PARKER | SMITH | FEEK

COMMERCIAL INSURANCE
EMPLOYEE BENEFITS
PERSONAL INSURANCE
RISK MANAGEMENT
SURETY

HEALTHCARE PRACTICE GROUP

AUGUST 2015

WASHINGTON STATE'S DATA BREACH NOTIFICATION LAW CHANGES (HOUSE BILL 1078) AND DATA BREACH FIDUCIARY RESPONSIBILITIES FOR HEALTHCARE ORGANIZATIONS

Effective July 24th, 2015, Washington State law H.B. 1078 amends the State's data breach notification statue. The amendment:

- Expands the statute to cover breaches of non-computerized data (hard copy data – which almost every business still houses)
- Imposes a 45-day deadline for notification of affected consumers (as opposed to 60 days previously)
- Mandates the notification of Washington State Attorney General for breaches larger than 500 Washington state residents
- Introduces a safe harbor for personal information that is secured or encrypted in a manner that meets or exceeds the National Institute of Standards and Technology (NIST) requirements

These changes are important for management and directors of healthcare organizations to know, especially as the number of data breaches continues to increase (per the Identity Theft Resource Center). Whether it be personal healthcare information, SSN's, or credit card information, understanding what is classified as secured (per the National Institute of Standards Technology) how to properly notify the appropriate parties, and what can be counted as an official breach is critical. For healthcare organizations, fiduciary responsibility of personally sensitive information storage is two-fold:

1) As a covered entity, for employee health plans and personal data and
2) For third party liability of patients' personal data

To ensure proper data breach response preparedness (and to show proper due diligence), your directors and leadership staff should be asking I.T. and key partners the pertinent questions now, before a breach occurs:

- Have we ever had system penetration testing done, and have we reviewed the results?
- Do we have adequate I.T. security policies in place?
- Are we using updated operating systems to help manage electronic medical records?
- Who would be working as our forensic team, post-breach?
- Do we have a breach response plan in place? A public relations firm to deal with the blowback after an attack occurs?
- Do we have sufficient cyber/data liability insurance coverage to mitigate the legal, reputational, and credit monitoring costs? And if we don't carry insurance coverage, will our current finances be sufficient to cover such costs when we have a data breach?

Proper documentation of these internal conversations (via minutes) and actions (i.e. having readily available system penetration testing results and documenting the actions shoring up weaknesses) will help defend the organization in federal and civil lawsuits, post-breach. It is important to note that historical lawsuits have shown that directors are not required to be experts in this area, but that they do need to rely on outside experts or expert internal management for advice when addressing these issues. The Ponemon Institute indicates that 90% of healthcare organizations had exposed their patients' data or had it stolen in 2012 and 2013.

The ever-changing requirements in data breach notification requirements within Washington State, continued increase in the number and severity of cyber attacks, and increase in the size of federal lawsuit judgments make this an important topic which needs to be addressed by healthcare organizations, both large and small. Partnering with a well-versed risk consultant who understands both the pre and post cyber breach actions necessary to defend your organization will provide better organizational resiliency when your organization is attacked.

Should you have any questions about data liability and the impact a breach will have on your healthcare organization, feel free to contact one of our cyber liability experts here at Parker, Smith & Feek:

Michael Reph
425.709.3724
mjreph@psfinc.com

Ryan Roberts
425.709.3786
reroberts@psfinc.com

We are committed to developing a thorough understanding of our clients' objectives, the nature of their business, their exposures to risk, and communicating alternatives available to them in a continuously changing insurance and risk transfer marketplace.

Parker, Smith & Feek's Healthcare Practice Group focuses on segments within the healthcare and biomedical industries. Our experience in professional liability and directors and officers insurance is unparalleled among other brokers. We collaborate with healthcare organizations and providers to identify areas of risk and assist in facilitating solutions to meet risk financing needs. While clinical operations often receive much of the organization's focus, we recognize that all of its operations - strategic, human capital, technology, legal/regulatory and financial – need to be considered when identifying exposures and evaluating risk financing options. We believe our value as insurance brokers is to find our clients the best market options available and to work collaboratively to implement risk management practices to avoid and control losses.

CLIENTS SERVED

- Hospitals
- Assisted living & independent long-term care
- Clinics
- Community health centers
- Mental health facilities
- Medical equipment manufacturers
- Healthcare non-profits
- Pharmaceutical companies