Data Breach

Policy Statement

At Health, LLC takes many proactive steps to protect against unauthorized access to private data, but acknowledges that in today's rapidly changing technology environment no security measures are 100% perfect. This policy outlines the response plan in the unlikely event of a data breach on the AtHealth.com website.

Reason For Policy

This policy ensures that the response to a data or security breach will be as coordinated and timely as possible to minimize the impact to user privacy.

Responsible Executive

The Website Administrator is responsible for this policy with oversight from the CE Coordinator.

Last Reviewed

20 January, 2026.

Policy

This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms.

At Health, LLC's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how At Health, LLC's established culture of openness, trust and integrity should respond to such activity. At Health, LLC is committed to protecting our employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

This policy mandates that any individual who suspects that a theft, breach or exposure of At Health, LLC Protected data or Sensitive data has occurred must immediately provide a description of what occurred via e-mail to Support@AtHealth.com or by calling (888) 284-3258. This e-mail address and phone number are monitored by At Health, LLC's Information Security Administrator, who will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information of At Health, LLC employees and customers.

In addition to the protections provided by our third-party vendors, At Health, LLC uses a combination of controls to monitor and protect sensitive data that include the following:

Firewall

- Web Application Firewall identifies and blocks malicious traffic. Built and maintained by a large team focused 100% on security of the web hosting platform used.
- Protection of site at the endpoint, enabling deep integration with the web hosting platform that does not break encryption, cannot be bypassed and cannot leak data.
- Integrated malware scanner blocks requests that include malicious code or content.
- Protection from brute force attacks by limiting login attempts.

Security Scanner

- Malware scanner checks core files, themes and plugins for malware, bad URLs, backdoors, SEO spam, malicious redirects and code injections.
- Ongoing comparison of core files, and website code with what is in the WordPress.org repository, checking their integrity and reporting any changes.
- Repair of files that have changed by overwriting them with a pristine, original version.
- Ongoing checks for known security vulnerabilities with alerts of any issues.
- Ongoing checks of content safety by scanning file contents, posts and comments for dangerous URLs and suspicious content.

Login Security

- Two-factor authentication (2FA), one of the most secure forms of remote system authentication available via any TOTP-based authenticator app or service.
- Login Page CAPTCHA stops bots from logging in.
- Disable or add 2FA to XML-RPC.
- Block logins for administrators using known compromised passwords.

Additional Security Tools

- Ongoing monitoring of visits and hack attempts in real time; including origin, IP address, the time of day and time spent on the site.
- Ability to block attackers by IP or to build advanced rules based on IP Range, Hostname, User Agent, and Referrer.

As soon as a theft, data breach or exposure containing At Health, LLC Protected or Sensitive data is identified, the process of removing all access to that resource will begin.

The CE Director will chair an incident response team to handle the breach or exposure. The team will include members from At Health, LLC staff and additional experts as required to address the following areas:

- IT Infrastructure
- Finance (if applicable)
- Legal

- Communications
- Customer Service (if Customer data is affected)
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the CE Director

The CE Director will be notified of the theft, breach or exposure. IT, along with the designated forensic team, will analyze the breach or exposure to determine the root cause.

As provided by At Health, LLC cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Based on the nature of the incident and scope of the impact, the At Health team will work with communications, legal and human resource experts to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

Roles & Responsibilities

- Sponsors - Sponsors are those members of At Health, LLC that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any At Health, LLC Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is the member of At Health, LLC, designated by the Executive Director or the Director, Information Technology (IT) Infrastructure, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the At Health, LLC community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives or third party experts: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Member Services; Human Resources.

Any At Health, LLC personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.