

CyberCrisis Vault



A crucial layer of assurance to access patient information **during** a cyber crisis

The CyberCrisis Vault is a robust solution for hospitals designed to ensure access to patient information when a hospital network has been immobilized from a cyber-attack. The increased number of such attacks has led Interbit Data, the leader in hospital business continuity software to develop a “hardened” version of our proven NetSafe software (in use at more than 300 hospital sites) to address the unique challenges of cyber crisis downtimes.

The Vault maintains current and essential patient information including MPI, Census, eMar and patient forms, on a protected NetSafe server isolated from the “trusted” HCIS network. During a cyber crisis, designated personnel can access the Vault. The information can be:



MPI



Census



eMar



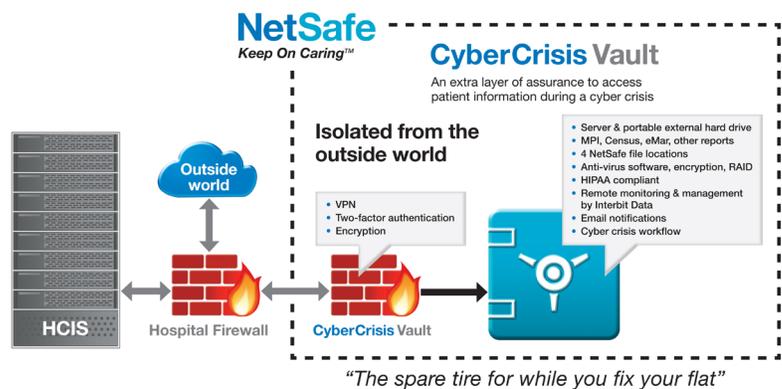
Forms

- Printed for distribution
- Viewed (and/or printed) via a web client accessing the server
- Transported to another location on a detachable hard drive, pre-configured with NetSafe.

The CyberCrisis vault serves as a critical tool to get thru the immediate impact of a cyber crisis. This allows the IT team time to address the other considerations required to restore the system. It buys a hospital time to continue to care for patients until the system is restored or a hospital’s disaster recovery plan can be put into place. It provides hospitals with peace-of-mind knowing they have an easy, fail-safe plan in place to access essential patient information.

Robust solution isolated from the outside attacks

With a robust system architecture designed to isolate the server from cyber threats, the Vault receives data from the HCIS through the hospital’s firewall and filtered by the Vault’s own firewall. This insures that, while patient information is inaccessible everywhere else, your Vault files will be there when you need them.



CyberCrisis Vault

Multi-faceted, multi-layered architecture assures your data is locked-down and always there.

Isolation	Restrictions	Security	Redundancy
 <p>One-way, single port of entry via hospital and Vault firewalls — locked down server separate from trusted hospital network</p>	 <p>Restricted inbound/outbound services with rigid rules at both firewalls</p> <p>Remote access via VPN w/Two-Factor Authentication</p>	 <p>Server and Firewall Filtered for threats by AI-based cyber protection engine by industry leading anti-malware software</p> <p>Encryption at rest on Firewall, NetSafe Server and external drive</p>	 <p>File storage – 4 locations</p> <ul style="list-style-type: none">• Server folders – NetSafe Client• Web Access – NetSafe Web Client• Portable encrypted USB drive with NetSafe Client• On-line view and/or printing <p>RAID 1 Storage</p> <p>Redundant disk and power supplies</p> <p>Anti-malware, encryption and two factor authentication at Firewall, Server & HD</p>

All-Inclusive, turnkey solution that's easy to purchase, implement, maintain and use

The CyberCrisis Vault is designed for:

1. Streamlined implementation with pre-configured hardware and software,
2. Easy setup and installation by IT in a secure area, and
3. Worry-free, on-going system monitoring and support provided by Interbit Data.



In addition, hospitals are provided with detailed workflow guidance for planning and staying prepared for cyber crisis events.

Industry-leading, best practice NetSafe

The CyberCrisis Vault is built upon Interbit Data's NetSafe Point-of-Care solution, which has been operating at hundreds of hospital sites for over 10 years. The CyberCrisis Vault itself has been installed, tested, and certified at several locations to ensure that your patient's information will always be available during a cyber-attack.

Benefits

- Clinicians and staff always have access to critical patient information ensuring on-going care to their patients DURING a cyber crisis
- Allows IT to focus on restoring HCIS, network and workstation operation
- Sustain staff workflow and productivity during a crisis
- Compliments cyber resiliency business continuity strategies
- Based on Interbit Data's award-winning NetSafe business continuity solution
- Hospital can continue to protect patient safety during a crisis
- Stress-free, fully-packaged solution with rapid implementation and on-going monitoring and maintenance means less headaches for IT department
- HIPAA compliance privacy protection
- Hospital can enhance reputation by pro-active preparation
- Peace of mind