DATALOCKER SOLUTIONS FOR HEALTHCARE

Encrypted USB Storage – External Hard Drives – Encrypted Virtual Drives – Central Management

HEALTHCARE HAS A SERIOUS DATA BREACH PROBLEM

Data breach incidents are on the rise. The Associated costs are at an all-time high. And that's to say nothing of the immeasurable damage to a care provider's reputation and trust. These days, hospitals, healthcare providers, and pharmaceutical companies must be incredibly vigilant about data security.

41 MILLION+
Patient records breached in 2019. (Fierce Healthcare)

$6.45 MILLION
Average cost of a healthcare data breach (IBM Security)

3X
Increase in total number of breach incidents between 2018 and 2019 (Protenus)

88%
Breach actors that were financial motivated (Verizon DBIR)

The challenge of securing data is compounded by the fact that healthcare personnel are working remotely more than ever. This increase in mobility can put personally identifiable patient data or other sensitive information at serious risk. Failing to anticipate and address these risks can compromise your ability to meet the strict data security mandates that govern healthcare data access and handling, including HIPAA, the HITECH Act, CMS, security requirements for EHRs, and a growing list of international standards.

Now is the time to take action to defend sensitive health records.

A POWERFUL APPROACH TO DATA BREACH PREVENTION

DataLocker® protects data while allowing employees to work wherever they need to. With DataLocker, any end-user can secure data with military-grade, AES 256-bit encryption using an easy-to-use USB device. Meanwhile, security administrators can monitor, track, and audit devices in the field from one central location using SafeConsole®.

DATALOCKER ENCRYPTED DRIVES

ENCRYPTION ANYONE CAN USE

- No software to install
- Easy-to-use alphanumeric keypad
- Built in malware software scans powered by McAfee®
- Manageable by SafeConsole

SAFECONSOLE MANAGEMENT PLATFORM

POWERFUL REMOTE ADMINISTRATION

- Manage and monitor encrypted endpoints
- Remotely track drive locations
- Remotely disable or wipe lost or stolen drives

CUSTOMER CASE STUDY

BJC HealthCare

PROJECT

BJC needed a way to manage and protect over a thousand hard drives and USB drives scattered across the nation.

SOLUTION

DataLocker SafeConsole Cloud, DataLocker H350 encrypted hard drives, and Sentry ONE USB flash drives.

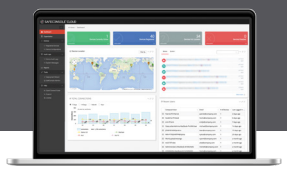
USE CASE

BJC is a non-profit healthcare organization operating in over 12 hospitals in the St. Louis area. They were seeking a way to ensure that employees could keep sensitive data protected, even in remote work environments. They turned to DataLocker SafeConsole to provide them with encrypted hard drives and USBs as well as a powerful central management system that would allow them to easily inventory, audit, manage, and control all devices. Today, DataLocker is still the only approved solution for BJC, and they have renewed their commitment to the solution for many years into the future.

THE RIGHT CHOICE FOR

- 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
- Performance of USB 3.0 with faster read/write speeds
- Requirements for HIPAA and other initiatives

SAFECONSOLE®



Managed by SAFECONSOLE®

DATALOCKER BENEFITS

DEPENDABLE ORGANIZATION

DataLocker solutions are trusted by thousands of enterprises ranging from multinational organizations to government agencies with highly sensitive data security requirements.

END-TO-END PROTECTION

DataLocker hardware and software work seamlessly together. The result is a comprehensive solution that encompasses robust, user-friendly physical drives, secure virtual drives, and a full cloud-based management for tracking and auditing.

MILITARY-GRADE SECURITY STANDARDS

Meet security mandates by relying on FIPS 197* validated devices and advanced auditing and reporting.

CENTRAL MANAGEMENT

Monitor your encrypted endpoints, audit device usage, and control policies with DataLocker's central management platforms.

ANTI-MALWARE DEFENSE

Powered by McAfee

In partnership with McAfee®, DataLocker offers built-in anti-malware protection that scans and removes any malware detected on the device and reports all action to the admin portal for audit.

Trusted By

McKESSON · Pfizer · Henry Ford Health System · CVS Health · Allscripts · Humana. · UnitedHealthcare · Saint Luke's Health System · QUINTILES · CardinalHealth · Banner Health · Children's of Alabama

*What is FIPS 197? 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 DataLocker certificate numbers, please visit datalocker.com/certifications

**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. DataLocker devices are waterproof and dustproof according to MIL-STD-810G/MIL-STD-810F standards.

DATALOCKER® SIMPLY SECURE

Get a Custom Demo

Datalocker.com

U.S. AND CANADA
sales@datalocker.com
+1 913-310-9088

LATAM
latam@datalocker.com

EUROPE
emea@datalocker.com

ASIA PACIFIC
apac@datalocker.com