Health IT Adoption Toolbox

- Meaningful Use
- Quality Improvement
- Financing
- Staffing and Expertise
- Technology Assessment
- Opportunities for Collaboration
- System Implementation
- Organization Change Management
- Open Source and Public Domain Software
- Evaluating, Optimizing, and Sustaining
- Personal Health Records
- Privacy and Security
- Electronic Prescribing

# What are the privacy and security risks of electronic v. paper health records?

Share

Most privacy and security risks apply to both paper and electronic records. However, the way that these are exploited and can be mitigated is different. Having a good understanding of risks is important to ensure that an organization makes informed choices regarding the privacy and security policies and procedures that they apply. In the sections below, we discuss the risks that are common for both paper and electronic records. We also discuss risks that are different based on the patient record format.

## THREE RISKS COMMON TO BOTH PAPER AND ELECTRONIC RECORDS

These include: 1) the risk of inappropriate access, 2) the risk of record tempering, and 3) the risk of record loss due to natural catastrophes.

### 1. The Risk of Inappropriate Access

Regardless of format, patient records are subject to the risk of inappropriate access.

About

Health Information Technology Toolboxes help health centers, safety net providers, and ambulatory care providers with electronic and online resources and technical assistance to improve patient care. More>

More Information

Get Updates

Contact Us

### Paper Records

For paper records, the risk materializes in the form of gaining access to record storage areas; finding records left on counters, exam rooms or copy machines; receiving misdirected fax copies; and other similar events. Inappropriate access can be accidental or intentional. Since access to paper records implies physical access, securing against inappropriate access is accomplished by segregating records into separate locked storage areas; restricting physical access to storage areas; recording sign in and sign out procedures; and maintaining records handling training and other similar procedures.

### Electronic Records

With electronic records, inappropriate access manifests itself in one of two ways: 1) an unauthorized user gains access to the EHR data; or 2) an authorized user violates the appropriate use conditions. For example, if office staff access the records of a friend or colleague that visited the practice. Electronic records can be subject to 'serendipitous' access in situations such as when a user account is left open or a passerby is able to view data on the screen or manipulate the EHR features. Electronic records can also be subject to breaches of network security that may allow a hacker to gain access to user credentials and thereby to bypass the access control protections.

## 2. The Risk of Record Tampering

Medical records can be altered in a number of ways, including back dating, fraudulent entries, erasures, or other modifications.

### Paper Records

Anyone who has access to the paper record can remove pages, add entries, erase or otherwise tamper with authentic entries.

### Electronic Records

The ability to make changes to an electronic record depends upon the rights assigned to a user. Users with data modification privileges can generally add, delete, or modify data or entire records. Data can also be tampered with by directly accessing the files stored on the EHR servers using a server account rather than an EHR user account.

### 3. The Risk of Record Loss Due to Natural Catastrophes

Fires, floods or other environmental disasters attack physical locations and can result in the complete loss of both paper and electronic medical records.

## RISKS MORE COMMON TO PAPER RECORDS

### 1. The Risk of Mislabeling Misfiled or Lost Records

Paper records must be manually filed. The shear volume of records increases the likelihood that records are lost because they are incorrectly filed or never returned to the file room. On the other hand, electronic records are rarely lost because they are never removed from the EHR system. EHR records are indexed in multiple ways allowing for fast searches and accurate retrieval.

## RISKS MORE COMMON TO ELECTRONIC RECORDS

### 1. The Risk of Record Degradation

Paper records deteriorate slowly. With proper storage controlling exposure to light and humidity, paper records can last for hundreds of years. If necessary, significantly deteriorated paper records can be copied to create new originals.

Electronic records can degrade catastrophically -- tapes break, a bearing

breaks on a piece of hardware, optical media is scratched. Such failures can happen at any time without warning. Depending on the type of storage and the amount of damage, it may be impossible to recover the affected data.

### 2. The Risk of Technology Becoming Obsolete

Retrieval and use of paper records is not affected by technological changes. Even where paper records are stored on film or micro-fiche, the expected technology life cycle is sufficiently long to avoid obsolescence concerns.

Electronic records depend upon computing technologies that have notoriously short lifecycles. For the past several decades, Moore's Law and its variants have been operating with respect to computing, storage and networking technologies. Following such laws, various performance characteristics of new computing systems double each year or two at a cost of one half that of the previous generation. This means that during the life of an average medical record, the computing technologies will have undergone multiple generational changes. With each technology generation, previous technologies lose market value and manufactures cease production. This means that the technology upon which the EHR system depends will become unsustainable as replacement parts become unavailable and while operating systems and database platforms lose vendor support.

Developed by the Health Resources and Services Administration as a resource for health centers and other safety net and ambulatory care providers who are seeking to implement health IT.