What is Your Small Business Doing to Protect Non-Public Personal Information?

August 2nd, 2012 | No Comments | Posted in General

By: John S. Pitts

tekcetera
making technology click™

Information security has become an increasingly hot topic in the media. Businesses are working to implement protective measures that ensure both company and employee non-public personal information (NPI) stays private, as its dissemination could have negative effects.

Not familiar? NPI data falls into four categories: individual personal information, corporate and individual financial information, personal educational information and personal medical information. All information is protected from disclosure by both state and federal laws. Not sure what type of information falls into these categories? Check out a few examples below:

- **Individual Personal Information:** Have you ever provided your bank account number for direct deposit? Social security number for tax purposes? Date of birth for employee identification? Then, your employer is holding individual personal information that is protected under NPI laws. What could happen if this information wasn't protected and were to be leaked? Your bank account could be drained, your identity stolen and government records jeopardized.
- **Corporate and Individual Financial Information:** Financial institutions collection personal financial information from clients in the course of doing business. However, not only can financial NPI impact individuals, but the dissemination of financial information on a corporate level could have an impact on the company's stock and lead to claims of insider trading. Additionally, under new laws, CEOs of financial institutions can now be held personally accountable for NPI leaks.
- **Personal Educational Records:** Schools and higher education institutions keep highly sensitive records of students. Under the Family Educational Rights and Privacy Act, these records are protected from public disclosure and may not be disclosed to third parties unless an exception exists, such as transferring schools, law enforcement and judicial order or subpoena. Imagine if this information were to be made public, it could jeopardize an individual's future career and education. Additionally, student records also include data covered under the individual personal information category like social security numbers.

- **Personal Educational Records:** Schools and higher education institutions keep highly sensitive records of students. Under the Family Educational Rights and Privacy Act, these records are protected from public disclosure and may not be disclosed to third parties unless an exception exists, such as transferring schools, law enforcement and judicial order or subpoena. Imagine if this information were to be made public, it could jeopardize an individual's future career and education. Additionally, student records also include data covered under the individual personal information category like social security numbers.

- **Personal Medical Records:** All patient medical records fall under NPI protection whether maintained by physician, hospital, ancillary service, business service or insurance company. Curious how this can impact your professional life? Imagine if your company's insurance agency leaked all your employee's medical information, from test results to physician visits, and it suddenly popped up on your company's shared drive.

As a business owner, one of my most important security objectives has been to implement measures to keep NPI secure. I have always wondered why employers would risk a data theft or breach when there are simple ways to protect data. How can your business ensure that it is doing its part to stay secure?

- **Use Firewalls:** With the increasing number of computer hackers and identity theft victims, it is imperative that you provide your company with reliable protection by using firewalls. These can either be software-based or hardware-based and are used to help keep a network secure. Ultimately, firewalls analyze data packets and determine what information should be allowed through, based on a predetermined rule set.

- **Implement Virtual Private Networks:** Virtual Private Networks (VPN) provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a head office network through the public Internet.

- **Employ System Monitoring:** A system monitor is hardware- or software-based and used to monitor resources and ensure that non-public files are not being shared without consent. It provides security for you, your employees and your business by observing computer activity on a 24-hour basis.

- **Impose Specific Confidentiality Obligations:** These obligations can be highlighted in confidentiality letters, agreements and notices – whether it is on documents, faxes or emails. In doing this, you establish an understanding with your employees, as well as any other third party, as to the seriousness of confidentiality in the workplace.

- **Screen, Inspect and Protect Your Email:** We use WatchGuard® XCS at Tekcetera, it delivers supreme email security and controls the traffic entering and exiting your company's email networks. Its main function is to act as a perimeter protector.

What does your business do to protect NPI? Leave a comment below and share your best practices.

###