The Ultimate Guide to Third-Party Remote Access
Compliance and the Healthcare Industry

Healthcare data breach costs are at a record high for the seventh straight year. A study published by the Ponemon Institute\(^1\) found that costs associated with Personal Health Information (PHI) or Electronic Personal Health Information (ePHI) averages an alarming $380 per record.

The same study marked malicious and criminal attacks as the most common means of data breaches: it’s important to understand that there is generally a bad actor behind these attacks. And these bad actors are seeking the least resistant means of ingress into networks.

\[\text{Area} \quad \text{Data Breach Costs Per Record} \]

<table>
<thead>
<tr>
<th>Area</th>
<th>Data Breach Costs Per Record</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTHCARE</td>
<td>$380</td>
</tr>
<tr>
<td>FINANCIAL</td>
<td>$336</td>
</tr>
<tr>
<td>SERVICES</td>
<td>$274</td>
</tr>
<tr>
<td>LIFE SCIENCE</td>
<td>$264</td>
</tr>
<tr>
<td>INDUSTRIAL</td>
<td>$259</td>
</tr>
<tr>
<td>TECHNOLOGY</td>
<td>$251</td>
</tr>
<tr>
<td>EDUCATION</td>
<td>$245</td>
</tr>
<tr>
<td>TRANSPORTATION</td>
<td>$240</td>
</tr>
<tr>
<td>COMMUNICATIONS</td>
<td>$239</td>
</tr>
<tr>
<td>ENERGY</td>
<td>$228</td>
</tr>
<tr>
<td>CONSUMER</td>
<td>$196</td>
</tr>
<tr>
<td>RETAIL</td>
<td>$177</td>
</tr>
<tr>
<td>HOSPITALITY</td>
<td>$144</td>
</tr>
<tr>
<td>ENTERTAINMENT</td>
<td>$134</td>
</tr>
<tr>
<td>RESEARCH</td>
<td>$123</td>
</tr>
<tr>
<td>PUBLIC SECTOR</td>
<td>$110</td>
</tr>
</tbody>
</table>

\(^1\) Data Risk in the Third-Party Ecosystem, Ponemon Report, 2017
A third party is any entity external to a company, typically referred to as a vendor, partner, or business associate. Most businesses, no matter the size, use third parties for essential business-critical solutions. In short, a third party is any external business-critical service provider retained by an enterprise or institution. In the healthcare industry third-party vendors are known as business associates (BAs). The HHS (The U.S. Department of Health and Human Services) defines a BA as a “subcontractor that creates, receives, maintains or transmits protected health information on behalf of another business associate.”

The interactions with BAs and healthcare entities are essential to operations within the industry. BA remote access solves problems for both the external vendors and companies needing access to networks or services. Most day-to-day operations in the industry would cease to function without some level of BA remote access, the most common being remote desktop access, or a similar critical support functionality. However, it is risky for a healthcare enterprise or institution to allow their BAs full or unlimited access permissions to a network. The Ponemon Institute has indicated that data breaches caused by unsecured third-party access are at an all-time high and rising.

Because healthcare data is a prize for hackers, and third-party remote access is quickly becoming the easiest attack surface, locking down your BA remote access is essential.

**EXAMPLES OF BUSINESS ASSOCIATES**

- A third-party administrator that assists a health provider
- A CPA firm whose accounting services to a healthcare provider require access to PHI
- Consultants or technical personnel
- Legal support or entities

© 2020 SecureLink, Inc
Understanding Compliance in the Healthcare Industry

According to a SecureLink-sponsored report, compliance with industry regulations, securing third-party access, and securing privileged credentials are the top priorities for managing secure access. The same report indicates that of the surveyed enterprises, “assurance that third parties are complying with security policies and requirements is the biggest challenge to healthcare enterprises.”

We need to talk about compliance... or what we talk about when we talk about compliance.

**HIPAA**

**HITECH**
The Omnibus Rule implemented a number of provisions of the HITECH Act to strengthen the privacy and security protections for health information under HIPAA and finalized the Breach Notification Rule. The HITECH Act requires BAs to comply with all provisions found within HIPAA, in addition to making BAs liable for noncompliance. The act requires BAs to comply directly with the HIPAA Security Rule provisions directing implementation of safeguards for PHI.
Everyone Benefits from HIPAA Compliance

Because of the rules implemented in HIPAA and the further BA requirements found within the HITECH Act, it behooves both covered entities and BAs to regularly check their systems to ensure compliance.

This interactive checklist represents a few essential components necessary to ensure your network setup is HIPAA compliant and that ePHI is protected. This checklist is composed of general checks your organization should have in place to aid you with your HIPAA compliance goals.

Improve Compliance and Mitigate Liability

- Identify gaps in information system activity review and ensure vendor adherence to enterprise policies
- Aid inventorying of remote access systems and vendor representatives
- Identify remote access control gaps

HIPAA and HITECH Compliance Checklist

**ACCESS CONTROL/ UNIQUE USER IDENTIFICATION/ AUTOMATIC LOG-OFF**

- Multi-factor authentication and increased defense-in-depth credential vaulting
- Unique username and password combination for all logins
- Restrict access as to time, scope, function, and application
- User, group, and role-based access controls
- Unilateral ability to terminate a session at any time
- Configurable time periods for automatic log-off after inactivity

**AUDIT CONTROLS**

- High-definition session recording
- Comprehensive system logging and user activity

**DATA INTEGRITY**

- Strict control of remote access to limit support related data corruption
- Detailed audit to identify changes and enable corrections

**TRANSMISSION SECURITY**

- Customer configurable encryption
- AES 128, 192, and 256-bit modes
- FIPS 140-2 encryption module employed by default
What Makes the Healthcare Industry a Target?

Healthcare organizations and business associates believe they are more vulnerable than other industries to a data breach. The majority of both healthcare organizations and BAs have not invested in the technologies necessary to mitigate a data breach, nor have they hired enough skilled IT security practitioners.

An overwhelming majority of healthcare organizations (69%) and BAs (63%) believe that they are at a greater risk than other industries for a data breach.3

In addition, 59% of healthcare organizations and 60% of BAs do not think, or are unsure, that their organizations security budget is sufficient to curtail or minimize data breaches. Similarly, more than half of healthcare organizations, or 56%, do not believe their incident response process has adequate funding and resources.

Insiders within BA organizations are a root-cause of medical identity theft. Of BA respondents, 74% say they are not aware or are unsure of any medical identity theft affecting their patients. Of the 26% who say they know about medical identity theft, the most often observed cause was intentional but non-malicious employee action were responsible for 33% of total data breaches. Unintentional employee action and malicious insiders were responsible for 20% of reported data breaches.

© 2020 SecureLink, Inc

3 Third-party access is a major source of data breaches, yet not an IT priority.
Ransomware: Recent Targets, Recent Costs, and Risks

In 2017 and 2018, PHI and ePHI became the new prize for hackers; this, alongside recent ransomware incursions, makes the threat to Covered Entities a danger that cannot be ignored. Further, if Covered Entities are a target, so too are their associates and BAs.

In January of 2018, a ransomware attack on Hancock Health occurred. Steve Long, the President and CEO of Hancock Health, penned a rare open letter that details the four harrowing days of the attack. He states they believe the attack originated in Eastern Europe and utilized credentials of a BA to install malware on their systems. Mr. Long shares his response and the costs associated with getting his enterprise back online.

Despite the admirable candor found in his open letter, he neglected to speak to how preventable this attack could have been given proper security and preparedness.

DataBreaches.net reported that FastHealth, a vendor for many healthcare facilities, was the victim of an attack that affected more than 9,000 patients. FastHealth was notified by law enforcement of a breach on their web servers. This is particularly worrisome because internal auditing or oversight did not reveal the breach, rather it was discovered by law enforcement. This demonstrates that BAs are equally responsible for maintaining security; it does not all fall to the covered entity. Compliance is the responsibility of all parties.

A December 2017 Mimecast survey indicated that “Preventing Malware and Ransomware,” was a top initiative for respondent’s data and cybersecurity. Among survey respondents, 78% of provider organizations had dealt with ransomware, malware, or both in the previous 12 months.

Healthcare data is the new prize for hackers.

It is important to note that ransomware infections are considered HIPAA data breaches and must be reported as such.

\footnote{The Cyber Attack—from the POV of the CEO}
Risks of getting Third-Party Remote Access Wrong

FINES
The costs of healthcare breaches has eclipsed all other data breach costs.

LIABILITY
According to IBM and Ponemon, healthcare data breaches are the highest among surveyed sectors, the average cost of a data breach is $3.62M, or about $380 per record.

LOSS OF TRUST
In the same Ponemon study, 31% of consumers survey said that they discontinued a relationship with the affected organization after a breach, and 65% reported a loss of trust in organizations affected by one of more data breaches.

LOST MONEY
In a survey of 113 publicly traded companies tracked for 30 days before a breach, and 90 days after a breach, the average share value fell 5%.

HARM TO PATIENTS
A researcher at Vanderbilt University claims more than 2,100 patient deaths a year may be attributable to data breaches.

Five steps to mitigating risk

STEP 1
Assess your current access
Determine who has access to your network
Assess their necessary permissions

STEP 2
Evaluate your current policies
Determine how BAs gain access
Determine necessary permissions for each user

STEP 3
Define your BA access needs
Document all vendors with access to PHI
Execute Business Associate Agreements with each to mitigate liability

STEP 4
Identify gaps in compliance
Once gaps are identified, institute employee compliance education
Create and implement policies to ensure employee and vendor understanding

STEP 5
Correct any gap in liability
Implement remediation plans to reverse any potential HIPAA violations
Establish plans for secure remote access to protect PHI

© 2020 SecureLink, Inc

7 Healthcare Data Breach Costs Highest for 7th Straight Year 8 “Study: How do Data Breaches Impact Reputation?” 9 “Study: Hospital data breaches tied to thousands of additional patient deaths”
Choose the Right Secure Remote Access

A 2018 threat assessment report published by Rapid 7 research, and supported by data from Trustwave and Ponemon reports, indicates that healthcare is pulling away from other industries as a focus for attacks. The data also shows that a large number of the attack vectors used to execute malicious attacks (e.g. ransomware, PHI theft, or denial of service attacks) are centered around remote access. These remote access weaknesses include suspicious logins, access attempts from disabled accounts, shared credentials, and account leaks.

Remote access makes doing business convenient and is necessary for BAs to conduct business with Covered Entities. However, with necessity can come vulnerability. Because unsecured remote access is quickly becoming the main attack vector, this guide provides information which will help Covered Entities and BAs create remote access solutions without compromising efficiency, security, or compliance.

10 “Rapid 7 Quarterly Report: Q2 2018”
About SecureLink

SecureLink is the leader in managing secure vendor privileged access and remote support for both highly regulated enterprise organizations and technology vendors. More than 30,000 organizations across multiple industries including healthcare, financial services, legal, gaming, and retail rely on SecureLink’s secure, purpose-built platform. SecureLink is headquartered in Austin, Texas.

securelink.com | 888.897.4498 | contact@securelink.com

© 2020 SecureLink, Inc. All Rights Reserved.