Cyber Security & You as a TPA

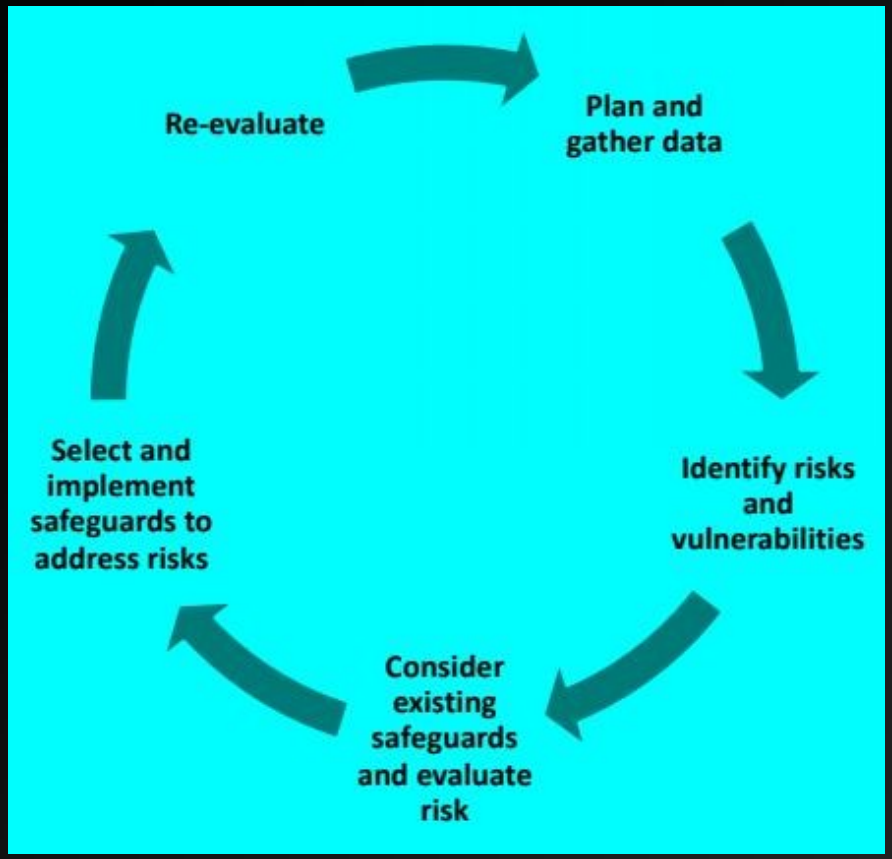
Your organization as a Third Party Administrator (TPA) is legally responsible for the security of Protected Health Information (PHI) and Personal Identifiable Information (PII), both, in your possession and or transiting through your organization; in electronic data or paper format.

Because of the volume of PHI & PII in your organization, you are a target; it is only a matter of "when". By Federal and State Regulation, you must have in place a highly developed assessment plan that is responsive to:

- Before and after risk assessment,
- High level operational considerations, and,
- High level organizational inquiries

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

Risk Assessment Guidelines



1. Does your organization have such guidelines or a plan?
2. Is it in writing?
3. Are you able to produce it at a moment's notice?
4. Has it been independently evaluated and tested recently?

If any of the above are answered with a "No", PLEASE consider the legal, regulatory and financial implications to your organization

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

Some Statistics For Your Consideration

(available at the National Privacy Rights Clearinghouse)

From mid-September 2009 to mid-February 2018:

- There have been 8,064 reported cyber incidents
- 3,980 of them attacked the health care industry, 49.36% of the total
- 81 of these 3,980 occurred between January 1st and February 17th of 2018

Because Of The Volume Of PHI & PII In Your Organization

You Are A Target

It Is Only A Matter Of "WHEN"

Attempts have been made to rationalize this cyber-health care problem

All have ultimately failed to the financial detriment of

The organization and the Consumer

BLUEFIRE RISK CONSULTANTS, LLC.

CONSULTANTS & ADVISORS

A Recent Event

(published by and obtained from a large insurer)

DESCRIPTION OF EVENT: A TPA firm outsourced the storage and protection of its data records to a third-party service provider without a clear Business Associate Agreement (BAA). Subsequently, the service provider's network was breached, and outsiders were able to obtain unauthorized access to PHI and PII of over 1,000 individuals. A class action was ultimately filed against the TPA, alleging failure to protect the PHI, failure to adhere to the firm's network security and written privacy policy, failure to timely notify the individuals affected about the breach, and, failure to properly retain and oversee a viable third-party service provider. (NOTE: All of these are current regulatory requirements, non-comformance brings heavy fines).

RESOLUTION: The TPA incurred $200,000 in expenses associated with notifying the individuals affected, in changing account numbers, establishing a call center and retaining independent counsel to assess notice and compliance obligations (all mandatory). In addition, the firm afforded the affected individuals with monitoring and restoration services for two years following the breach at a total cost of $50,000. Further, after incurring approximately $100,000 in legal defense costs, the class-action lawsuit was resolved for $950,000.

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

Another Recent Event

(published by and obtained from a large insurer)

DESCRIPTION OF EVENT: A rogue employee improperly accessed PHI and PII data of a TPA firm. The employee acquired and sold some of the PHI on the black market before being apprehended by law enforcement. Thereafter, several cases of identity theft were perpetrated against the firm's clients.

RESOLUTION: The TPA firm engaged a forensics investigator and outside compliance counsel. It also notified clients of the breach, established a call center and provided monitoring and restoration services to impacted clients (all mandatory). Costs associated with the event totaled $375,000.

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

And Yet Another Recent Event

(published by and obtained from a large insurer)

DESCRIPTION OF EVENT: An employee of a TPA had a business laptop stolen from his personal residence. The laptop did not include any clients' PHI or PII, however, it was not encrypted; it failed to contain password protection and thereby the thief was able to obtain access to the TPA's network and subsequently the PHI and PII data for more than 7,500 clients. The breach also included clients' business and proprietary information. After providing notice to the clients regarding the theft, a number of lawsuits were filed against the firm for negligence, invasion of privacy and breach of contract.

RESOLUTION: The TPA incurred $1 million in expenses in notifying clients about the theft of PHI, PII and business and proprietary information, changing account numbers, hiring a public relations firm, establishing a call center, and retaining independent counsel to assess notice and compliance obligations (all mandatory). The TPA also afforded clients with monitoring services for a year following the theft, for an additional $150,000. Finally, after incurring approximately $250,000 in legal defense costs, the lawsuits against the firm were resolved for an additional $2 million, the most significant aspects of which were driven by the theft of PHI and PII data.

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

Threats Landscape

Health care and those who provide services or infrastructure to the industry are vulnerable to a variety of cyber attacks. Among the top aggressively trending are ransomware attacks and data breaches, which have recently thrown organizations of all sizes into financial, administrative and operational disarray for weeks to months.

- Malware/Ransomware: During a malware attack, hackers infiltrate systems and networks via harmful software that is intended to damage or disable the system's components. In the case of ransomware, the perpetrators often encrypt and hold accessed files, demanding a ransom to decrypt the data.

- Data breaches: Next to malware, data breaches are among the most common attacks perpetrated against health care organizations and those that serve them. A single attack can put in jeopardy millions of HIPAA protected records.

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

An Infamous Quote Brought Current

"I rob banks because that's where the money is"

Infamous bank robber, Slick Willie Sutton

"I hack for personal health and identifiable information because that's how I can get other peoples' money with impunity"

Yet to be named hacker

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

Why Bluefire

- If your organization already has prescribed secure protocols in place, we will coordinate with your IT Department to examine and report potential vulnerabilities, perform the required audits and, if in conformance, provide you with an independent certification of regulatory compliance.

- If you do not have secure protocols in place or you have some concerns, we will work with you to identify your areas of concern and plan and develop protocols to prioritize and mitigate cyber risk; we will further plan and develop integrated solutions and processes to stay ahead of cyber risk, implement the plan(s) you approve and train your executives and workforce to further enhance your data security.

- If you require and opt for, we will continuously monitor the progress of your data security protocol(s) and manage and track emerging threats.

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS

Thank You For Considering Us

Please visit our home at
BFRisk.com
to learn more about
what we can do for you
and to make a
direct, private and secure contact
with us

BLUEFIRE RISK CONSULTANTS, LLC.
CONSULTANTS & ADVISORS