SOX, Compliance, Access Management & Security	UNIVERSAL AMERICAN A WellCare Company	**Effective Date** 03/31/10	**Owner** Patrick Kittell V/P & Chief Security Officer
		Policy # SCAMS.0803.04	**Revision Date** 11/10/16
	PHI and PII Data Security and Handling	**SOX Ref #** N/A	**Approved By** Anne Mercer Vice President, Internal Audit
		Next Review Date 11/01/17	**Last Review Date** 11/10/16
	Approvers Name (Printed): Anne Mercer - signature on file		Date: 11/10/16

1.0 PURPOSE

1.1 The purpose of this procedure is to define procedures for the security and handling of all physical and electronic documents containing protected health information (PHI) and personal identity information (PII) data.

2.0 POLICY

2.1 It is the policy of Universal American (UAM) to maintain the confidentiality of Protected Health Information (PHI) and Personal Identifiable Information (PII).

2.2 This policy ensures the Company's ability to manage, access, and utilize protected data consistently while maintaining the Company's need for confidentiality, integrity and availability.

2.3 This policy also ensures that any authorized and officially designated delegated entity (DE) must adhere to the same standards as those of UAM that are described in this document.

3.0 APPLICABILITY

3.1 This policy and procedure applies to all individuals performing tasks on behalf of UAM, and includes employees, consultants, independent contractors, temporary staff personnel, agents, vendors, delegated entities, or business partners with access to UAM PHI and/or PII data or information from any Company source.

3.1.1 Delegated entities/vendors identified in this policy have delegated authority for developing and implementing procedural guidance for ensuring their departmental responsibilities under this policy are communicated and enforced.

3.1.2 This policy also applies to all individuals performing tasks on behalf of Collaborative Health Systems (CHS), and includes employees, consultants, independent contractors, temporary staff personnel, agents, vendors, delegated entities, or business partners with access to CHS PHI and/or PII data or information from any Company source.

4.0 DEFINITIONS

4.1 UAM – Universal American Corp.

4.2 CHS – Collaborative Health Systems.

4.3 SCAMS – SOX, Compliance, Access Management and Security Department.

4.4 PHI – Protected health information.

4.4.1 Any member/patient information that is created or received by a health care provider,

health plan, public health authority, employer, life insurer, or health care clearinghouse, etc. and linked to a specific individual is consider PHI, as follows:

4.4.1.1 Name.

4.4.1.2 Address.

4.4.1.3 Social security number.

4.4.1.4 Phone numbers, fax numbers, email addresses, unique URL or IP addresses.

4.4.1.5 Dates (date of birth, date of death, date of medical service).

4.4.1.6 Medical record number.

4.4.1.7 Medicare Health Insurance Claim Number (HICN).

4.4.1.8 Health plan beneficiary number.

4.4.1.9 Medical history data.

4.4.1.10 Account numbers.

4.4.1.11 License or serial numbers (including license plates).

4.4.1.12 Fingerprints or photographs.

4.5 PII – Personal identifiable information.

4.5.1 Any information that can be used to uniquely identify, contact, or locate a single person, as follows:

4.5.1.1 Name.

4.5.1.2 Address.

4.5.1.3 Phone number.

4.6 PHI and PII may reside in hard copy or electronic records; both forms of PHI/PII fall within the scope of this policy.

5.0 PROCEDURE

5.1 **Vendors.**

5.1.1 Individuals or companies that have been approved by the Contracts Administration or Legal Department as a recipient of organizational PHI/PII and from which the Contracts Administration or Legal Department has received certification of their data protection practices conformance with the requirements of this policy.

5.1.1.1 Vendors include all external providers of servicers to the company and include proposed vendors.

5.1.1.2 PHI/PII information cannot be transmitted to any vendor in any method unless the vendor has been pre-certified for the receipt of such information.

5.2 **PHI / PII Data Retention and Storage.**

5.2.1 UAM understands the importance of minimizing the amount of PHI/PII data it maintains

and retains only what is necessary and requires the same understanding of all delegates.

5.2.1.1 Permanent – Data that is stored for consistent and historical use and access on a permanent basis:

5.2.1.1.1 Must be stored on secured drives on UAM IT-managed servers located in approved secured facilities or on drives on business partner IT Departments' servers located in approved secured facilities. These are drives that are only accessible by using a password. Data stored on servers not located in approved secured facilities must be encrypted.

5.2.1.1.2 This includes but is not limited to application databases, network and computer databases, reporting replication servers, departmental databases and spreadsheets.

5.2.1.1.3 Data cannot be stored on "public" drives at UAM (O: Drive in Orlando, H: Drive in Houston, etc.). These are drives that are accessible without a password.

5.2.1.2 Temporary – Data that is stored for short-term use only, and **not** stored for any consistent or historical use:

5.2.1.2.1 May be temporarily stored on the encrypted hard drive of an UAM-owned PC or laptop computer.

5.2.1.2.2 Data must be immediately deleted from the hard drive once the work is completed.

5.2.1.2.3 Temporary storage periods are no more than 14 days.

5.2.1.3 Data may **not** be stored on any portable media (i.e. flash drive, CD/DVD–ROM disc, etc.) unless express permission is made by the UAM Chief Security officer.

5.2.1.4 Data may **not** be stored on any portable device (i.e. BlackBerry, cell phone, iPod, iPad, etc.).

5.3 **PHI and PII Data Transmission.**

5.3.1 By email:

5.3.1.1 PHI/PII data **must** be sent through the internal UAM Outlook email system when sending electronic data between and among UAM staff.

5.3.1.2 PHI/PII **must** be encrypted. Please see an IT Infrastructure staff member if you need assistance with this.

5.3.1.3 Staff may **not** use *personal* or *external* electronic mail to send electronic data (i.e. Hotmail, Yahoo Mail, Google Mail, etc.).

5.3.1.4 Staff who access Microsoft Office 365 and, specifically, Outlook 365 may retrieve email from outside companies or sources, but must **not** send any email containing PHI /PII through Outlook 365.

5.3.1.5 Staff **must** use the "Send Securely" button in UAM Outlook, **or** ensure that one of the following are present in the email SUBJECT line (exactly as written

below) whenever you send any PHI/PII data to third party vendors or organizations outside of UAM.

5.3.1.5.1 **SECURE**

5.3.1.5.1.1 *Example:* Subject: SECURE December ACO Member Files.

5.3.1.5.2 ****CONFIDENTIAL****

5.3.1.5.2.1 *Example:* Subject: **CONFIDENTIAL** December ACO Member Files

5.3.1.5.3 **[psm]**

5.3.1.5.3.1 *Example:* Subject: [psm] December ACO Member Files.

5.3.1.6 Please see an IT Infrastructure staff member if you need assistance with this.

5.3.1.7 Please remember that Universal American does *not* allow password-protected documents to be sent via email. If you send email from our UAM Outlook either internally (within UAM) or externally (to third party vendors or organizations outside of UAM) according to the method described above, your document *will be sent via encrypted email*.

5.3.2 By FTP and electronic interface:

5.3.2.1 Data transferred between UAM and third party vendors or business associates when FTP is accepted must use the UAM IT Department secured and encrypted FTP process or the UAM-supported FTP Web Portal.

5.3.2.2 Requests to initiate utilization of the FTP process or to access the UAM FTP Web Portal must be submitted through a TeamTrack.

5.3.3 By fax:

5.3.3.1 Data may only be transmitted from a designated UAM fax machine or through the UAM RightFax application software application.

5.4 **PHI and PII Data Reporting.**

5.4.1 Data requests to include reports, extracts, or interfaces to/from UAM must be

5.4.1.1 Approved by the UAM business through the UAM TeamTrack process, **and**

5.4.1.2 Programmed, tested, and implemented by UAM or delegated entity IT Departments, or

5.4.1.3 If developed from non-IT Department resources (data marts, business databases), be approved by the UAM IT Security and Privacy Officers following a PHI/PII review of the data being included in the report, extract or interface.

5.4.1.4 Be encrypted by using approved UAM encryption methods for data storage and transmission (i.e., secure file transfer protocol [SFTP] or secure email).

5.4.1.5 Please see an IT Infrastructure staff member if you need assistance with this.

5.4.2 The PHI Audit Step in TeamTrack ensures that the reports, extracts or interfaces have been reviewed and approved by both the UAM Privacy Officer and the UAM Security Officer for content appropriateness, storage, transmission, and qualification of the receiving entity.

5.4.2.1 Any TeamTrack that contains one or more of the PHI data elements in this policy must be identified by answering "YES" to the question "PHI Data Required" in the TeamTrack itself.

5.4.2.1.1 This must be done by anyone (business user, IT management, IT developer, etc.) who encounters the TeamTrack and recognizes the presence of PHI in the request.

5.4.2.2 Each TeamTrack designated to have PHI contained within it is approved by both the UAM Privacy Officer and the UAM Security Officer prior to the data being released.

5.4.2.3 A PHI TeamTrack Log is maintained on a daily basis, containing all requests, approvals, and other actions.

5.5 **Displaying PHI and PII Data on Websites.**

5.5.1 Data may only be displayed on public websites developed and hosted by UAM or business partner IT Department.

5.5.2 Data may not be displayed on third party public websites unless the following exists:

5.5.2.1 The website has been approved by the UAM Chief Security Officer, Chief Administrative Officer, or the UAM Legal Department.

5.5.2.2 The website is encrypted per UAM website standards.

5.5.2.3 A specific and unique user sign-on must be required to access the data on that portion of the website.

5.5.2.4 The user sign-on must be assigned by UAM.

5.6 **Paper Storage**

5.6.1 All paper containing PHI/PII data must be stored in locked file cabinets, locked desk drawers, or sealed storage containers.

5.6.1.1 Paper documents containing PHI/PII data must not ever be left unattended on desks, fax machines, or copiers.

5.7 **Employee and Delegated Entity Acknowledgement.**

5.7.1 All UAM employees are required to sign (via electronic signature, electronic attestation, or by hardcopy) and date the PHI and PII Data Security and Handling Policy Acknowledgement Form:

5.7.1.1 When first hired by UAM;

5.7.1.2 On an annual basis thereafter (in January).

5.7.2 Delegated entities/vendors identified in this policy have delegated authority for developing and implementing procedural guidance for ensuring their departmental responsibilities under this policy are communicated and enforced.

5.7.3 Policy violations:

5.7.3.1 Any employee who knowingly violates this policy will be subject to disciplinary action up to and including termination.

5.7.3.2 Any consultants, independent contractors, temporary staff, agents, vendors, delegated entities, or business partners who knowingly violate this policy will be subject to immediate removal from working with the UAM account, and will be immediately reported to the UAM business segment/department manager.

6.0 TRAINING

6.1 All UAM employees and third-party business associates and delegated entities are notified on an annual basis of this procedure,

6.1.1 UAM provides training materials relating to securing and handling protected health information upon delegate's request to assist in ensuring the workforce is fully aware of obligations.

7.0 REPORTING

7.1 None.

8.1 SOURCES, STANDARDS AND PRACTICES

8.1 CobiT:

8.1.1 DS 5.11 – Exchange of sensitive data.

8.1.2 DS 11.6 – Security requirements for data management.

8.2 ITIL:

8.2.1 SD 5.2 – Data and information management.

8.3 ISO:

8.3.1 10.8.1 – Information exchange policies and procedures.

8.3.2 10.8.3 – Physical media in transit.

Related Documentation

- PHI TeamTrack Log