Don’t Be the Next Headline! PHI and Cyber Security in Outsourced Services.

June 2017

Melanie Duerr
Fazzi Associates
Partner, Director of Coding Operations

Jami Fisher
Fazzi Associates
Chief Information Officer

Don't Be the Next Headline! PHI and Cyber Security in Outsourced Services.

The purpose of this white paper is to help agencies understand and mitigate the risks of PHI data breaches and cyber security attacks in outsourced services. It covers:

- The trend of increased outsourcing.
- The risks surrounding PHI and cyber security when outsourcing back office functions.
- How to mitigate those risks in order to take advantage of the benefits of outsourcing.

Outsourcing Trends in Home Care and Hospice

Outsourcing is not new to this industry when you consider that most agencies use vendors for Home Health and Hospice CAHPS and outside payroll services. But with today's unprecedented regulatory and payment complexities and pressures, more and more agencies are outsourcing additional back office functions.

According to the 2016-2017 National State of the Industry Report™, agencies have moved to outsourcing to "reduce cost, increase sophistication for specific functions, ensure 24/7 operations and avoid the growing challenges of turnover and staff shortages."

The study also provides these data points:

- 29% of agencies are outsourcing part or all of their coding, a number that has more than tripled since the previous study in 2014.
- Agencies that used outsourced coding had significantly higher quality scores than agencies that did not.
- 15% of agencies are outsourcing their billing function.
- 58% of agencies have an online training system or learning management system (LMS).

As the industry continues to move toward a pay-for-performance model and experience the escalating staffing crisis, to name a few of our collective challenges, the trend of increased outsourcing is likely to continue.

The Risks of PHI Breaches and Cyber Security Attacks

The HIPAA Privacy Rule accommodates the longstanding and increasing use of outsourced services in healthcare. In fact, according to HHS.gov, "…most health care providers and health plans do not carry out all of their health care activities and functions by themselves.... The Privacy Rule allows covered providers and health plans to disclose protected health information to "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule." (45 CFR 164.502(e), 164.504(e), 164.532(d) and (e))[i]

That's the good news. The bad news is that according to the Ponemon Institute, "only 53% of business associates agree that policies and procedures are in place to effectively prevent or quickly detect unauthorized patient data access, loss or theft." Further, that same study reported that nearly 90% of healthcare organizations have suffered a data breach in the past two years and "criminal attacks from the outside and negligence from the inside continue to put patient data in the crossfire." [ii]

The financial and reputational costs of HIPAA breaches are extremely high. The HIPAA Enforcement Rule governs the investigations that follow a breach of ePHI. The penalties that could be imposed on covered entities responsible for an avoidable breach of ePHI include:

Maximum Possible fines for HIPAA Violations

Violation	Fines Per Violation	Maximum Fine
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect - (Corrected)	$10,000 - $50,000	$1,500,000
Willful Neglect - (Uncorrected)	$50,000	$1,500,000

And that's just the beginning. Once you add in the costs for investigation of how the breach occurred, remediation to ensure that the problem is fixed, notification to patients, credit monitoring or medical identity theft protection for those affected; the average cost of a data breach for healthcare organizations is estimated by the Ponemon Institute to be more than $2.2 million. Lastly, these costs do not include losses due to a damaged reputation.

Mitigating Risks When Outsourcing

The statistics and risks described above suggest the need for agencies to conduct due diligence to make sure their outsourcing partners have the proper policies, procedures and systems to keep PHI and all data safe and secure. Asking the following questions will help agencies assess their vendors' capabilities to do so:

- What are your policies and procedures for safeguarding data, including incident response?
- Do you utilize two-factor authentication for access to data?
- Is data encrypted at rest including with laptops and mobile devices?
- Is data encrypted in motion?
- Is email encrypted?
- What type of regular user account reviews do you conduct?
- What is your backup and disaster recovery plan?
- What is your patch management plan?
- Does staff have access to personal e-mail, sync and share applications, clipboard transfers or social media?

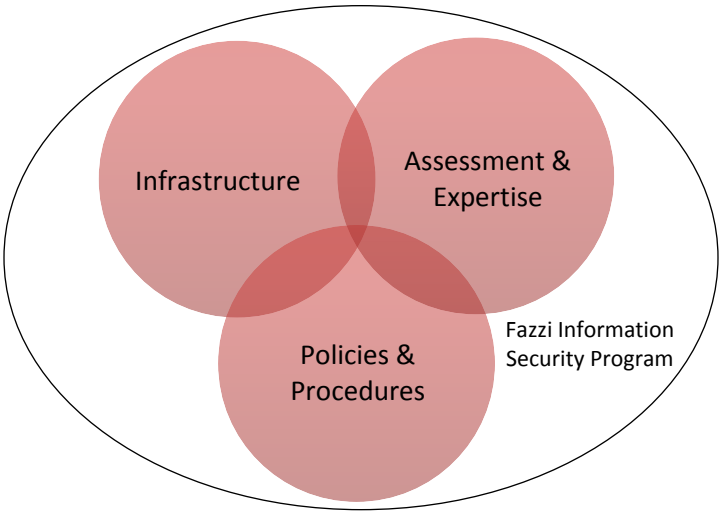
Once you have conducted a proper security assessment and are satisfied that a vendor is capable of keeping your data secure, you need to make certain that you have a proper and signed Business Associate Agreement (BAA) with that entity.
HHS provides a complete explanation of and sample language for a BAA here:
https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html

For further explanation and detail of a highly secure outsourced services platform, we can describe our own as an example.

At Fazzi our Information Security Program is built within the ISO 270001 framework and on these pillars: Assessment and Expertise, Policies and Procedures and Technology and Infrastructure.

Assessment and Expertise

We have assembled our own in house team of highly qualified Information Technology (IT) experts. Additionally, our team works with outside experts in the field to ensure that we stay up to date with new developments – and – new threats. Together these experts regularly inventory, assess and test every aspect of our IT systems and business processes for information security.



Policies and Procedures

Fazzi's security program meets the most rigorous demands in the industry including HIPPA and state regulations, HITECH (Health Information Technology for Economic and Clinical Health Act) and ISO 27001 which is one of the most rigorous information security standards in the world.

Our written policies embody these regulations and standards and bring them to life in how we handle client data in motion, at rest and over time. PHI is always encrypted in transit using the strongest ciphers available. All PHI and working documents stored on our servers are encrypted on disk and retained only per policy. Fazzi is prepared to respond to disasters with planned procedures defined in the Disaster Recovery plan. Further, per our policies, we regularly train our staff on fraud and abuse and information security.

Technology and Infrastructure

Fazzi uses desktop virtualization and a suite of security technologies to protect PHI. With this system, all PHI is encrypted at rest and in motion. Access to data is managed centrally no matter where the work occurs. Data never leaves our data center in Atlanta or our disaster recovery back up site in Phoenix.

These data centers are certified for SSAE/16 Type II, PCI DSS and HIPAA.

These policies and infrastructure enable Fazzi to protect PHI throughout the entire outsourced services workflow, from the agency's EMR system, to the Fazzi data center, to the staff performing the work and back again. Our outsourced services staff launch a secure virtual desktop session in the data center and only the keyboard, mouse and video display are served. A secure encrypted file share is provided for working documents. Personal email, 'sync and share' (e.g. Dropbox), social media and clipboard transfers (cut/paste) are blocked.

From the virtual desktop, our staff connects to the agency EMR system. This connection can take one of many forms. Fazzi can support all major secure connections including Citrix, HTTPS/SSL, RDP and site-to-site tunnels. In this way, PHI is protected throughout its lifecycle in the Fazzi infrastructure and business process.

For further information, please contact info@fazzi.com or 800-379-0361.

---

[i] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html?language=en

[ii] Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data by Ponemon Institute published May 2016