Patient Data Security

4 Ways to Protect Your Organization from a Data Breach
It’s a treasure trove of personal data.

The proverbial pot of data gold. For every patient who walks in, a hospital collects the following information, at minimum: name, phone number, address, SSN, date of birth, occupation and insurance information. It is all maintained meticulously and kept up to date. And it makes hackers salivate.

Healthcare is the new cyber fraud frontier, and the personal patient data that hospitals have readily available is more lucrative, more comprehensive, and more attractive than retail and banking data ever was. This is why fraud perpetrators spent months assaulting Anthem/BlueCross BlueShield, stealing more than 90 million records, continuously, over the course of 4-6 months. It was a hacker’s dream, and a healthcare organization’s worst nightmare.

90% of healthcare organizations experienced a breach within the past year

Hospitals work tirelessly to ensure patient privacy in the physical world, but privacy threats are increasingly leaving patients standing in the cold without a hospital gown in the digital domain. Cyber fraud attacks on patient privacy leave healthcare organizations vulnerable. Unfortunately, it’s not a question of if a data breach will happen, but when a data breach will happen.

What can you do to prepare? Here are four ways to protect your healthcare organization from a data breach.
1. Have greater insight into what’s really happening

Know what your users are doing. Oftentimes, fraud is committed by people authorized to be in your system. While log files may give you a glimpse into an action taken, they will never provide you with a holistic view of user behavior. For example, when a healthcare worker looks at a VIP patient, a log file may track that they viewed the VIP patient file, but it will not be able to provide any context around whether the worker searched under the VIP’s alias (indicating they may have been reviewing case files to determine treatment) or if they searched for a VIP’s real name (an indicator that the worker was not providing care to that individual, and may have been breaching security). The ability to see everything they did before and after can provide both clarity and context to help you determine whether behaviors are normal or nefarious. Get a tool that gives you complete visibility into what users are doing by having screen-by-screen replay and full accountability of all activity.

Your investigators will have greater insight and confidence into explaining what happened and why – and, the analytics engine will have more valuable data points to find suspicious behavior.
2. Get real-time alerts for suspicious behavior

Have the right tools in place to monitor in real-time. Become truly pro-active by being told something is happening rather than waiting to look. Wailing 24-48 hours to know about a patient privacy violations is too long.

A lot of damage can be done in that period of time, and not getting notified in real-time of potential fraud is the difference between proactively protecting your patient data and being permanently stuck in a reactionary posture.

3. Understand your users through behavioral profiling and analytics

Know the person; know the persona… by profiling the employees against their previous activity and against their peers. The best way to detect a risk is to recognize a change or difference in patterns. Whether someone internally has decided to invade patient privacy, or if your system is being hacked; behavior profiling and analytics allow you to immediately pinpoint anomalies that can raise a flag to suspicious behavior.

Allow me to introduce you to my imaginary acquaintance Jack. Jack signs in every day to your system from 9:15 am when he gets a coffee and sits down at his desk, until about 6pm. Jack normally only works late during end of quarter closing periods. If you know this about Jack, you may think it is strange that Jack is signing in every night from a different IP address, always after midnight, and often looking at employee records that have nothing to do with his end of quarter closing activities.

Without user profiling and analytics, coupled with real-time alerts, you may or may not find out about Jack’s extracurricular activities until days, weeks or even months from the time of the incident. And imagine if it wasn’t Jack at all – what if hackers just took over Jack’s credentials looking for 90 million records.
It took Anthem over 4 months to detect the account takeover that led to this exact scenario. And, it was only discovered by luck after the user became suspicious to a login notification. And, it was possible because there was no insight, into the change of behavior or frequency, to detect the takeover.

68% of patients are not confident their healthcare providers’ security measures will protect their medical records from loss or theft.

4. Empower your investigators

Arm your investigators with the tools needed to keep you and your organization safe from data security threats. Create policies, workflow, and case management that will enable investigators to handle all cases and complaints brought forth, and ensure that you are in compliance with regulatory requirements.

When determining what tools are right for your organization, ask yourself the questions: how can our organization help investigators be more effective and efficient at finding what they need?

Bring a magnet if you want to find the needle in the haystack. Investing in monitoring technology that will capture and analyze user activity across networks and applications, and allow you to find what you are looking for no matter where it comes from or how it got there is critical.
Being able to do so with a google-like search and flexible dynamic reports that allow you to leverage your data, will empower you. Envision the task of finding all the places that a social security number has traveled through your network between systems and/or users. And imagine being able to search for that trail.

When aiming to protect your organization from cyber fraud, including threats from trusted and authorized employees, cast a net wider than simply trying to prevent a breach: protecting your organization means securing your data, monitoring and analyzing your user behavior and safeguarding your organization from the legal implications of any suspicious behavior (attempted or realized).

Is your privacy data and security solution able to stand up to the evolving threat landscape? Find out how you can stay ahead with this informative video.

To learn more about privacy data and security solutions, visit Bottomline Technologies at www.bottomline.com or contact:

Phone: 800.472.1321
Email: info@bottomline.com

About Bottomline Technologies

Bottomline Technologies (NASDAQ: EPAY) powers mission-critical business transactions. We help our customers optimize financially-oriented operations and build deeper customer and partner relationships by providing a trusted and easy-to-use set of cloud-based digital banking, fraud prevention, payment, financial document, insurance, and healthcare solutions. Over 10,000 corporations, financial institutions, and banks benefit from Bottomline solutions. Headquartered in the United States, Bottomline also maintains offices in Europe and Asia-Pacific.