Bottomline Healthcare

Privacy and Data Security
# Table of Contents

<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>03</td>
<td>The Patient Privacy Challenge</td>
</tr>
<tr>
<td>05</td>
<td>Bottomline Healthcare Privacy and Data Security</td>
</tr>
<tr>
<td>07</td>
<td>How it Works</td>
</tr>
<tr>
<td></td>
<td>Features</td>
</tr>
<tr>
<td></td>
<td>Data Capture &amp; Collection</td>
</tr>
<tr>
<td></td>
<td>Profiling &amp; Alerting</td>
</tr>
<tr>
<td></td>
<td>Investigation &amp; Resolution</td>
</tr>
<tr>
<td>08</td>
<td>Case Study</td>
</tr>
</tbody>
</table>
The number of patient privacy threats and the resulting costs are skyrocketing.

Attackers, whether inside or outside your healthcare organization, are using more sophisticated techniques to gain access to sensitive patient information. Additionally, these evolved tactics are difficult for traditional security systems to identify. In order to protect patient data, decision makers must rethink how they approach patient privacy and overall cyber security. Your healthcare organization needs complete visibility into user behavior. Without it, you’re missing a critical line of defense.

You’re only as productive as your tools allow you to be.

Traditional, siloed, and rigid solutions lack the technical sophistication to ward off hordes of fraudsters who are constantly evolving their methods of subterfuge and omnichannel fraud. Unless you adapt, your healthcare organization is at risk.

Criminal attacks in the healthcare industry have more than doubled in the past 5 years.


- Get a complete picture of user behavior across systems.
- Use instant alerts to stop fraud in real time.
- Stay compliant with full data capture, audit, and analytics.
The key to protecting your healthcare organization is in the strategy that defines the tools you employ. More than collect and analyze, you need to be equipped with the visibility and intelligence necessary to act.

Leveraging Intellinx technology, Bottomline Healthcare Privacy and Data Security provides cutting-edge tools to noninvasively monitor and analyze user activity, alert, and resolve fraud before and as it happens, and all from within one dashboard. Going beyond log files and capturing user behavior activity as the attacker breaches, Bottomline solutions aid in protecting patient privacy and ensuring regulatory compliance, and does so quickly.

Rethink your patient privacy strategy.

79%: Percentage of healthcare providers that have had more than one data breach in the past 24 months


$2.1M: The average cost of a data breach for healthcare organizations
Fight for your healthcare organization—and for your patients.

Bottomline Healthcare Privacy & Data Security is uniquely designed to protect both your organization and your patients by managing healthcare risks and compliance regulations. Without relying solely on log files, this solution protects your whole healthcare organization, ensuring that federally mandated private files remain private.
Healthcare is one of the most at-risk industries.

Providers are facing a growing threat to their patients’ privacy and their own reputations.

Malicious insiders who utilize their knowledge of IT systems and controls to manipulate internal systems can cause much greater damage than external parties.

Your patients are depending on you to protect them.

Their data is in your hands. Regulations require healthcare organizations to maintain a full audit trail of access to patient data and report all breaches to the federal government. While doing so takes time and money, it safeguards all parties against fraud. You need a solution that not only protects your healthcare organization, but helps you protect your patients too.

65 million:
The number of patient identities exposed annually.


- Protect patient privacy and your reputation.
- Reduce the risk of non-compliance of HIPAA and HITECH.
- Empower your investigators with complete visual replay and audit trails.
How it Works

Bottomline Healthcare Privacy and Data Security records end-user activity by noninvasively sniffing network traffic. The recorded user sessions and inter-server messages are analyzed and reconstructed in real time, allowing a visual replay of user activity screen by screen. This solution monitors activity on a wide range of healthcare platforms.

With a curated healthcare-tuned rules library, and the ability to create and manage unique lists, Bottomline Healthcare Privacy and Data Security is the next line of defense against privacy threats. Should it detect unusual activity, the solution flags the behavior and creates an alert. An investigator can access and act on any alerts triggered from the Investigation Center.

Additional Features Include:
- Compliance with HIPAA and other regulations.
- Proactive alerts.
- Enforced security policies.

Examples of Rules:

**Employee snooping**
Alert: An employee accesses...
- A co-worker’s record.
- Their own medical record.
- A VIP’s record.
- Patient information from a different location.

**Fraudulent billing**
Alert: An employee changes...
- Information that normally wouldn’t change (e.g., name).
- Bill recipient(s) and prints bill within a short period of time.

**Enforcing access controls**
Alert:
- The same user logs in simultaneously from different systems.
A large northeastern healthcare provider had 14,000 patients’ personal information leaked—including names, addresses, dates of birth, social security numbers, and credit or debit card numbers—by a former employee who accessed billing records outside of normal job duties. This could have been detected much earlier with Bottomline Healthcare Privacy and Data Security—an investigator would have been alerted the moment the employee accessed records that were outside his assigned responsibilities.
01 Data Capture & Collection

Traditional solutions may collect vital data from log files and provide general database analysis, but it's not enough. Log files are time-consuming to analyze and they don't provide the level of insight into all user actions, queries, screen views, and transactions that are necessary to proactively track down and stop fraudulent behavior.

The platform's data capture and collection approach is comprehensive. All data exchanged on the monitored applications across a corporate network is recorded via patented network-sniffing technology and available for viewing and investigation in real time. The solution can capture data from text and binary files, log files, database tables, XML and CSV files, user queries, message queues, and other sources.

Encrypted using 128/256 AES and digitally signed with MD5 and RSA, the recorded data may be acceptable as forensic evidence in the U.S. court of law.
The challenges posed by profiling and alerting involve effectively developing behavior analysis that can identify suspicious behavior, while keeping false positive rates low. Traditional solutions cannot alert on targeted behavioral scenarios, and tend to generate more alerts than a healthcare organization can handle. The platform gets smarter over time, providing better visibility, and generates less false flags and more true potential instances of fraud—resulting in more accurate alerts for your team.

The platform’s data model can maintain static and dynamic data on employees, accounts, and customers. As the system profiles each user or user group, the data is relayed with full transparency to the discerning analytics engine.

The analytics engine applies a risk score to unusual actors, generates immediate alerts, and limits the rate of false positives. The rules and scoring functions can be tweaked and fine-tuned to ensure its continued success.

Dynamic profiling allows the system to learn and adapt, helping to define what activity is normal and what is suspicious.
Due to complexity, system and department silos, limited log capturing, and an overwhelming number of false positives, investigations are difficult to manage.

The Investigation Center is the hub where you can perform all activities in the investigation’s life cycle. It is composed of a set of integrated functions, each assisting the investigators with various facets of fraud investigation and resolution.

---

**Alert and Case Manager:**
Assists investigators in the prioritization and review of captured suspicious activity from beginning to end.

---

**Unique Replay Capabilities:**
Allows investigators to re-watch screens where suspicious activity occurred (even if screens were merely viewed), giving full context into the actions performed.

---

**Cross-Platform Search of User Activity:**
Performs a Google-like search on the content of all screens accessed by users across disparate systems in a given timeline to find, for example, all users who accessed a specific customer account in a specific timeframe.

---

**Link Analysis:**
Visually displays relationships between employees, customers, accounts, and many other parties. Fraudulent entities, or those under investigation, are highlighted to allow further examination.

---

**Control Business Rules:**
Allows investigators to manage the scoring function to reduce false positive rates.
Is your privacy and data 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 and data 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.