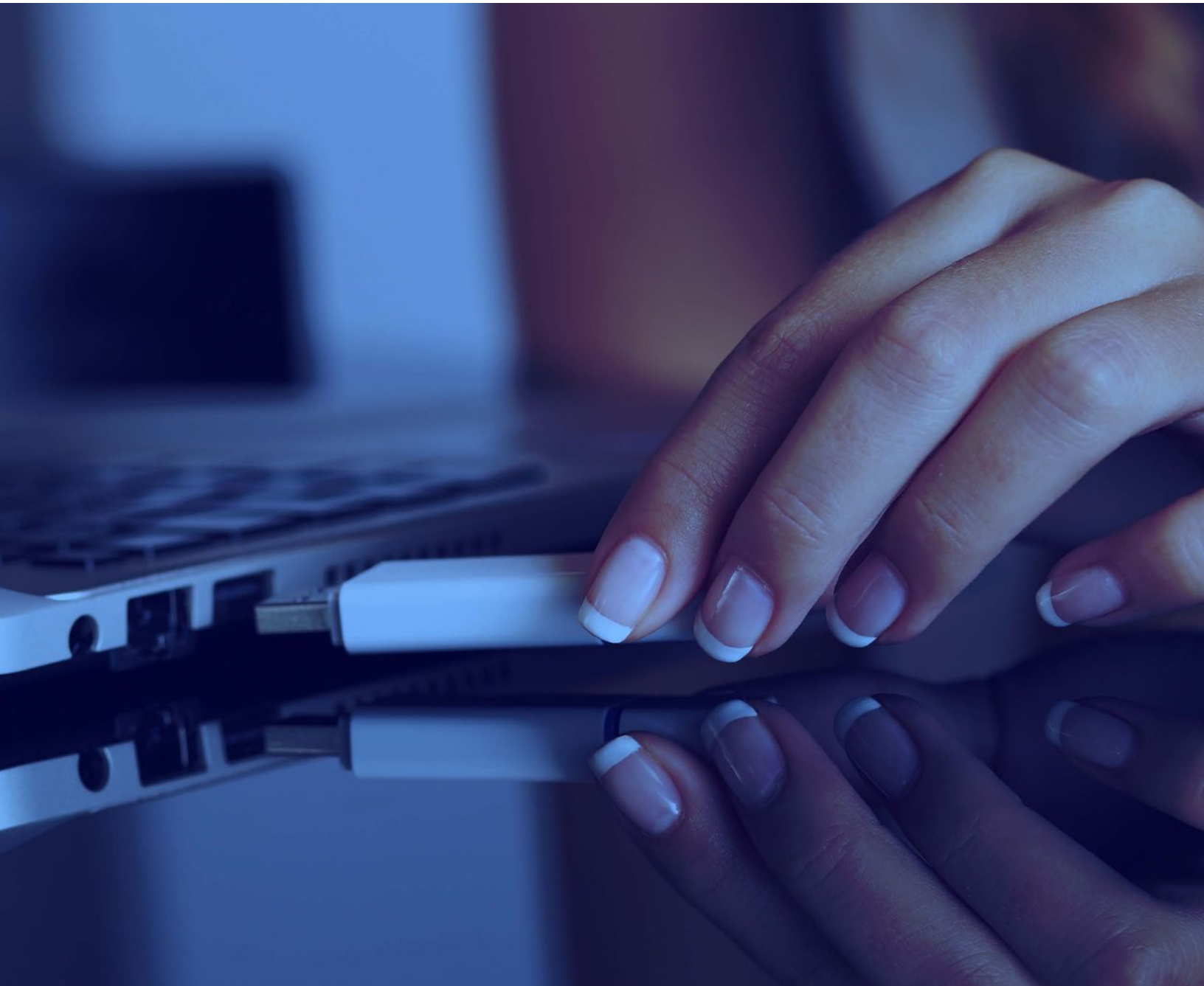
WINZIP

WinZip SafeMedia: Safe, Effective Removable Media Data Protection for Law Firms

White Paper | WinZip SafeMedia



Introduction

Law firms and their clients commonly store and exchange data on portable media, including USB memory sticks, external hard drives and CDs.

Copying, archiving, and exchanging data on portable media is a key process in today's increasingly distributed business environment. This data is often regulated and may include client records, "internal eyes only" legal briefs, and other sensitive information. However, portable media can easily be lost or stolen. It's thus critical that data stored on this media is protected.

WinZip® SafeMedia™ secures your data. It manages the encryption of data on portable media, including USB flash memory devices and optical discs, making it easy for law firm personnel to monitor, control, and protect confidential information and ensure compliance with regulatory obligations.

Data Breaches: A Major Problem in the Legal Sector

Data security is a critical element in protecting your law firm's reputation. From private practices to in-house legal teams, attorneys and employees collect large volumes of highly sensitive and confidential information.

Cybercriminals know the value of this information, and firms of all shapes and sizes may be subject to targeted security threats. A 2020 American Bar Association (ABA) Legal Technology Survey Report found that 29% of firms experienced some sort of security breach, up from 26% in 2019.

Law firms have both ethical and legal responsibilities to protect confidential client files containing regulated information. These files often contain highly sensitive and valuable information, including:

- Intellectual property.
- Financial information.
- Trade secrets.
- Personally identifiable information (PII).
- Protected health information (PHI).

Accessibility and portability are ubiquitous and industry neutral. Therefore, legal professionals do well to implement data protections designed to reduce the risk of data breach. Unsecured data leads to monetary, legal, and compliance ramifications.

While encrypting the data law firms store on portable media can help prevent unwanted access to data, the ABA's 2020 technology report found that only 43% of surveyed law firms use encryption to protect sensitive files.

ABA rules impose specific requirements regarding cybersecurity in the legal sector. Attorneys must maintain the confidentiality of client information and documents. This includes making reasonable efforts to prevent unauthorized access to such information.

According to ABA Ethics Opinions 483 and 95-398, legal professionals can be held liable for data breaches, even if the law firm has non-legal staff or contractors responsible for their technical operations.

The Challenge of Protecting Data in a Mobile Business World

The COVID-19 pandemic caused major disruptions across all industries and business sectors inclusive of Legal. Impacts resulted in creation of new processes for legal service delivery. Both remote work and increased reliance on portable media requires non-repudiable data security controls.

According to a recent industry report, the number of lawyers in the US who want or plan to work remotely has doubled from the pre-pandemic period, with 76% of individuals favoring a remote work option.

In the simplest terms, encryption of data prevents unauthorized access and ensures communication and data remain private while residing on portable storage. Due to the legal field's broad reach servicing individual office level and practice groups, encryption methods must comply minimally with government and client requirements.

One of the biggest challenges in protecting data on portable media is the ease of storing files without appropriated technical controls enabled. Those controls include access based on roles along with recoverability of data when the owner is unavailable.

41 percent of all data breaches between 2005 and 2015 were the result of lost devices. A laptop is lost or stolen every 53 seconds. Roughly 70 million smartphones are lost each year—and only 7 percent are recovered.

WinZip SafeMedia Protects Data on Portable Media

WinZip SafeMedia is specifically designed to enable users to quickly secure data stored on portable media. It offers enhanced administrative controls, which make it easy to customize and scale to meet the needs of any law firm, regardless of size. Additionally, it provides safe harbor when devices containing regulated information are lost through DOD level encryption.

With a user-friendly design and powerful tools for system administrators, WinZip SafeMedia protects your organization against data breaches. This added layer of security extends to portable media, with IT-controlled protocols that ensure adherence to organizational security procedures.

Users can easily and securely add, burn, and save files on USB devices, CDs, DVDs, and Blu-ray Discs using a simple drag and drop interface. System administrators can set and enforce security policies, including the ability to customize settings at the user, group, or organizational level.

WinZip SafeMedia uses powerful data encryption to safeguard intellectual property, private client information, and more. This allows legal professionals to go beyond simple encryption on standalone machines, ensuring fail-safe protection on removable devices.

WinZip SafeMedia arms law firms with the tools to not only meet internal security policies, but also comply with industry and government-mandated privacy measures and regulations.

With WinZip SafeMedia, law firms can:

- Transparently encrypt data copied to USB storage devices, CDs, DVDs, and Blu-ray Discs using an easy drag and drop interface.
- Use the powerful WinZip 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*, with powerful 256-bit AES encryption and SHA-2 standard support.
- Span files that are 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 and secure data on portable media. This protects law firms and their clients from the expense and hassle of data breaches and non-compliance with mandated regulations.

It's a convenient, effective way for law offices to ensure that confidential records stored on removable media are only viewable by authorized personnel.

Learn how WinZip SafeMedia can protect your law firm's sensitive data.

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

winzip.com/safemedia/