential. Secure, timely and reliable delivery is essential for patient-focused and cost-conscious healthcare organizations.

## WHAT IS HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) has changed the way healthcare organizations send, receive and store confidential information. HIPAA establishes regulations for the use and disclosure of an individual's Protected Health Information (PHI).

To achieve HIPAA compliance, healthcare providers (known as "covered entities") must improve the efficiency of document transmission, while ensuring the security and confidentiality of information. Under the security standards of HIPAA, covered entities must implement administrative, physical and technical safeguards to protect the confidentiality, integrity and availability of electronic health information.

The healthcare industry works with an array of healthcare solution providers and outsourcers (known as "business associates"). HIPAA's business associates that serve a healthcare provider or institution are subject to audits by the Office for Civil Rights (OCR) within the Department of Health and Human Services and can be held accountable for any data breach and penalized for noncompliance.

With these regulations in mind, a HIPAA business associate must demonstrate the different procedures and measures put in place to help its clients (covered entities) reach HIPAA compliance.



## XMEDIUSFAX<sup>®</sup> CLOUD AND HIPAA COMPLIANCE

With over 10 years of experience within the healthcare industry, XMediusFAX<sup>®</sup> has helped numerous medical clinics rationalize and secure their fax services, in order to meet HIPAA compliance. XMediusFAX<sup>®</sup> digitizes processes and stores fax documents. While eliminating manual processes and paperwork, XMediusFAX<sup>®</sup> provides security, accountability and traceability.

Sagemcom can be defined as a "business associate" (BA), performing a service for a covered entity, which is why we oblige our HIPAA regulated customers to enter into a BA agreement with us. This demonstrates our commitment to compliance and ensures peace of mind for our customers that use the XMediusFAX<sup>®</sup> Cloud service.

XMediusFAX<sup>®</sup> Cloud is committed to helping covered entities become compliant with HIPAA regulations, through the core set of safeguards: Administrative, Physical and Technical.

## ADMINISTRATIVE SAFEGUARDS

HIPAA policies describe “Administrative” safeguards as administrative actions, policies and procedures used to manage the selection, development, implementation, and maintenance of security measures to protect Electronic Patient Health Information (ePHI) and to manage the conduct of the organization’s workforce in relation to the protection of that information.

Sagemcom implements all the administrative safeguards on its company policies, employees and finally its client base:

### 1. Business Associate Contracts

A business associate contract is required by Sagemcom for any organization that requires HIPAA compliance.

### 2. Assigned Security Responsibility

Sagemcom has a security officer in place to help enforce and implement HIPAA compliance across its network and infrastructure.

### 3. Workforce Security

Sagemcom allows only a limited number of highly trained workforce members to access secure and confidential data.

### 4. Information Access Management

Sagemcom will only allow authorized members to access secure data under strict and limited circumstances exclusively on behalf of the client.

### 5. Security Awareness and Training

All members of Sagemcom staff have Level I HIPAA training.

### 6. Security Incident Procedures

Sagemcom has a well-established detection, reporting and resolving procedure for any security breaches.

### 7. Contingency

Sagemcom offers organizations multiple ways to ensure their data is not lost by implementing a collective contingency plan.



## PHYSICAL SAFEGUARDS

HIPAA policies describe “Physical” safeguards as physical measures, policies and procedures to protect the organization’s electronic information systems, related buildings and equipment from natural and environmental hazards and unauthorized intrusion.

Sagemcom works with two Tier-1 data centers that have been designed for their top level physical security in an extremely controlled environment with limited physical access to the servers where secure data is housed and transmitted.

To safeguard all facilities, systems, and equipment used to store electronic protected health information (ePHI) against unauthorized physical access, tampering, or theft: Sagemcom implements the following:

### 1. Contingency Operations

Sagemcom’s data center provider allows only authorized physical facility access during emergencies to support restoration of data under the Disaster Recovery Plan.

### 2. Access Control and Validation

Sagemcom’s data center provider controls and validates workforce member access to facilities based on their role or function.

### 3. Physical Access Records

Sagemcom logs physical access to any facility containing ePHI-based systems. Examples of facilities requiring physical access records are computer and system rooms.

### 4. Maintenance Records

Sagemcom data center provider ensures document maintenance, repairs and modifications to the physical security components of the facility including locks, doors, and other physical access control hardware.

### 5. Workforce Access Controls

Sagemcom’s data center provider also validates workforce member access to all facilities used to house ePHI based systems.

### 6. Visitor Access Controls

Sagemcom’s data center provider controls, validates, and documents visitor access to any facility used to house ePHI based systems. Visitors include vendors, repair personnel, and other non-workforce members.

Sagemcom’s XMediusFAX<sup>®</sup> Cloud enforces service access to its portal by implementing and assisting its users with best practices on HIPAA compliant procedures for workstation<sup>1</sup> access, use and control such as:

- Strict password policies
- Workstation privacy and protection policies
- Information storage policies
- Workforce access policies

<sup>1</sup> It is important to note that the term “workstation” means any electronic computing device, such as a desktop computer, laptop, PDA, etc.

## TECHNICAL SAFEGUARDS

Implementing “Technical” safeguard policies are the third and final tier in ensuring that an organization is 100% secure and protected when faxing communications containing confidential information such as PHI, financial and legal documents transmitted electronically over open networks.

HIPAA policies describe technical safeguards as a set of technology and policy procedures that protect ePHI and control access to it.

Although there are no rules or specific requirements for the types of technologies to be implemented for compliance, Sagemcom as a covered entity has taken the utmost precautions to determine which security measures and specific technologies are reasonable and appropriate for the implementation of its XMediusFAX<sup>®</sup> Cloud solution for all its clients.

Many of Sagemcom’s clients may not have the manpower and resources to audit and implement a secure and HIPAA compliant environment. As a partner and HIPAA Business Associate, Sagemcom helps its customers reach compliance by implementing collectively the following five technical safeguard standards:

1. [Access Controls](#)
2. [Audit Controls](#)
3. [Integrity](#)
4. [Person or Entity Authentication](#)
5. [Transmission Security](#)

### Access Controls:

HIPAA policies describe Access Controls as the management of users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access Controls should enable authorized users to access the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules.

XMediusFAX<sup>®</sup> Cloud helps organizations meet their HIPAA requirements by requiring each workforce member to have a unique user identifier; XMediusFAX<sup>®</sup> Cloud controls user access to a single account. No duplicate emails may exist on the Cloud service. XMediusFAX<sup>®</sup> Cloud also assigns both administrator and user roles within the solution. Only administrators may have full control and access to the entire solution and may invite and remove user access as they see fit.

### Audit Controls:

HIPAA describes Audit Controls as the following: “Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information”.

XMediusFAX<sup>®</sup> Cloud activity is available for full auditing by all our clients for their specific information via the fax retention policy or if fax retention is not selected then Meta data of all fax transactions is logged to verify activity.

### Integrity:

HIPAA describes Integrity as “the property that data or information have not been altered or destroyed in an unauthorized manner”.

Sagemcom works with its clients to help them implement policies and procedures to protect electronic protected health information from improper alteration or destruction, via such methods as secure FTP routing or routing to document management solutions such as SharePoint for archiving and access control within the client network.



### Person or Entity Authentication:

HIPAA describes Person or Entity Authentication as the following: "Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed".

XMediusFAX<sup>®</sup> Cloud has secure service login and enables only service administrators to assign and invite new users to the cloud faxing solution.

### Transmission Security:

The final standard listed in the technical safeguard's section is Transmission Security. This HIPAA policy is described as the following: "Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network". XMediusFAX<sup>®</sup> Cloud utilizes major security protocols to ensure maximum protection:

- HTTPS for all Internet connectivity.
- FTPS, SCP and SFTP to route fax image files to customer folder destinations.
- SSLIOP is used by SendFAX (Windows Thick Client) to submit faxes.
- TLS encryption is available for e-mail communication.

XMediusFAX<sup>®</sup> Cloud also uses Access Tokens (randomly generated keys) to provide applications access to system services to manage users, query the user directory and send and manage faxes. Tokens are required for AD Synchronization and submitting faxes via Ricoh ESA, Xerox EIP and Web Services.

All data is encrypted at the hard drive controller. All fax images and fax transmission metadata are fully encrypted. Sagemcom's third-party payment processor that processes the billing transactions and retains information on XMediusFAX<sup>®</sup> Cloud customers is PCI Level1 compliant. Credit card information is never accessed or processed by XMediusFAX<sup>®</sup> Cloud.

## SUMMARY

With XMediusFAX<sup>®</sup> Cloud, there are no obstacles to processing confidential and sensitive documentation through our cloud faxing solution. Not only has the solution been designed for the most secure policies but Sagemcom also works with the clients to help them implement HIPAA policies into their workplace. Though there are no strict guidelines on how any one organization should implement compliance; as an official business associate Sagemcom is constantly evaluating and improving the methods in which they instill the Administrative, Physical and Technical safeguards to ensure maximum protection for their clients.

All rights reserved. The information and specifications included are subject to change without prior notice. Sagemcom Documents tries to ensure that all information in this document is correct, but does not accept liability for error or omission. Non contractual document. XMediusFAX is a registered trademark of Sagemcom Documents. Simplified joint stock company - Capital 8.479.978 Euros - 509 448 841 RCS Nanterre.

Distributor/Reseller:

**5252 de Maisonneuve Blvd. West, suite 400  
Montreal, Quebec  
H4A 3S5 Canada**

**Telephone : +1 514-787-2100  
Fax : +1 514-787-2111  
Toll-free (U.S./Canada) : 1-888-766-1668  
[xmediusfax.sagemcom.com](http://xmediusfax.sagemcom.com)**

# SAGEMCOM