ENCRYPTED USB STORAGE SOLUTIONS FOR HEALTHCARE

IRONKEY™ SECURE STORAGE

DON'T BE TOMORROW'S HEADLINE

With the global healthcare market undergoing upheaval and transformation, you can't afford a costly data breach to further shake the confidence of patients, partners or regulators. Yet when you equip a growing mobile workforce with devices that store personally identifiable patient data or R&D information, you may be putting that data at serious risk.

Failing to anticipate those risks could compromise your ability to meet the strict data security mandates that govern healthcare data access and handling, including the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, Centers for Medicare & Medicaid Services (CMS) security requirements for Electronic Health Records (EHRs), and a growing list of international standards.

Clearly, it's never been more crucial for hospitals, healthcare providers, insurers and pharmaceutical companies to take the risk out of mobility.

DEPLOY THE HIGHEST STANDARDS OF PROTECTION

With IronKey, you can achieve all these goals. Our military-grade encrypted USB storage devices put a wall between unauthorized users and your important data you need to protect. Choose from an array of IronKey solutions:

- encrypted USB flash drives
- encrypted USB external hard drives
- USB drive management solutions

IronKey devices offer multiple layers of protection, including: strong, multifactor authentication; XTS-AES and AES 256-bit hardware encryption; and tamper- and waterproof** enclosures.

GET THE IRONKEY ADVANTAGE

Mobilize doctors, trial managers, adjusters and others by enabling them to safely access sensitive data from virtually any PC or tablet.

Shield healthcare data with a virtually indestructible drive that exceeded military waterproof testing requirements.

Lock down patient and R&D data by putting military-grade encryption and a ruggedized enclosure between unauthorized users and your IronKey drive's contents.

Meet security mandates by relying on FIPS 140-2 Level 3* validated devices and advanced auditing and reporting.

Simplify HIPAA audits with advanced auditing and reporting capabilities.

Centrally manage data access and use, no matter where employees go.

WITH IRONKEY SECURE STORAGE DRIVES...

- Doctors can securely and easily access patient data no matter where they are.
- Temporary medical and pharmaceutical personnel can gain trusted access to applications and records when on assignment or working from home.
- Clinical trial contributors, managers and auditors can securely enter or review trial data at any location with a PC or tablet.
- Insurance claims adjusters, examiners and investigators can always have access to records.
- Organizations can provide key personnel with critical data to maintain operations if severe weather or other disasters strike.
- IT can enforce access and use policies from a central console.

BUILD YOUR SECURITY MOBILE STORAGE STRATEGY WITH IRONKEY

ENCRYPTED USB FLASH DRIVES 2GB-128GB

HIGHEST SECURITY (FIPS 140-2 LEVEL 3)* + CENTRALIZED MANAGEMENT	*The right choice for . . .*
IRONKEY ENTERPRISE S1000 USB 3.0 performance with cloud or on-premises centralized management, enhanced XTS-AES 256-bit encryption, optional antivirus and lifetime warranty	• Auditing and reporting for compliance with widest range of data security mandates • Broad deployments • High-risk, high-traffic environments
IRONKEY ENTERPRISE S250 + D250 Cloud or on-premises centralized management, optional antivirus, ID management and VeriSign® Identity Protection (VIP)	
IRONKEY F150 Rugged metal enclosure, optional centralized management and antivirus	
IRONKEY F100 Durable polymer housing, optional centralized management and antivirus	• Affordable deployment • Compliance with strict data security mandates

HIGHEST SECURITY (FIPS 140-2 LEVEL 3)*	*The right choice for . . .*
IRONKEY BASIC S1000 USB 3.0 performance, enhanced XTS-AES 256-bit encryption, lifetime warranty	• Deployments without the need for centralized management, reporting or auditing • High-risk, high-traffic environments • Compliance with most data security mandates
IRONKEYBASIC S250 + D250 Self-service password reset	

***What is FIPS 140-2 Level 3?** A U.S. government computer standard that defines a high level of cryptographic and physical protection designed to keep sensitive data safe from theft or hacking. For a listing of IronKey certificate numbers, please visit http://www.ironkey.com/en-US/website/certification-and-compliance.html.

****What is the waterproof standard?** MIL-STD-810G/MIL-STD-810F, also referred to as US Department of Defense Test Method Standard for Environmental Engineering Considerations and Laboratory Tests, establishes testing standards to evaluate the durability of products, especially in extreme circumstances. IronKey devices are waterproof and dustproof according to MIL-STD-810G/MIL-STD-810F standards.

EASE THE BURDENS OF COMPLIANCE

Passing your HIPAA audit doesn't have to be a headache. Use IronKey's advanced reporting and auditing capabilities to document how, where and when users have accessed, saved or modified confidential data. And for maximum flexibility, we offer both on-premises management solutions (when device management must reside behind your firewall) and cloud-based management solutions (which eliminate the need for capital investments in servers and other hardware).

DEPLOY TOUGH, PROVEN IRONKEY DRIVES

IronKey USB flash drives undergo thousands of hours of rigorous read/write tests, and we encase each one in a sturdy, tamper-proof chassis that's water, dust and shock-proof.

RELY ON AN END-TO-END IRONKEY SOLUTION

IronKey solutions are designed to work seamlessly together and create a cost-effective, end-to-end solution that you can use to reduce your potential exposure to non-compliance, drive down operating costs, improve productivity, and maintain operations no matter what happens. Deploy our encrypted USB storage devices in conjunction with secure portable workspace products to fully and confidently mobilize any workforce.