INFORMATION SECURITY
VULNERABILITY ASSESSMENT AND TESTING

COMPLIANCE; POLICIES AND PROCEDURES

BURTELSON CORPORATION

Burtelson

EXECUTIVE SUMMARY

Transforming how the healthcare industry deals with cyber security is our number one priority. This starts with redefining how security protocols are designed, implemented and enforced. Healthcare organizations cannot afford take a reactive approach to IT security; there is simply too much at stake.

This paper summarizes the complete aspect of Burtelson's compliance and policies & procedures protocol deployment; we will address both aspects of this compliance strategy.

ASSESS YOUR DATA INFRASTUCTURE REQUIREMENTS

Some healthcare organizations are hesitant to adopt preemptive security solutions due to concerns around cost, integration with legacy IT systems, hefty management requirements and limited visibility into existing security vulnerabilities. Not to mention the fact it can be difficult to instigate IT changes, even when such changes are made to improve and support business operations. But by enhancing compliance, including policies and procedures, healthcare organizations and practices can help reduce the risk of information theft while enabling connectivity for employees, patients, partners, researchers and other trusted third parties. In addition, organizations can more proactively identify and address inappropriate network activity and document the effectiveness of security policies and identity-related controls.

Increasing data security helps healthcare organizations meet compliance requirements and ensure that confidential patient data is properly protected. To achieve a truly secure data environment, organizations must first establish a core data security architecture by:

➢ Setting information asset profiles to determine where critical data resides, who can access it and how well it's protected

➢ Applying and managing a comprehensive encryption strategy to help keep protected health information (PHI) confidential and meet compliance mandates

➢ Implementing enterprise management for encryption and data protection, from storage on local, removable devices through servers and hosts to long-term backup and storage on tape

➢ Managing the disposal of data-bearing media—whether on paper, magnetic media or optical media—to help protect the organization's confidentiality, and that of its patients.

PROPERLY SECURING
HEALTHCARE INFORMATION
HAS NEVER BEEN
MORE CRITICAL

AS AN ESTABLISHED INFORMATION SECURITY ADVISOR TO HEALTHCARE ORGANIZATIONS, BURTELSON UNDERSTANDS HEALTHCARE ORGANIZATION AND PRACTICE SECURITY STRATEGIC AND IT REQUIREMENTS

When healthcare organizations are looking for a trusted information and cyber security adviser that can take on security management on an outsourced or out-tasked basis, Burtelson is well suited to help establish and maintain a security program, virtually regardless of the model deployed. Burtelson also provides direct access to expert security consultants who understand attack design, underlying vulnerabilities, security policies and compliance mandates. To help address an organization's needs from physical and data security to identity management and compliance audits, Burtelson provides skilled consultants to complement the efforts of internal staff or to provide comprehensive managed security services.

POLICIES AND PROCEDURES

Security begins and ends with a healthcare organization's established policies and procedures protocol. It's not just about having such protocols in place, but ensuring that they're the right protocols that will keep PHI safe and confidential.

Burtelson has vast experience in establishing and maintain information security policies and procedures, and ensuring that such protocols are adhered to, understood by staff, and hold up to the most scrutinizing security tests. Research shows that if an organization's staff are not fully trained on and fully understand not only the policies and procedures themselves, but also why they're in place and the results of not following them, security holes will remain large.

Only by securing the best protocols and the training necessary to enforce them will an organization's security holes get smaller and PHI stay protected.

THE FIRST STEP

We get started by understanding your organization's specific needs for compliance auditing and policy & procedure establishment and maintenance. This first step is perhaps the most difficult. Your organization should be asking this question again and again, as your needs, budget, and risk posture evolves.

For more information
To learn more about Burtelson security solutions, please visit us at www.BurtelsonSecurity.com or email us at info@burtelsonsecurity.com