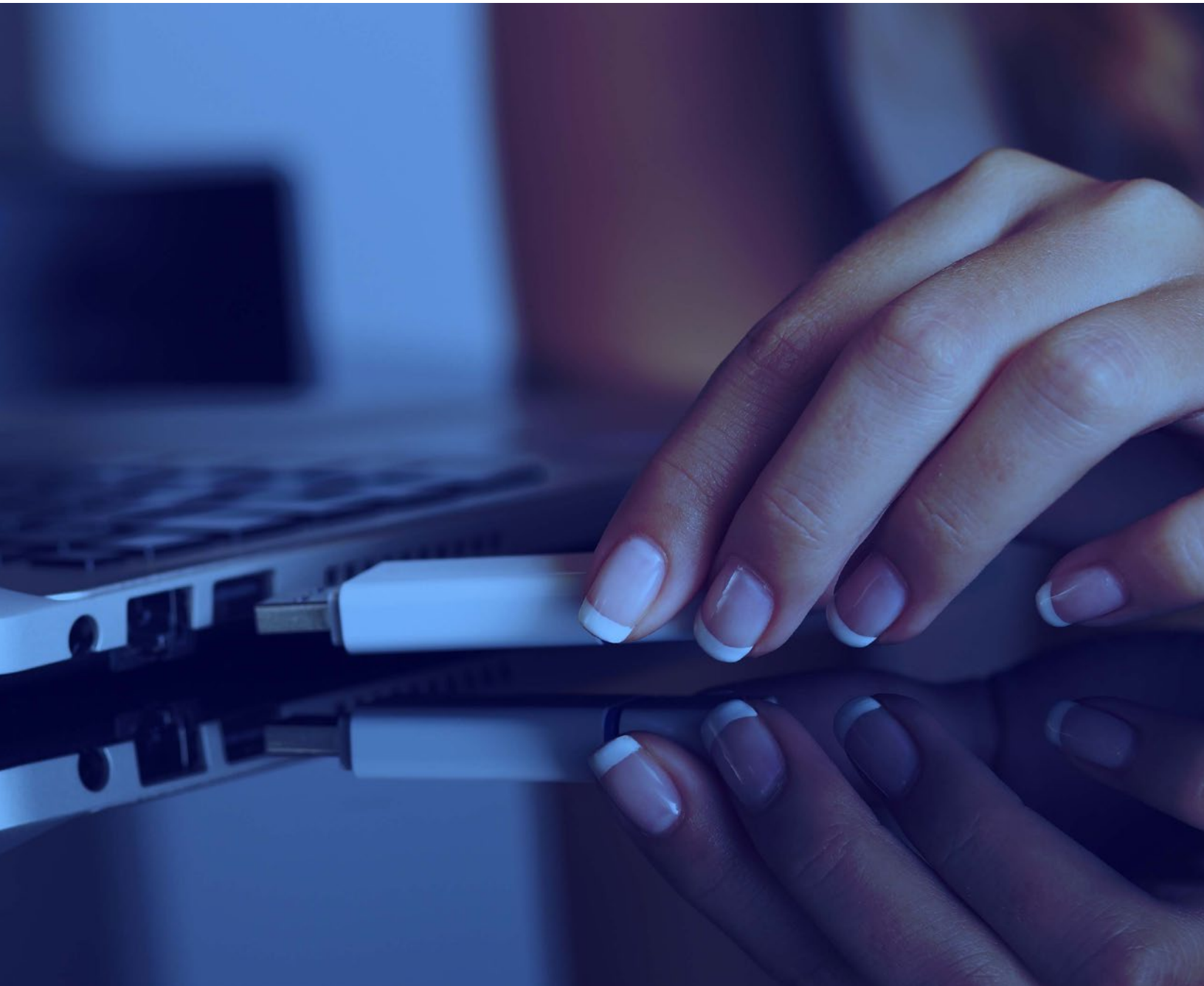
WINZIP

WinZip SafeMedia: Helping Healthcare Organizations Secure Data to Comply with HIPAA and HITECH Rules

White Paper | WinZip SafeMedia



Introduction

Healthcare organizations transmit, manage, process, and store vast amounts of regulated information, from patient health records to financial information to internal employee data. This data is often stored and shared on removable media devices, such as USB flash drives, external hard drives, CDs, DVDs, and Blu-Ray Discs.

In addition to the challenge of securing this volume of information, healthcare organizations also must comply with strict federal regulations that control how data is accessed and protected, as well as how clients must be notified in the event of a data breach.

HIPAA and HITECH Rules for Healthcare Data Regulation

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the US Department of Health and Human Services (HSS) to develop regulations protecting the privacy and security of protected health information (PHI).

As part of this requirement, the HHS established a set of rules and national standards for the protection of health information. These rules apply to "covered entities," including health plans, healthcare clearinghouses (such as billing services), and community health information systems and healthcare providers that transmit healthcare data in a way that is regulated by HIPAA.

HIPAA includes a set of administrative simplification provisions that, among other things, include rules to help protect the privacy of PHI:

- **The Privacy Rule** regulates who can access PHI, the circumstances in which PHI can be used, and when and how PHI can be disclosed without patient authorization. The rule applies to all PHI, regardless of how it is created, used, stored or disclosed.
- **The Security Rule** requires appropriate administrative, physical and technical safeguards to restrict unauthorized access to electronic PHI, prevent unauthorized disclosure of electronic PHI, and ensure the confidentiality, integrity and availability of electronic PHI both in transit and at rest.
- **The Breach Notification Rule**, issued as part of the Health Information Technology for Economic and Clinical Health Act (HITECH), requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured PHI.

The HHS has issued guidance on how to secure protected health information appropriately. This includes the technologies and methodologies that render PHI "unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction."

These methods apply to commonly recognized data states, including data in transit and data at rest (e.g., data stored on CD, DVD or USB flash memory devices).

The Challenge of Protecting Health Data in an Increasingly Mobile Business World

Data breaches have become a major problem for businesses and organizations, especially with the increase in remote work environments. According to Gartner, 32% of employees worldwide will work remotely by the end of 2021, up from 17% in 2019.

With the rise of remote and hybrid work environments, the need for data protection in this business world is at an all-time high. According to a recent study by IBM Security and the Poneman Institute, data breaches in 2021 had the highest average cost in 17 years.

Healthcare organizations have both ethical and legal responsibilities to protect confidential patient data, and doing so has only gotten harder. There's been an upward trend in healthcare data breaches over the past decade: From 2009 to 2020, the HSS' Office for Civil Rights received reports of 3,705 data breaches of 500 or more healthcare records, affecting 268,189,693 total records.

In addition to PHI requirements, healthcare organizations must protect internal information, such as employee records, administrative data, and patient surveys. The need to protect personally identifiable information (PII) about individuals is of particular concern, and PII may be found in a variety of data sources and electronic devices.

Encryption is one reliable way to prevent unwanted access to data. In the simplest terms, encryption of data on portable media (e.g., USB drives, CDs, DVDs) can prevent unauthorized users from accessing it.

Encryption takes a plaintext message and renders it unintelligible by processing it into ciphertext. This process depends on a cipher algorithm and a secret key, which is used by the cipher algorithm to modify data as it is encrypted.

A reliable encryption method must be strong enough to prevent circumvention and protect digital data. In addition to security, some organizations must also comply with compliance regulations that require specific encryption standards. For example, the Advanced Encryption Standard (AES) meets government and legal requirements for protecting confidential data.

WinZip SafeMedia Removes the Risk from Portable Media

WinZip® SafeMedia™ is specifically designed to make it extremely easy to secure data on removable media. Ideal for healthcare organizations of all sizes, WinZip SafeMedia makes it easy for employees to automatically encrypt data per organizational policies. It also enables customized administrative tools that let IT set and alter read, write and access permissions at group and individual levels.

Flexible administrative tools simply the application of custom security protocols, giving IT better visibility and control over software protocols, ensuring that users cannot bypass or forget security procedures.

With powerful AES encryption and support for FIPS 140-2 certified* encryption and password protection, WinZip SafeMedia helps organizations comply with government and healthcare industry security standards while protecting their intellectual property, PII and PHI.

Encryption can be controlled by the user or by the system administrator at the user, group or organizational level based on policy.

With user-friendly design and powerful tools for system administrators, WinZip SafeMedia provides an added layer of security that extends to your portable media, with IT-controlled protocols that ensure adherence to organizational security procedures.

Employees can quickly save information on USB devices using powerful data encryption that safeguards the content from being accessed by unauthorized users. The solution's simple drag and drop functionality ensures users experience virtually no impact on their workflow while building a failsafe, secure environment.

WinZip SafeMedia goes beyond simple encryption on standalone machines to provide advanced endpoint security features for both small family practices and multi-departmental global enterprises.

It's a solution that arms healthcare organizations with the tools to not only meet internal security policies, but also comply with industry- and government-mandated privacy measures and regulations. Additionally, the solution supports Safe Harbour Privacy Principles should a storage device become lost or if your infrastructure is breached.

With WinZip SafeMedia, healthcare organizations can:

- Burn data on CDs, DVDs, Blu-ray Discs and USB drives using an easy drag and drop interface.
- Use the powerful WinZip Zip engine to maximize storage space with file compression capabilities.
- Burn and copy multiple discs and disc image files simultaneously.
- Encrypt data using a FIPS 140-2 encryption module.*
- Secure files with powerful 256-bit AES encryption and SHA-2 standard support.
- Span files too big to fit across multiple discs.
- Read and write disc image files.
- Verify data after burning.
- Enable discs to be read on PCs within permitted departmental groups.
- Restrict permission to read discs on PCs outside permitted departmental groups.
- Support read/write permissions set by system administrators.
- Enable logging to keep track of data, device name, username, files, folders, and other information.
- Supports business continuity and disaster recovery through "break-the-glass" functionality for access encrypted zip files for which the owner is not immediately available to decrypt.

WinZip SafeMedia makes it easy for employees to automatically encrypt data per organizational policies. It also enables customized administrative tools that let IT set and alter read, write and access permissions at group and individual level, and IT-enabled security measures like forced encryption and password protocols.

It's a hassle-free security solution that works in the background to protect intellectual property, private information and more, safeguarding healthcare organizations from the expense of data breaches and non-compliance with mandated regulations.

Learn how WinZip SafeMedia can protect sensitive healthcare data.

**WinZip SafeMedia secure disc burning uses a FIPS 140-2 certified encryption module from Microsoft.*

winzip.com/safemedia/