

# OpenText Compliance Brief - HIPAA Privacy and Security Rules

## Overview of HIPAA Privacy and Security Rule (Physical Safeguards)

The **Health Insurance Portability and Accountability Act** (HIPAA) is US federal legislation enacted in 1996.

Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, known as the Administrative Simplification (AS) provisions, are meant to improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange in the U.S. healthcare system. The AS provisions also address the security and privacy of health data.

Per the requirements of Title II, there are five rules regarding Administrative Simplification: the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule.

The **Privacy Rule** standards address the use and disclosure of individuals' "protected health information" (PHI) by organizations subject to the Rule or "covered entities," as well as standards for individuals' privacy rights to understand and control how their health information is used.

**PHI** is any information which concerns health status, provision of healthcare, or payment for healthcare that can be linked to an individual.

A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality healthcare and to protect the public's health and wellbeing.

The **Security Rule** requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The Security Rule defines **physical safeguards** as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

Failure to comply with HIPAA can result in civil and criminal penalties ranging from \$100 per violation to \$1.5 million annually.

## INDUSTRY

---

US Healthcare

## WHO IS SUBJECT

Healthcare clearinghouses, employer sponsored health plans, health insurers, medical service providers and any healthcare provider who transmits health information in any form

## OPENTEXT SOLUTIONS

---

### OPENTEXT™ RIGHTFAX OPENTEXT™ FAX2MAIL

OpenText™ RightFax and OpenText™ Fax2Mail are market-leading electronic fax solutions with a long-standing history of being the fax solutions of choice for a variety of healthcare information systems (HIS).

These systems allow healthcare professionals to share PHI—both electronic and paper-based records. For existing paper-based records yet to be digitized, RightFax and Fax2Mail support faxing from Multi-Function Printers (MFPs). For electronic records, many organizations choose to setup faxing directly from their EMR or EHR—eliminating the need to print records while keeping a complete audit trail of sent information.

#### Improve security

- Extend existing platforms and applications with RightFax or Fax2Mail to eliminate error-prone, time-consuming and inefficient manual processes
- Automate delivery, receipt, and tracking of sent and received patient information
- Centralize communications hub for protected health information
- Enable audit trail of sent and received faxes

#### Improve HIPAA compliance

- Helps to maintain compliance with HIPAA regulations as well as other protected information requirements
- Electronic delivery of inbound faxes ensure content remains private and does not sit in open public areas with unauthorized access
- Increase confidence that sensitive health information reaches its intended recipient with notifications and options for encrypted and certified delivery

[www.opentext.com](http://www.opentext.com)