LayerCompliance™

Top 3 Best HIPAA Practices

FOR PHOTOCOPIERS, PRINTERS, AND FAX MACHINES

CAEK™

INTRODUCTION

Healthcare providers are more aware of data breach risks from their photocopier, printer, and fax machine after a covered entity was find over $1.2 million dollars in 2013 for returning leased copiers that contained protected health information on the hard drives. Here are the three top best practices to consider when creating your HIPAA policy and procedure for photocopiers, printers, and fax machines.

#1. Locate office machines in well-supervised areas and away from plain view

Any document that is printed, faxed, copied, or scanned on your office machines likely includes protected health information. Use good judgement to decide where these machines are placed in your office. Is someone always close by so that it is difficult for unauthorized person(s) to view or access the printed information? Review the location of equipment with your staff and their responsibility to monitor access to your office machines.

#2. Document your policy and procedure for protecting data stored on office machine hard drives

Almost every modern photocopier, printer, and fax machine has a hard drive that stores document images that may contain protected health information. Consider your options for protecting the data stored on the hard drive such a data removal techniques. Your office equipment may come with the ability to perform a data wipe of the drive that meets federal standards for removal. Document your policy and procedure to protect the information stored on the hard drive before the machine is removed for offsite repair, replaced, or returned to a leasing company.

#3. Review your policy with any third party who owns or maintains your equipment

Review your policy and procedure for protecting any health information that may be stored on a photocopier, printer, or fax machine hard drive with the company that owns or maintains your equipment. When a machine needs to be repaired, returned, or replaced, make sure that you document the procedure performed to protect the data, such as removal of the data from the hard drive or destruction of the hard drive.

DO YOU USE TEMPLATE POLICIES AND PROCEDURES?

The Office for Civil Rights (OCR) has fined providers for using sample policies and procedures that are not followed. We provide custom policies and procedures and the ability to document that your staff is complying with your policies. Providing the tools and expert help your staff needs is critical to implementing a successful HIPAA security program in your practice. Let LayerCompliance™ help you get in and stay in compliance. Contact us today to get started (800) 334-6071.

LAYERCOMPLIANCE™– A COMPREHENSIVE PROGRAM

CONSULT-LEVEL SERVICE. COST EFFECTIVE PRICE.

Risk Analysis

A full Risk Analysis that assesses systems and provides both HIPAA Security compliance and threat analysis.

Policies & Procedures

Custom HIPAA Security policies based on your individual organization—not generic templates.

Implementation

You can document HIPAA Security compliance activities, including the implementation of policies and security measures.

Risk Management

A once-a-year audit or assessment isn't enough. Breaches can happen every day and you need to stay in compliance all year round.

With LayerCompliance™, organizations can get the expert help and tools they need to get in and stay in compliance.

Live Support

Our team is ready to assist with HIPAA Security questions, incidents and potential breaches

HIPAA Security Training

We provide HIPAA Security awareness & security policy staff training

LAYERCOMPLIANCE™

800.334.6071