

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; 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-64GB	
HIGHEST SECURITY (FIPS 140-2 LEVEL 3)* + CENTRALIZED MANAGEMENT	THE RIGHT CHOICE FOR...
IRONKEY ENTERPRISE S250 + D250 CLOUD OR ON-PREMISE CENTRALIZED MANAGEMENT, OPTIONAL ANTIVIRUS, SECURITY SOFTWARE, ID MGMT. AND VERISIGN® IDENTITY PROTECTION (VIP)	<ul style="list-style-type: none"> • AUDITING AND REPORTING FOR COMPLIANCE WITH WIDEST RANGE OF DATA SECURITY MANDATES • BROAD DEPLOYMENTS • HIGH-RISK, HIGH-TRAFFIC ENVIRONMENTS
IRONKEY F200 BIOMETRIC AUTHENTICATION, OPTIONAL CENTRALIZED MANAGEMENT AND ANTIVIRUS	
IRONKEY F150 RUGGED METAL ENCLOSURE, OPTIONAL CENTRALIZED MANAGEMENT AND ANTIVIRUS	
IRONKEY F100 DURABLE POLYMER HOUSING, OPTIONAL CENTRALIZED MANAGEMENT AND ANTIVIRUS	<ul style="list-style-type: none"> • AFFORDABLE DEPLOYMENT • COMPLIANCE WITH STRICT DATA SECURITY MANDATES
HIGHEST SECURITY (FIPS 140-2 LEVEL 3)*	THE RIGHT CHOICE FOR...
IRONKEY PERSONAL S250 + D250 ID MGMT, OPTIONAL ENCRYPTED PASSWORD BACKUP, SECURE WEB BROWSER AND VERISIGN® IDENTITY PROTECTION (VIP)	<ul style="list-style-type: none"> • DEPLOYMENTS WITHOUT THE NEED FOR CENTRALIZED MANAGEMENT, REPORTING OR AUDITING • HIGH-RISK, HIGH-TRAFFIC ENVIRONMENTS • COMPLIANCE WITH MOST DATA SECURITY MANDATES
IRONKEY BASIC S250 + D250 SELF-SERVICE PASSWORD RESET	
HIGH SECURITY	THE RIGHT CHOICE FOR...
IRONKEY D80 BUILT-IN AES-256 HARDWARE ENCRYPTION, PASSWORD PROTECTED	<ul style="list-style-type: none"> • DEPLOYMENTS WITHOUT THE NEED FOR CENTRALIZED MANAGEMENT, REPORTING OR AUDITING • COMPLIANCE WITH MANY DATA SECURITY MANDATES
ENCRYPTED USB HARD DRIVES 320GB-1TB	
HIGHEST SECURITY (FIPS 140-2 LEVEL 3)* + CENTRALIZED MANAGEMENT	THE RIGHT CHOICE FOR...
IRONKEY H200 BIOMETRIC, STRONG PASSWORD, OPTIONAL CENTRALIZED MANAGEMENT AND ANTIVIRUS	<ul style="list-style-type: none"> • AUDITING AND REPORTING FOR COMPLIANCE WITH WIDEST RANGE OF DATA SECURITY MANDATES • LARGE DATA SETS AND FULL OR PORTABLE APPLICATIONS • HIGH-RISK, HIGH-TRAFFIC ENVIRONMENTS
IRONKEY H100 STRONG PASSWORD AUTHENTICATION, MULTI-USER COLLABORATION THROUGH SAFESHARE, AUTHENTICATION, OPTIONAL CENTRALIZED MANAGEMENT AND ANTIVIRUS	
HIGH SECURITY + CENTRALIZED MANAGEMENT	THE RIGHT CHOICE FOR...
IRONKEY ENTERPRISE H300 EXTERNAL HARD DRIVE USB 3.0 PERFORMANCE, AES 256-BIT HARDWARE ENCRYPTION	<ul style="list-style-type: none"> • AUDITING AND REPORTING FOR COMPLIANCE WITH A WIDE RANGE OF DATA SECURITY MANDATES • PERFORMANCE OF USB 3.0 WITH FASTER READ/WRITE SPEEDS
HIGH SECURITY	THE RIGHT CHOICE FOR...
IRONKEY BASIC H300 EXTERNAL HARD DRIVE USB 3.0 PERFORMANCE, AES 256-BIT HARDWARE ENCRYPTION	<ul style="list-style-type: none"> • DEPLOYMENTS WITHOUT THE NEED FOR CENTRALIZED MANAGEMENT, REPORTING OR AUDITING • PERFORMANCE OF USB 3.0 WITH FASTER READ/WRITE SPEEDS • COMPLIANCE WITH MANY DATA SECURITY MANDATES

*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-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-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 premise-based 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. And our **IronKey USB hard drives** are protected by high-strength, tamper-proof aluminum enclosures that resist break-ins.

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.

SALES CONTACTS

WEBSITE

www.ironkey.com

US AND CANADA

securitysales@imation.com

+1 888 435 7682 or +1 408 879 4300

EUROPE

emeasecuritysales@imation.com

+44 (0)1332 597 168

ASIA PACIFIC

apacsecuritysales@imation.com

+65 6499 7199