WWW.TROJANONLINE.COM

TROJAN TODAY

VOLUME 20 ISSUE 08 AUGUST 2018

A NEWSLETTER FOR CLIENTS OF TROJAN PROFESSIONAL SERVICES, INC.

INTRODUCTION TO PROTECTED IDENTIFIABLE INFORMATION

by Debi Carr

Protected Identifiable Information, or **PII** for short, is any information that could be used to identify an individual. Forty-eight states now have privacy laws that require all businesses to protect a consumer's Protected Identifiable Information. This is already established in healthcare, as we are required to safeguard patients' Protected Health Information or PHI. Any information, or combination of information, that could possibly be used to identify individuals should be protected.

Healthcare entities have been required to secure patient PHI since 1996 under the Health Insurance Portability and Accountability Act. However, considering recent data breaches such as those with Equifax and Uber, forty-eight states and three territories have enacted privacy laws meant to protect general consumers; and the other two states can't be far behind.

continued on page 2 • • •

previous page

What is considered Protected Identifiable Information? Any information that could identify or locate an individual. In most states, this is considered the First Name or Initial in combination with any of the following:

- Address
- Phone Number
- SSN
- Account Numbers
- Email Address
- DOB
- Vehicle Information
- Digital Signature
- Any Medical Records
- Fingerprints
- Any Physical Image
- Retina Scans
- Iris Scans
- Etc.

This trend in data privacy protection brings a new level of vulnerability to medical practices. Protocol states that in the event of a theft or data breach that compromises PHI, the practice must report to the Office of Civil Rights. The fines for failing to safeguard this sensitive information can be up to $50,000 per record. Now, because most medical practices are also considered by states to be businesses, sensitive information is also treated as PII. This means the state government can fine and, in some cases, impose jail time when an executive (Doctor) fails to safeguard and report a data breach in a timely manner.

To complicate the issue further, several states strive to protect their citizens beyond state lines. For example, if you are a New York resident but you visit a business or medical practice in Florida that experiences a data breach, said practice is required to notify you in accordance with both Florida laws and New York laws.

Practices that have patients that primarily reside within the European Union may be subject to the newly enacted General Data Protection Requirements or GDPR. This requires that any business providing services to EU residents, including healthcare providers, will insure that adequate security controls are in place. This includes data encryption at rest and in transit, backups, redundancy, and intrusion detection mechanisms to ensure data is not compromised in any way.

Cyber-attacks are quickly becoming the new battleground, and risks will only increase as new technology is introduced. As a result, businesses, including healthcare entities, must implement a comprehensive security plan. This requires a well-educated team, recognized security controls, and continuous system monitoring and training. The consequences of failing to protect PHI and PII could be too great to recover from.

Debi Carr *is the CEO of D.K. Carr and Associates, LLC, a Security and HIPAA Consulting Firm. She has over 23 years of dental practice management experience and over 30 years of experience in technology and security. She assists dentists in obtaining and maintaining HIPAA compliance including performing annual risk analysis and team security awareness training. She also leads a team of security professionals that respond to cyber-attacks.*

FMI: *844-352-2771 or www.dkcarr.com.*

next page