6 STEPS & EFFECTIVE DATA BREACH RESPONSE

AN ACTION PLAN FOR HEALTHCARE IT

Whether a device containing sensitive information is lost or stolen, breached with malicious intent or unsecured by accident, the costs and consequences are the same.

How a healthcare organization responds can be the difference between a simple security incident and long-term reputation and financial damage.

Follow these six steps to keep your cool and emerge as unscathed as possible if your data is threatened.

YOUR RESPONSE PLAN OF ACTION

ACTIVATE

Assemble a crisis management team to plan and practice how to respond to a breach. This will eliminate a panic situation in the event of a real breach and allow for a faster response.



THE DAMAGE

Determine the facts of the breach.

Then, depending on how severe, either remotely freeze or delete the data on the device to keep the problem from spreading.



Ensure the team has the most current iterations of breach notification laws,

UNDERSTAND

such as HITECH, HIPAA and Gramm-Leach-Bliley Act.





Risk assessment must demonstrate that due diligence was completed

with consistent and defensible methodologies.

COLLECT,

DOCUMENT AND

ANALYZE EVIDENCE

DETERMINE

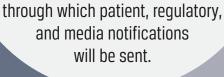
THE EXTENT

OF THE DAMAGE

was the breach accidental or malicious? Who was affected? What types of data were accessed? Answers to these questions determine the level of exposure.

SEND COMPLIANT

NOTIFICATIONS



If required to send data breach notifications, determine the channels

TAKEAWAYS:



organization.

EFFECTIVE HEALTHCARE DATA BREACH RESPONSE: HOW NOT TO PANIC WHEN SENSITIVE DATA IS COMPROMISED

Limit damage from a data breach by building your own action plan. Find out how in

the free whitepaper, Effective Healthcare Data

While healthcare organizations must support a mobile workforce,

they must also ensure and prove that PHI is secure, and that

they are in compliance at all times. Technology solutions that

help IT enable staff mobility, while mitigating the risks of data

breaches are critical to quality patient care and the success of an

DOWNLOAD THE WHITEPAPER

/ABSOLUTE

ABOUT ABSOLUTE Absolute provides visibility and resilience for every endpoint with self-healing endpoint security and always-connected IT asset management to protect devices, data, applications and users — on and off the network. Bridging the gap between security and IT operations, only Absolute gives enterprises visibility they can act on to protect every endpoint, remediate vulnerabilities, and ensure compliance in the face of insider and external threats. Absolute's patented Persistence technology is already embedded in the firmware of PC and mobile devices and trusted by over 12,000 customers worldwide.

Breach Response.



EMAIL: sales@absolute.com

North America: 1-877-660-2289

EMEA: +44-118-902-2000

/ABSOLUTE®

PHONE:



SALES: absolute.com/request-info

absolute.com

