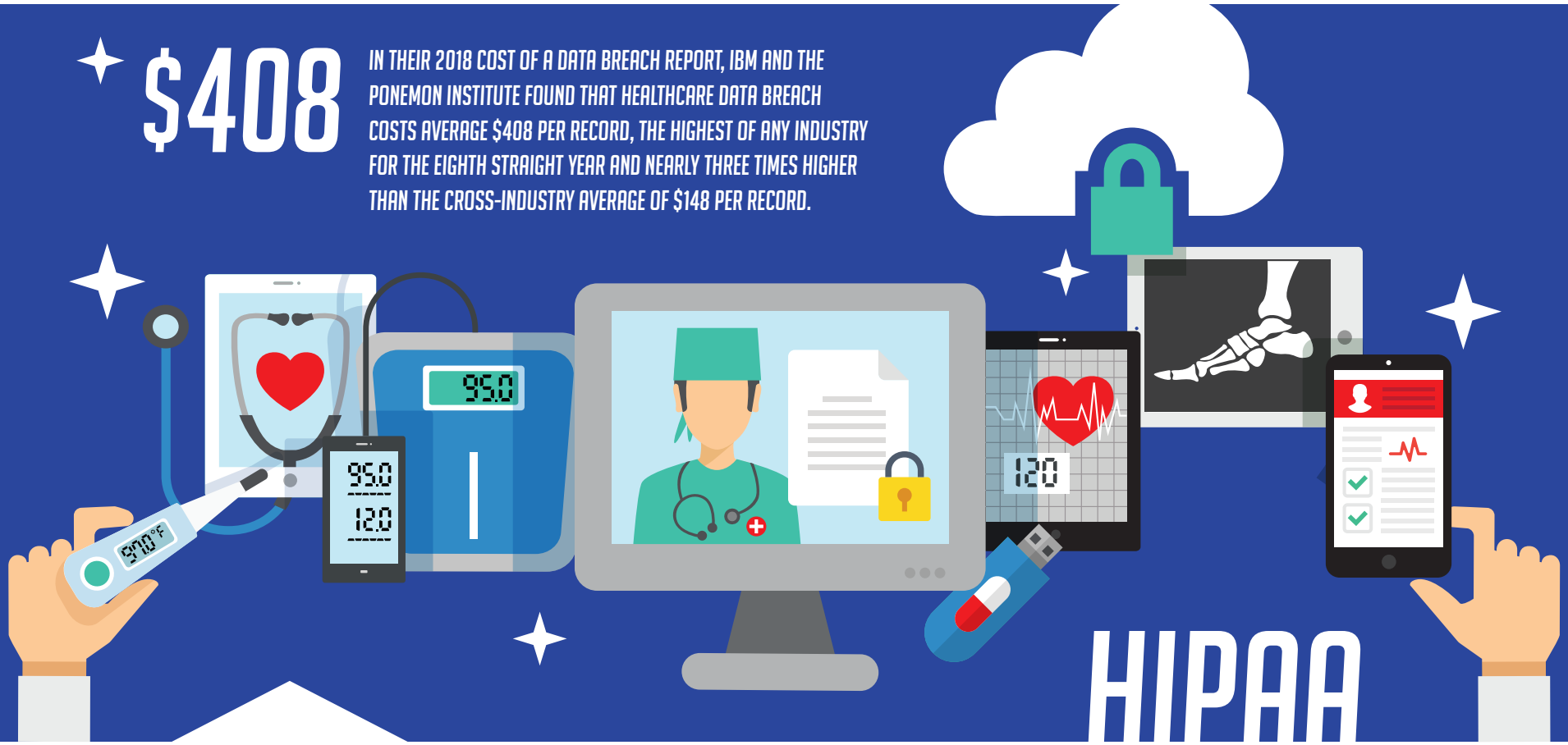
eBOOK

datamax + All Covered
IT SERVICES FROM KONICA MINOLTA / HEALTHCARE

$408

IN THEIR 2018 COST OF A DATA BREACH REPORT, IBM AND THE PONEMON INSTITUTE FOUND THAT HEALTHCARE DATA BREACH COSTS AVERAGE $408 PER RECORD, THE HIGHEST OF ANY INDUSTRY FOR THE EIGHTH STRAIGHT YEAR AND NEARLY THREE TIMES HIGHER THAN THE CROSS-INDUSTRY AVERAGE OF $148 PER RECORD.



8 QUESTIONS

WHY HEALTHCARE PROVIDERS SHOULD TAKE A HARD LOOK AT MANAGED COMPLIANCE SERVICES.

THE BURDEN OF A DATA BREACH IS A HEAVY COST TO BEAR.

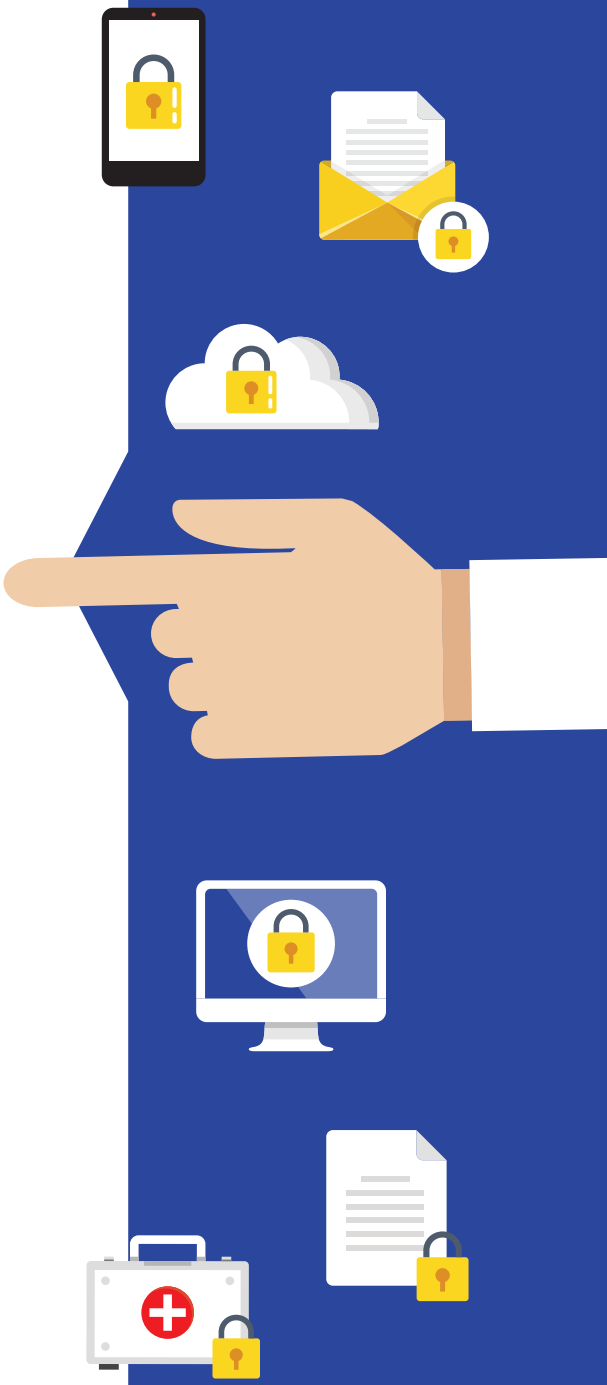
According to the Ponemon Institute's 2018 Cost of a Data Breach study, the cost of a healthcare data breach is $408 per record — higher than any other industry. Your healthcare organization literally can't afford to avoid taking proper HIPAA security and compliance measures.

THE BURDEN OF PROOF WEIGHS SOLELY ON YOU.

In the event of a data breach, your organization carries the burden of demonstrating that all notifications were made to affected individuals, or the use or disclosure of unsecured protected health information did not constitute the breach. You need proof that all compliance bases were covered.

ASK YOURSELF: IS IT WORTH THE BURDEN?

On the pages that follow, we've compiled 8 additional questions that you should ask yourself as you consider your current HIPAA compliance strategies and challenges. Do you feel secure? Do you feel burdened? Is it time to take a hard look at Managed Compliance Services?



*Among all surveyed industries, Healthcare experienced the highest customer churn rate following a breach, at **6.7 percent**, as customers have high expectations for the protection of their data in such a highly regulated industry.*

1.

DO YOU HAVE A COMPLIANCE PORTAL WITH DASHBOARD TO VIEW ASSETS, CONTROLS, POLICIES, VULNERABILITIES AND BUSINESS ASSOCIATE AGREEMENT CONFORMITY?

A Security Risk Analysis will uncover your current security weaknesses. But moving forward, access to a compliance portal offers visual insight into maintaining policies and procedures, viewing assets and current risk levels, as well as scanning for ongoing vulnerabilities.

2.

IF YOU ENGAGE WITH THIRD PARTY SUPPLIERS, DO YOU KNOW IF THEY ARE COMPLYING WITH HIPAA AS PER YOUR BUSINESS ASSOCIATE AGREEMENT (BAA)?

Covered entities must ensure that they have a current HIPAA Business Associate Agreement (BAA) in place with each of their partners to maintain PHI security and overall HIPAA compliance. HIPAA regulations require that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity.

As a covered entity that uses ePHI, a thorough assessment will demonstrate your organization's compliance, as well as assess your third party vendors, with the required regulatory requirements of HIPAA and HITECH.

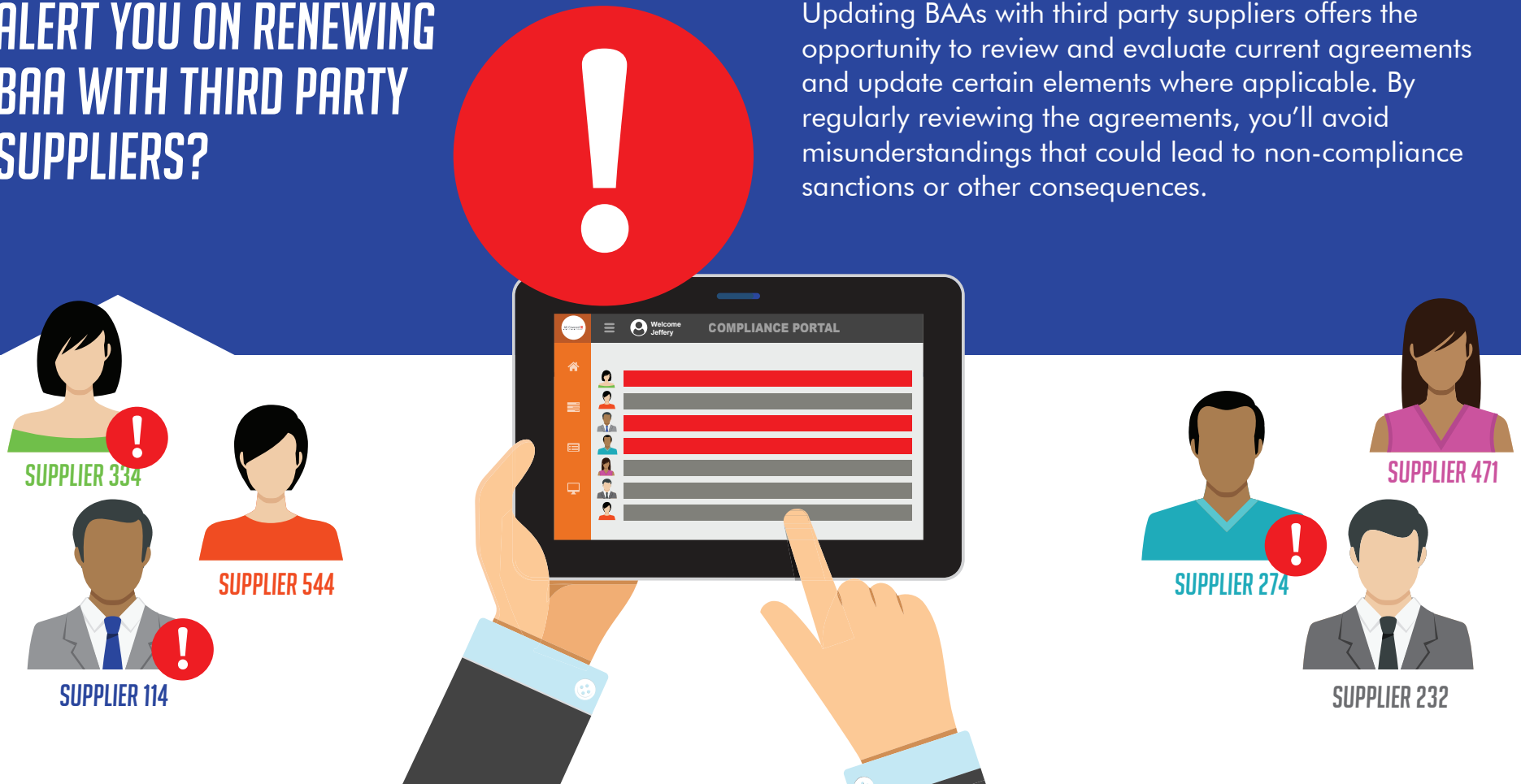
3.

*Per **Ponemon Institute's 2018 report**, 48 percent of data breaches worldwide involved a malicious or criminal attack, 27 percent were due to negligent employees or contractors (human factor) and 25 percent involved system glitches, including both IT and business process failures.*

DOES YOUR CURRENT SYSTEM ALERT YOU ON RENEWING BAA WITH THIRD PARTY SUPPLIERS?

An expired Business Associate Agreement (BAA) is the same as not having one at all. BAAs must be up to date with their own compliance to satisfy HIPAA regulations.

With visual intelligence tools available through a Managed Compliance Services Program, your organization will receive ongoing alerts on renewing appropriate BAAs. Updating BAAs with third party suppliers offers the opportunity to review and evaluate current agreements and update certain elements where applicable. By regularly reviewing the agreements, you'll avoid misunderstandings that could lead to non-compliance sanctions or other consequences.

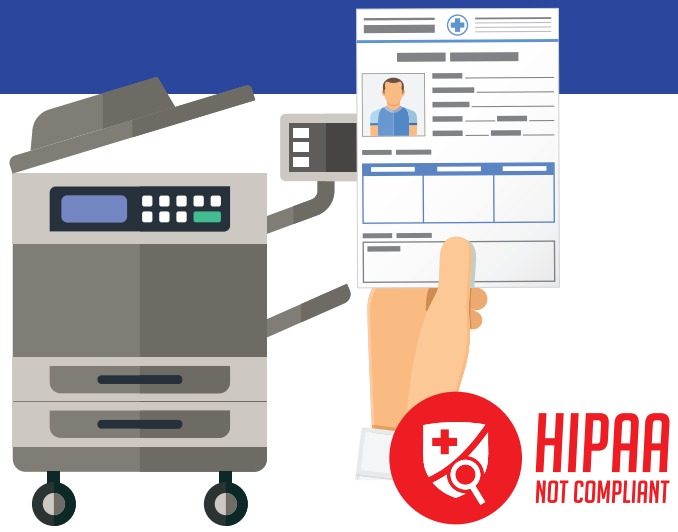


4.

DO YOU HAVE SECURITY POLICIES IN PLACE THAT PROTECT THE NON-TECHNICAL ASPECTS OF YOUR OPERATIONS?

Certain assessments analyze and mitigate technology-related threats. However, Patient Health Information could be breached under non-technical circumstances; something as simple as an employee printing information and leaving it at a printer, or someone going into a patient record and seeing information.

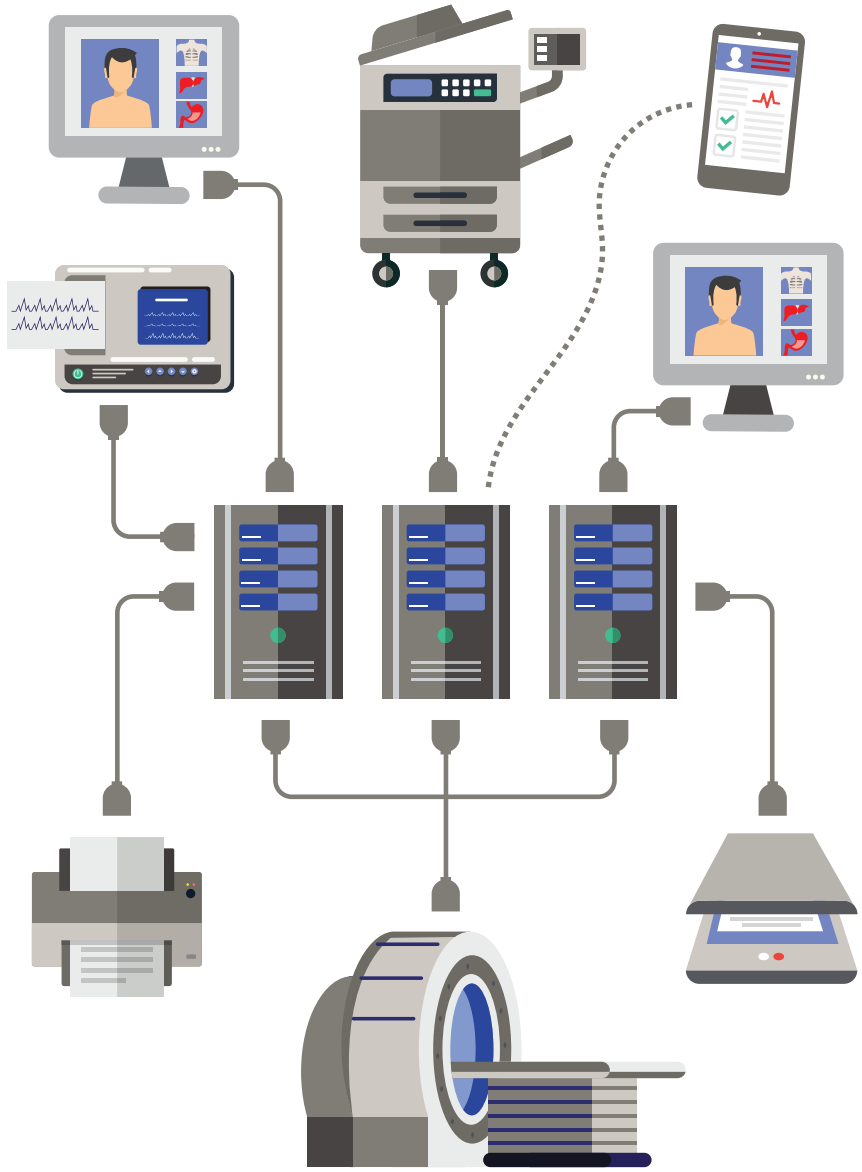
It all comes down to organizational communication – from boardroom stakeholders to end users – when addressing these non-technical safeguards. Such communication is reinforced through a Managed Compliance Services Program.



5.

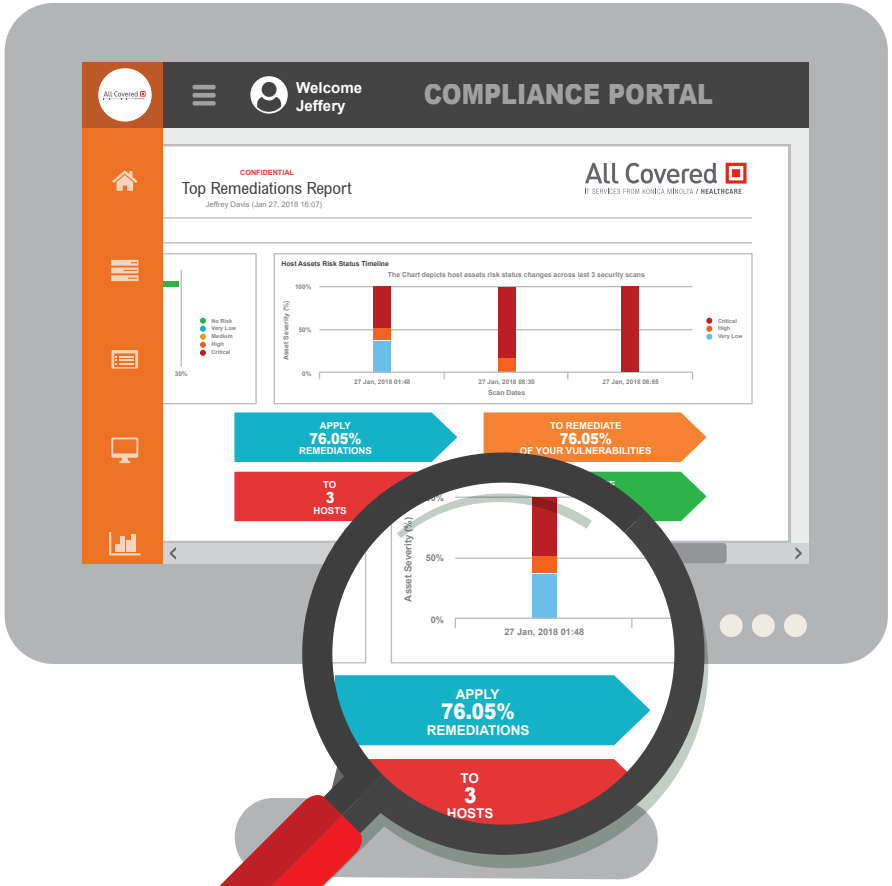
*According to **HealthIT Security**,"78 percent of healthcare providers reported that they experienced a healthcare ransomware or malware attack in 2017."*

DO YOU KNOW ALL THE ASSETS CONNECTED TO YOUR NETWORK (WIRED/WIRELESS) INCLUDING MEDICAL DEVICES AND THEIR VULNERABILITIES?



The Office of Civil Rights (OCR) requires that covered entities identify vulnerabilities to ePHI that is collected, stored, processed, or transmitted.

A Technical Vulnerability Assessment identifies both internal and external security gaps, as well as provides a thorough wireless assessment to identify any and all technical security weak points.



6.

DO YOU MONITOR YOUR POLICIES AND PROCEDURES WITH AUDIT LOG-ON CHANGES?

System logs are a required component of HIPAA Compliance for covered entities and business associates. They also play a critical role in monitoring activity on your network.

With the ability for administrators to monitor activities and changes within operating systems and other network devices, they can accurately detect problems regarding organizational security and current policies and procedures. With the right audit controls in place, your organization can proactively monitor and protect sensitive patient health information.

7.

DO YOU HAVE ONGOING HIPAA AND SECURITY AWARENESS TRAINING?

Breaches often are a result of simple employee negligence. As attacks get harder and harder to decipher, your employees are susceptible to compromising patient health information. Workforce awareness of potential threats and best practices is essential.

Establishing clear, universal communication standards across your organization, as well as extensive employee HIPAA training both onsite and online, are major components to a Managed Compliance Services program.

8.

*In the **2018 Cost of a Data Breach Report**, IBM and the Ponemon Institute found that organizations that had extensively deployed automated security technologies saved more than **$1.5 million** on the total cost of a breach.*

IF A DATA BREACH OCCURS CAN YOU DEMONSTRATE THAT APPROPRIATE SECURITY CONTROLS, POLICIES AND PROCEDURES WERE IN PLACE?

Should a breach occur, covered entities and business associates have the burden of demonstrating that all required notifications to affected individuals and HHS have been provided. They must also prove that a use or disclosure of unsecured protected health information did not constitute a breach.

Armed with a "Defense in Depth" approach that Managed Compliance Services offers, your organization can demonstrate that all appropriate controls and procedures were in place. This program can also guide you on the necessary steps for notifying appropriate parties in the event of a breach.

HOW DO I GET STARTED?

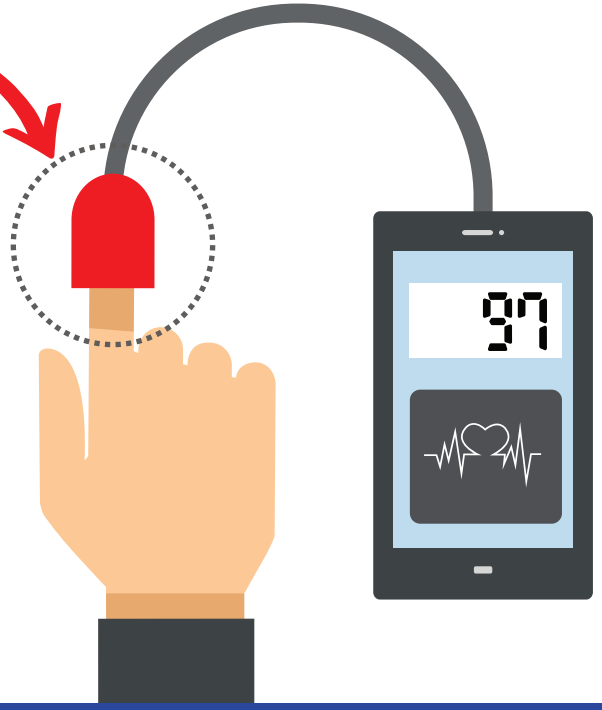
CHP Certified HIPAA Professional
HIPAA Academy

CLICK HERE

... IF YOU'RE READY TO CHECK YOUR PULSE ON THE NEED FOR MANAGED COMPLIANCE SERVICES AND TO SCHEDULE A MEETING WITH ONE OF OUR **CERTIFIED HIPAA PROFESSIONALS (CHP)** TODAY!

CAN'T WAIT?

REQUEST INFORMATION OR CALL US NOW AT **800-482-5772.**



ABOUT DATAMAX

Datamax provides a powerful portfolio of business technology services and solutions uniquely focused on document management, print management, network management, and office equipment — including multifunction printers, color printers, and production print systems. Our thought process concentrates on identifying corporate objectives, researching relevant technical options, and providing unbiased recommendations that align business goals with technology.

We are a Microsoft Gold Certified Partner, and enjoy collaborative alliances with companies including Canon, Konica Minolta, Lexmark, and Laserfiche. Discover how our sixty-plus years of insightful thought process can empower you with the freedom to focus on what you value the most — your forte — your business. At Datamax, we're all about Creating Raving Fans®!

Datamax Little Rock
7400 Kanis Road
Little Rock, AR 72204
Toll Free: 800.482.5772

Datamax Hot Springs
317 Third Street
Hot Springs, AR 71913
Toll Free: 800.364.4255

Our Locations:
Little Rock, AR • Hot Springs, AR
Dallas/Fort Worth, TX • Tyler, TX
Longview, TX • Lufkin, TX

DATAMAXARKANSAS.COM

Various references and content within are from KONICA MINOLTA & ALL COVERED Brochures: *Risk Management Program Through HIPAA Consulting Services From Konica Minolta, Healthcare IT Services And Solutions* and Presentation: *HIPAA Risk Assessment*.

eBOOK

HIPAA

8 QUESTIONS
WHY HEALTHCARE PROVIDERS SHOULD TAKE A HARD LOOK AT MANAGED COMPLIANCE SERVICES.

datamax + All Covered
IT SERVICES FROM KONICA MINOLTA / HEALTHCARE