Whom Do You Trust with Your Customers' Medical Information?

Make Sure Your Vendors and Providers Are Secure

By Andrew Weaderhorn

Information about us is everywhere. Tracked via computers and transmitted across the Internet, information can be sent around the world with a few clicks on a computer keyboard.

Keeping confidential information private is paramount. This is especially important when it comes to information concerning our health care. Beyond not wanting others to know about our most sensitive information, there are numerous reasons to protect medical records because they contain important data points: private health information, social security number, date of birth, home address, contact information, and medical insurance information.

Medical records are a treasure trove for computer hacks and thieves. They can utilize this information to engage in endless mischief. People who have access to this information should protect your right to privacy and the security of your personal health care information. This includes health care providers and other professionals who receive your medical records.

Threats to Protected Health Information (PHI)

There are countless threats to your PHI, which comes from a variety of sources. These can include:

- Healthcare professionals working inside a facility, company or government entity
- Malware and other malicious programs
- Cybercrime and other data-driven security threats
- Services providers that have access to healthcare information from the people they serve and have daily interactions

These threats are real and will only continue to grow. In 2015, Verizon collaborated with several large accounting and insurance firms to study the impact of PHI data breaches in the United States. This report was entitled the Protected Health Information Data Breach Report.

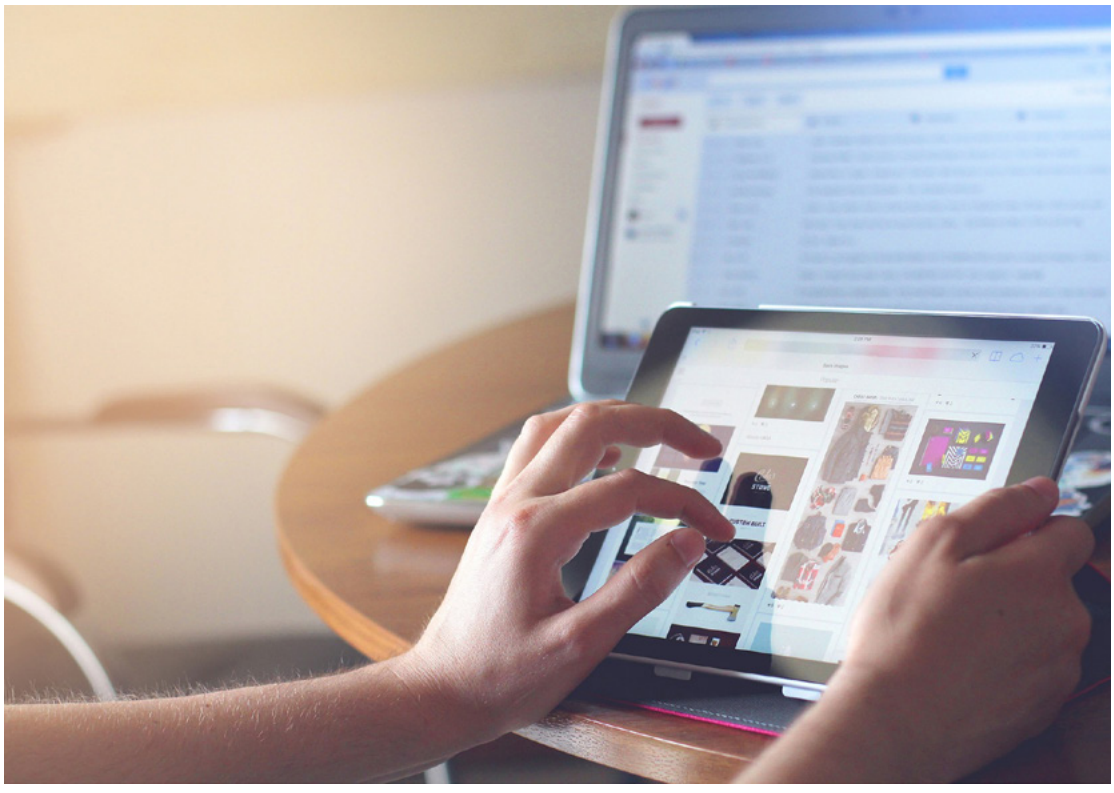
According to the report, "There has been a significant increase in reported data breaches involving PHI every year…and this trend will only continue to increase." It also states that "industries involving healthcare are the most frequently targeted industries to data breach and unauthorized release of PHI… with the most significant reported breaches involving PHI coming from a physical attack from an outside threat." Of the reported instances contained in the report, there were 1,523 incidents involving medical records, with over 217 million known records disclosed in an unauthorized manner.

Security of Data Shared With Vendors

As noted in the Verizon report, data security is a far-reaching problem. Because of this, many companies are making investments and taking proactive steps to focus more on cybersecurity.

The important point to recognize is that data shared with a large organization is also shared with their often smaller third-party vendors. The large, recognized company may have significant investments in cybersecurity; however, the investments in security from their vendor relationships are equally important.

One such example is Target and the 2013 security breach that exposed millions of Americans and their private financial data. All of the details of the attack have not been released publicly, but enough information is available to understand the important lesson.



It was reported in Bloomberg that six months prior to the attack Target began installing a $1.6 million malware detection tool made by the computer security firm FireEye, whose customers also include the CIA and the Pentagon. Target told the Wall Street Journal that the initial intrusion into its systems was traced back to network credentials that were stolen from a third-party vendor.

Multiple sources named the vendor as Fazio Mechanical Services, an HVAC firm. Investigators determined the primary method Fazio used to detect malicious activity on its internal system was a free version of anti-malware software, which was inadequate.

The Target data breach shows that although your systems, or those of a large service provider, may meet the industry standard to provide protection, failure to require third-party vendors to use the same process can lead to huge breaches.

How Do You Ensure Your Data Is Secure?

Risk managers face the question of how to ensure their data is safe in their own organization, as well as with their vendor partners. Best practices dictate to examine and view reports on a service organization's controls over:

- Security
- Availability
- Processing integrity
- Confidentiality of information processed or maintained
- Privacy of personal information the organization collects, uses, retains, discloses, and disposes of

SOC 2, Type 2 Designation

A simple way to ensure these controls are followed is to look for a SOC 2, Type 2 designation. A SOC 2, Type 2 report is a formal audit process completed by a Certified Public Accountant following the quality control standards of the International

Auditing and Assurance Standards Board (IAASB). According to the American Institute of Certified Public Accountants (AICPA), a SOC 2 report is "intended to meet the needs of a broad range of users who need information and assurance about controls at a service organization."

A type 2 report differs from a type 1 report in that "a type 1 report does not include tests of the operating effectiveness of controls and the results thereof; therefore, it is unlikely to provide report users with sufficient information to assess the effectiveness of controls."

The best practices required to achieve a SOC 2, Type 2 designation should play an important role in vendor selection and management, as well as internal security and risk management.

Holistic Approach to Data Security

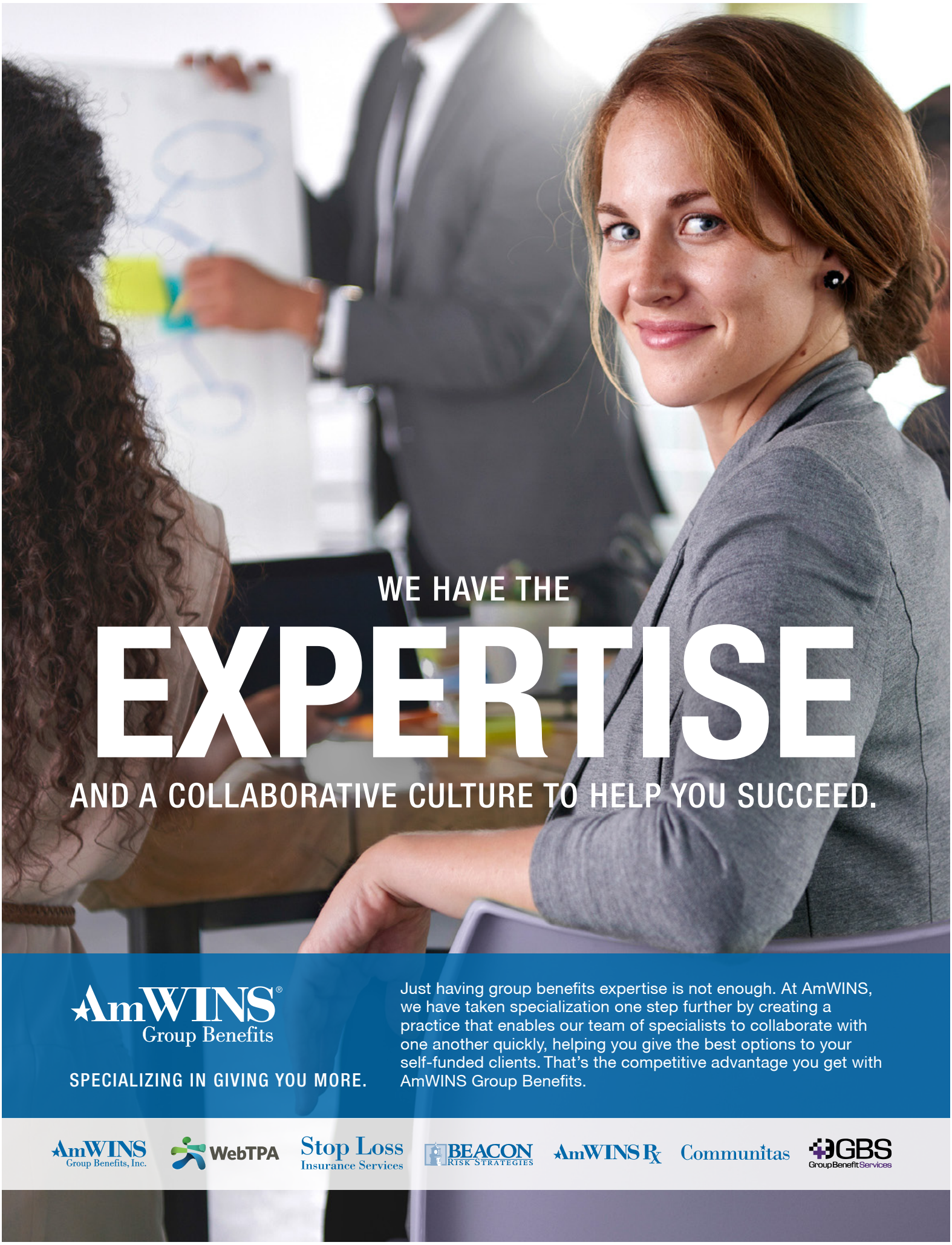
To obtain and preserve a SOC 2, Type 2 designation requires a holistic approach to data security where every decision made considers the security impact and potential for vulnerability. It requires company senior management to run their organization with a new philosophy and perspective.

As you are evaluating the data security at your organization, and those of your vendor partners, consider the following tests, controls, and questions:

Organization and Management

Organization and management include management philosophy, security management, and security policies. This addresses the integrity and values of an organization including the qualifications and accountability of personnel. Ask:

- What is senior management's philosophy concerning data and information?
- Is there a comprehensive security policy in place at the organization?



AmWINS® Group Benefits

SPECIALIZING IN GIVING YOU MORE.

Just having group benefits expertise is not enough. At AmWINS, we have taken specialization one step further by creating a practice that enables our team of specialists to collaborate with one another quickly, helping you give the best options to your self-funded clients. That's the competitive advantage you get with AmWINS Group Benefits.

AmWINS Group Benefits, Inc. | WebTPA | Stop Loss Insurance Services | BEACON Risk Strategies | AmWINS Rx | Communitas | GBS Group Benefit Services

Communications

Communication criteria relate to how employees understand and are able to effectively implement the philosophy and policy crafted by senior management. This includes both formal and information communication to train and evaluate employees on the operation of the system. Ask:

- Is there a formal communication of security commitment as a new client or employee?
- Can the organization provide information regarding the design and operation of its system which is communicated to staff and relevant users?

Risk Management and Design and Implementation of Controls

Risk management controls include the ability to identify, evaluate, and monitor potential risks that may threaten data security. As part of a comprehensive plan, these risks should be discussed and evaluated for any necessary changes or adjustments needed in the security policy. Ask:

- How are potential threats to data security identified?
- Is this information documented in a risk assessment report along with an evaluation of changes in internal controls?

Monitoring of Controls

Monitoring of controls uses a variety of techniques to evaluate how well the data security system is operating. The results are reviewed daily and action will be taken on any deficiencies in the system.

- Is there evidence that normal business operation can continue and data be recovered in the face of a disaster?
- Is there evidence that paid "ethical hackers" have attempted to access the system. Were any corrective actions implemented to address for discovered weaknesses?

- With employees and company guests, what controls exist to ensure a safe data environment including background checks and physical access?
- What is the procedure to terminate system access?

System Operations

System operations involve how well the system detects, evaluates, and mitigates threats to the system in real time. These criteria include the documentation of such events.

- Is there evidence of security incidents that were logged, mitigated, and documented in the system?

Change Management

Change management deals with the reality that the world of data security is constantly changing. This criterion evaluates how an organization assesses and identifies needed changes, as well as implements these changes without creating new security risks.

- Is there evidence of an assessment report of the system identifying potential risks?
- How are these risks evaluated by management for potential changes to the system?

Data security is of paramount importance in today's world and it affects every person, and every company, large or small. Given the sensitivity and importance of medical information, it is important to ask critical questions of your own data security and especially that of your vendors. Ensure the providers you work with are up to the highest level of standards to protect your customers' data. ■

Logical and Physical Access Controls

Logical and physical access controls are relevant to the Target breach as it relates to preventing unauthorized access to the data system. The organization should have the ability to provide and remove access, as well as physically restrict access on-site.

Andrew Weaderhorn is one of the Founders and Chief Executive Officer of MedSource National (SOC 2, Type 2 Compliant Firm). As CEO and majority co-owner, he has utilized his more than 12 years of experience in managed care services to offer a flexible technology solution to the national claims market, while maintaining a high level of local service. Mr. Weaderhorn's "hands on approach" is a key factor in helping MedSource National achieve operational success.