PatagoniaHealth

EHR 2.0
Ensure HIPAA Compliance

Security Risk Assessment Summary

Prepared for:

Patagonia Health

5/1/2015

EHR 2.0

150, Cornerstone Drive,
Suite# 104,
Cary
NC 27519

Phone: 866-276 8309

E-mail: info@ehr20.com

Patagonia Health Inc.

1915 Evans Road

Cary, NC 27513

Email: info@patagoniahealth.com

http://patagoniahealth.com/

Patagonia Health is enlisting EHR 2.0 as a third-party security agency to conduct independent security and HIPAA audits. EHR 2.0 follows a standards-based risk assessment program (i.e., NIST) to ensure security, privacy, and administrative processes required under HIPAA are met by its clients. Assessments are conducted based on point-in-time analysis of systems and existing processes. Patagonia Health Inc. has provided details about their operation to the best of their knowledge, and EHR 2.0 is not claiming responsibility for any inaccuracies reported, for instance due to a change in processes, people, and technology.

SECURITY RISK ASSESSMENT

EXECUTIVE SUMMARY

Under the HIPAA Privacy and Security Rule, Patagonia Health, as a Business Associate (BA), is required to perform active risk prevention and safeguarding of patient information essential to patient privacy. The HITECH act allows only the **minimum necessary** to be disclosed when handling protected health information (PHI).

This security risk assessment report has been prepared to support the requirements of the Department of Health and Human Services (HHS), Office for the Civil Rights (OCR), Center for Medicare and Medicaid Services (CMS) Meaningful Use, and other applicable state data privacy laws and regulations. A detailed risk management plan is maintained continuously, based on the gaps identified from the risk analysis. The gaps identified and recommendations provided are based on input provided by the staff, budget, scope, and other practical considerations.

At EHR 2.0 we have developed the following information to provide a quick reference for answers to many security questions raised by the requirements for meeting Meaningful Use security measures and HIPAA/HITECH regulations. The responses on this list are based on our best understanding of the questions, as they pertain to the Patagonia Health EHR system and its components as well as the hosting environment. This information is current as of May 1, 2015 but is subject to update as new information and questions are brought to our attention.

Risk Assessment Approach

Our risk assessment approach is expected to identify only reasonably anticipated threats or hazards to the security or integrity of electronic Protected Health Information (ePHI). The results of the risk assessment are used to develop and implement appropriate policies and procedures. Interviews, questionnaires, and automated scanning tools are used for gathering information required for this security risk analysis report. When mitigating significant risks, not all are equally important. Management will take into account the cost of intervention and the business impact of loss of confidentiality, integrity, or availability of data.

1. Security policy

Formal and documented security policies, standards, plans, and procedures

A set of rules and procedures regulating the use of ePHI, including our processing, storage, distribution, and presentation is maintained in the information security policy document. The set of laws, rules, and practices that regulate how Patagonia Health manages, protects, and distributes PHI information is frequently updated in the security policy document.

2. Change control

Change control procedure to support security policy

Changes to the system, network, applications, databases, other system components, and physical/environmental factors are monitored and controlled through an approved change management process. Changes are reviewed, approved, and monitored during post-implementation to ensure that expected changes and their desired result are accurate.

3. Encryption

When and how encryption is employed to guard all PHI

Electronic Protected Health Information (ePHI) data is encrypted while in transit, on any network, or stored selectively on any device within or outside the premises. ePHI (including authentication credentials) is encrypted while in transit over any public network or wireless network. Key management procedures are employed that assure the confidentiality, integrity, and availability of data as per the HIPAA security rule.

4. Access Control

Process for granting and documenting access

Every user in our system is managed within Active Directory, which controls access to all levels of data from the system perspective. This does not include application level user accounts, which are controlled by a more granular level of security to the medical records within a practice. User accounts are setup to “lockout” after a set limit of incorrect login attempts. Procedures are also in place to verify the user and grant access back into the system in the event of lockout happening to a legitimate user.

5. Vulnerability Assessment

Periodic vulnerability assessments or penetration testing

Patagonia Health continuously gathers and analyzes information regarding new and existing threats and vulnerabilities, actual attacks on the organization, and the effectiveness of the existing security controls using Qualys security guard. This assessment takes into account related policies and procedures, viruses and malicious code, intrusion detection, and event and state monitoring. The key purpose of this particular assessment is to highlight and investigate network security vulnerabilities.

6. Baseline Security Configuration

Identification and implementation of baseline security configuration of the key ePHI systems

Patagonia Health maintains all servers at the hardware and software levels. Patagonia Health monitors security patch releases from the vendors, whose products are used, and schedule routine updates during specified maintenance windows. Patagonia Health uses perimeter equipment from Fortinet that addresses "Unified Threat Management" protection for all traffic that passes to and from our network. Intrusion protection, Anti-virus/Anti-spyware/Anti-malware, Firewall, VPN, and traffic shaping are some of the protections that are utilized for protecting patient data. Exception-based log notifications are reviewed periodically to identify any potential intrusion attempts.

7. Physical Security

Monitoring devices used to track and/or prevent unauthorized access to secure areas which are housing or processing PHI data

Patagonia Heath data center is protected via lock and key, and all access to the data center is recorded using security key chips that are assigned to employees who need physical access. Patagonia Health has established policies and procedures which govern how our staff processes requests for addition/modification/deletion of user access permissions.

8. Breach Response

Documented breach response process and procedures

The HIPAA Breach Notification Rule requires companies to notify patients of a "breach," if unsecured information about patients is seen or accessed by unauthorized persons. A web-based breach determination tool is used to determine and analyze the risk exposure of an incident to prepare and notify the necessary parties covered entities in case of a data breach.

9. Business Continuity

Recovery plans in place to support essential services in case of a disaster

Formal documented recovery plans exists to identify the resources and specific actions required to minimize losses in the event of a disruption to the business unit, support group unit, application, or infrastructure component. Plans include timely and orderly recovery of the business, support processes, operations, and technology components, within an agreed upon timeframe, and include orderly restoration of patient care activities when the primary PHI environment is unavailable.

10. Backup and Offsite Storage

Documented process for how system, application and data backups are performed

Patagonia Health implements system-level functions which include data backup and disaster recovery planning. Patagonia Health maintains both near-line (in data center) and off-site (another separate data center) copies of the data which allow quick access to backups for single file retrieval, etc. Off-site backup copies are for disaster recovery scenarios, in which Patagonia Health would need to provide access to the systems at an alternate data center location in the event of a total failure of our primary site. Patagonia Health utilizes virtualization technologies from both VMware and Microsoft that allow for the recovery of systems on "rented" virtualization engines from partners, in the event of such need.

11. Sub-contractors arrangement

Dependent service providers engaged in providing any services related to outsourced application, service or system

Patagonia Health requires all third party organizations or subcontractors that receive, send, transmit, store, control, or process PHI information to or from Patagonia Health or its client(s)to have a business associate contract before the engagement. Patagonia Health has a process to review all dependent third party service providers' (i.e., subcontractors') security policies and procedures to ensure that appropriate security language is incorporated into all business associate agreements as per the HITECH act.

12. Training and Education

Identity and background of all staff servicing customer is known based on security background checks and periodic awareness training

Virtually every staff member is involved in handling ePHI by creating, maintaining, sharing, and/or storing patient health information is affected by HIPAA/HITECH privacy, security, breach notification, and enforcement rules. Web-based security awareness training and face-to-face training sessions on HIPAA/HITECH compliance prepares Patagonia Health staff to comply with

the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).

13. Asset Inventory

Inventory control methods and procedures in place to maintain an inventory of ePHI assets for hardware, software, information assets, physical assets, and services

A complete list of ePHI inventory, including system hardware, software, and other applications that are processing electronic Protected Health Information (ePHI), has been documented. Periodic scoping exercise is done on systems, processes, and applications-based ePHI data created, shared, stored, and/or transmitted.

Summary

Since cost, timeliness, and ease of use are a few of the many important factors in managing the identified risks, Patagonia Health attempts to implement security measures in addition to the above listed security controls that are sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. In addition, an active security risk management plan is maintained to handle any evolving security threats.

Disclaimer: Patagonia Health Inc. has provided details about their operation to the best of their knowledge, and assessments were conducted based on point-in-time analysis of systems and existing processes. EHR 2.0 is not claiming responsibility for any inaccuracies reported, for instance due to a change in processes, people, and technology..