PROTECTING PHI *in* 7 STEPS

THE PATH TO CYBER RESILIENCE FOR HEALTHCARE

Healthcare is data. Information is shared, analyzed, and transmitted to treat patients and create new forms of care. With specific and practical steps, digital care models are secured with continuous vigilance and data protection across all devices, no matter where they are.

1

Pinpoint every laptop, desktop, tablet, and mobile phone with access to PHI.

2

Identify unauthorized sharing and cloud storage apps on endpoints.

3

Deploy a minimum 128-bit encryption on every device – especially on those with access to PHI.

4

Use a persistent connection to devices, extract asset intelligence, and validate that data protection is always running (required to satisfy the HIPAA Security Rule).

5

Benchmark each endpoint's cyber hygiene and security posture to align with ever-changing requirements of HIPAA Privacy and Security Rules.

6

Implement remote command capabilities such as: data delete, data retrieval, device freeze, and forensics in the event of security incidents or exposures.

7

Learn from other organizations that have experienced a data breach; review these scenarios and make relevant adjustments to ensure you don't suffer the same fate.

TAKEAWAYS:

Asset intelligence, automated endpoint hygiene, and continuous compliance together give healthcare IT and security teams the tools to succeed in the digital care frontier.

With myriad new data protection regulations to contend with, along with the constant threat of a breach, data security is a top concern for healthcare organizations. Read about some of the most costly recent data breach incidents that resulted from lost or stolen devices and learn how to avoid similar data disasters.

DOWNLOAD THE WHITEPAPER

ABSOLUTE®

absolute.com