FOXIT ESIGN HIPAA COMPLIANCE OVERVIEW

WHITE PAPER

TABLE OF CONTENTS

INTRODUCTION

The move to electronic data is in full effect. More efficient communication of information between health providers and the demand for providing a better patient experience have led to a wider adoption of digital processes for handling patient records. Yet, with higher efficiency that digital processes bring, it is accompanied by intense scrutiny. The leakage and selling of sensitive information like a patient's health information is attractive to hackers, and one with devastating consequences. As such, patient data management is held accountable to an airtight regulation known as HIPAA. Health care providers and businesses in the same industry must find ways to provide efficient care patients expect without mishandling the health data entrusted to them.

This document provides an overview of the HIPAA regulation and how it impacts your organization. It also answers some of the most common questions related to the usage of electronic documents in the healthcare industry and how Foxit eSign addresses these challenges.

WHAT IS HIPAA AND THE PRIVACY RULE?

The Health Insurance Portability and Accountability Act (HIPAA) is a sweeping US healthcare regulation that was enacted in 1996. Originally signed into law to improve the portability and accountability of health insurance coverage, HIPAA has since evolved to protect the confidentiality of patients. Title II of HIPAA contains the Standards for Privacy of Individually Identifiable Health Information, or simply the Privacy Rule, which outlines a set of standards for the protection of health information. The Privacy Rules governs the usage and disclosure of protected health information, or PHI, by covered entities, which include health care providers, health plans, and health care clearinghouses.

The protection of PHI has since been extended under two acts. Under the HITECH Act of 2009, protection extended to include the transmission of electronic records and data. The HIPAA Omnibus Rule of 2013 extended protection requirements to Businesses Associates (BAs). A BA is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of a covered entity. Under these rules, HIPAA-covered entities who seek to work with vendors or contractors are required to enter into a Business Associate Agreement (BAA) such that their products and/or services ensure the protection and security of PHI in compliance with HIPAA.

WHAT IS CONSIDERED PHI UNDER HIPAA?

HIPAA defines protected health information, or PHI as any health information in the custody of a covered entity which can be used to identify a patient. Essentially, all information related to the patient is considered PHI. PHI is information that can be found in things such as medical records, health histories, lab work results and medical insurance bills. 18 individual identifiers that are categorized as PHI under HIPAA include, but are not limited, to the following:

Names	Contact numbers	Medical record numbers
Social security numbers	Addresses (Physical and Email)	Birth dates
Gender	Medical history	Immunization history

WHO IS A COVERED ENTITY UNDER THE PRIVACY RULE?

Covered entities under the HIPAA include, but are not limited, to the following:

Health Care Providers	Health Plans	Health Care Clearinghouses
• Doctors • Health Clinics • Dentists • Psychologists • Pharmacies • Optometrists • Chiropractors • Medical specialists • Nursing Homes	• Health insurance companies • HMOs • Company health plans • Medicare • Medicaid • COBRA	Any public or private entity that processes or facilitates the processing of health information into a standard format, or vice versa • Billing services • Repricing companies • Community health information systems • Community health management systems

The Privacy Rule also requires that covered entities obtain satisfactory assurances from Business Associates that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.

BAs include, but are not limited to:

- Law office or accounting firms
- Software vendors
- Medical device makers
- Billing companies
- Web hosts

If your organization is a covered entity under HIPAA, then you must ensure that all PHI in your custody, as well as those shared with your BAs for business purposes, are completely protected to stay compliant with the regulation. It's important to note that

before entering an agreement with BAs, it is the responsibility of the covered entity to ensure that it has an adequate compliance program in place and to fully verify the BA's ability to meet HIPAA's requirements for PHI protection.

Foxit eSign is an electronic data transaction solutions provider and may transmit and hold encrypted PHI in its servers, qualifying it as a BA. Foxit eSign offers BAAs with covered entities under Pro and Enterprise plans.

DOES HIPAA APPLY TO NON-US ORGANIZATIONS?

No, HIPAA is applicable only to healthcare organizations within the US. Anyone under a US healthcare system is protected by the regulation, including those who are not US citizens. Conversely, US citizens under a healthcare organization outside of the US are not covered by HIPAA.

WHAT ARE SOME COMMON HIPAA VIOLATIONS?

HIPAA violations are steep, leading to fines of up to $50,000 per infraction and a maximum annual penalty of up to $1.5 million per infraction. Even more severe, class action lawsuits from affected parties may cripple covered entities. Therefore, it is imperative for covered entities to ensure HIPAA compliance in their practice. With most information transmitted primarily through electronic means, some of the most common HIPAA violations arise from improper disclosure or exposure of data. Common examples include:

- Unencrypted data – Electronic files containing unencrypted PHI may lead to a data breach.
- Data breach – Weak protection policies or security loopholes are prone to hacks and can lead to illegal exposure of patient data.
- Unauthorized access – It is essential that only those required to access patient data should be able to do so. Anyone outside of this requirement who accesses the PHI is in violation of the rule.
- Disposal of PHI – Even removing electronic PHI without the appropriate methods could leave data vulnerable to hackers.

Foxit eSign is audited by a HIPAA compliancy group on an annual basis to allow it to work with covered entities. All electronic PHI are securely encrypted and transmitted from origination directly to our secure servers. All data is completely secured at-rest and in-motion.

HOW DOES FOXIT ESIGN COMPLY WITH HIPAA?

Foxit eSign is certified HIPAA compliant and to help ensure that the handling of your patient's private and sensitive documentation is always within regulation. To maintain PHI, Foxit eSign provides secure fields to mask this information. We use encryption and tokenization to prevent PHI data leaks. All data is encrypted at rest and in motion. Each Foxit eSign Signature transaction contains a fully traceable, tamper-proof audit trail and is given a Certificate of Completion.

Documents stored in our SOC2-audited data centers are encrypted with the AES 256 standard at the application level for customer documents to ensure full confidentiality.

Foxit eSign also complies with HIPAA regulations through the following:

- Legally binding electronic signatures (in accordance with UETA and ESIGN) that will hold up in court
- Strict adherence to HIPAA electronic safety and security standards
- Detailed documentation standards that include source and identity verification, encryption keys, hash algorithms to lock documents, and other signature technology that supports compliance
- Secured access and transmission of the document
- Thorough auditing that tracks each document's movement and signing
- Detailed logs to provide the detailed activity history of each interaction including the location of the parties accessing the documents before and after signing the document

ABOUT FOXIT ESIGN

Foxit eSign is a legally binding electronic signature solution that is used to prepare, send, sign, and manage important digital documents. Simply upload your document, create your template, assign recipients, and send for signing. API workflows can also be easily established for both direct signature and sender-based eSignatures. Foxit eSign automates workflows, providing a seamless process to allow the user to send, sign, track, and manage signature processes using a browser. Following completion, you have a tamper-proof and legally signed document that can be used for practically any function. Additionally, eSigning is further simplified by allowing senders and signers to engage from anywhere in the world that an internet connection is available and on practically any device.

Foxit
39355 California Street, Suite 302
Fremont, CA 94538, USA

Sales: 1-866-680-3668
Support: 1-866-693-6948
Or 1-866-MYFOXIT

Support Center
www.foxit.com