Marketware, Inc. HIPAA Compliance

Learn how Marketware, Inc. not only complies with HIPAA, but builds a better, more secure environment to mitigate your risk & help you prove compliance with HIPAA. We did the hard work so you don't have to & you can inherit a lot of the work that we've done in terms of audits. Our HIPAA compliant API, platform, & data integration service simplify compliance for you.

In an effort to be transparent, we go into a good amount detail on this page. As a lead in, below is a high level summary our major architecture, our guiding principles, & how it maximizes our security posture.

Need	Marketware, Inc. Approach
Encryption	All data is encrypted in transit, end to end, & at rest. Log data is also encrypted to mitigate risk of ePHI stored in log files
Minimum Necessary Access	Access controls are setup with the system administrator before general access with minimum necessary access as a guiding principle.
System Access Tracking	All access requests & changes of access, as well as approvals, are tracked & retained.
PHI Segmentation	All customer data is segmented into its own database.
Monitoring	All network requests, successful & unsuccessful, are logged, along with all system logs. API PHI requests (GET, POST, PUT, DELETE) log the requestor, location, & data changed/viewed. Additionally, alerts are proactively sent based on suspicious activity. OSSEC is used for IDS & file integrity monitoring.
Auditing	All log data is encrypted & unified, enabling secure access to full historical network activity records.
Minimum Risk to Architecture	Secure, encrypted access is the only form of public access enabled to servers. All API access must first pass through Marketware, Inc. application server. Calls must be authenticated before access to data is granted.
Vulnerability Scanning	All customer & internal networks are scanned regularly for vulnerabilities.
Intrusion Detection	All production systems have intrusion detection software running to proactively detect anomalies.

Backup	All customer data is backed up every 24 hours. Seven (7) days of rolling backups are retained.
Disaster Recovery	Marketware, Inc. has an audited & regularly tested disaster recovery plan. This plan also applies to customers, & they inherit this from us.
Documentation	All documentation (policies & procedures that make up our security & compliance program) is stored & versioned using Dropbox, & published here (www.markeware.com/policy)
Risk Management	We proactively perform risk assessments to assure changes to our infrastructure do not expose new risks to ePHI. Risks mitigation is done before changes are pushed to production.
Workforce Training	Despite not having access to the ePHI of our customers, all Marketware, Inc. workforce members undergo HIPAA & security training regularly.

See the finer grain details of how we comply with HIPAA below. These are mapped to specific HIPAA rules. There's a lot here but again, we are taking this responsibility on so that our customers don't have to. Controls marked with an (Req) are Required. Controls marked with an (A) are Addressable. In our environment, controls outlined below are implemented on all infrastructure that processes, stores, transmits or can otherwise gain access to ePHI (electronic protected health information). If have questions, please email us.]

Administrative Safeguards (see 164.308)

Taken directly from the wording of the Security Rule, administrative safeguards are administrative actions, & policies & procedures, to manage the selection, development, implementation, & maintenance of security measures to protect electronic protected health information & to manage the conduct of the covered entity's workforce in relation to the protection of that information. There aren't specific security settings in this section, & the most important area covered is the risk assessment. The risk assessment is a fundamental process for any organization that wants to become compliant.

Security Management Process - 164.308(a)(1)(i)

Standard	Description
Risk Analysis (Req)	Conduct an accurate & thorough assessment of the potential risks & vulnerabilities to the confidentiality, integrity, & availability of electronic PHI held by the covered entity.
Risk Management (Req)	Implement security measures sufficient to reduce risks & vulnerabilities to a reasonable & appropriate level to comply with Sec. 164.306(a) [Security standards: General rules; (a) General requirements].
Sanction Policy (Req)	Apply appropriate sanctions against workforce members who fail to comply with the security policies & procedures of the covered entity.
Information System Activity Review (Req)	Implement procedures to regularly review records of information system activity, such as audit logs, access reports, & security incident tracking reports.

Marketware, Inc., Inc. has a risk management policy that defines the risk analysis & risk management process. This policy is operationalized with processes to conduct regularly risk assessments. Marketware, Inc. uses NIST800-30 & 800-26 for performing risk analysis. Our policy begins with an inventory of all Marketware, Inc. systems, mapping of where ePHI is processed, transmitted, or stored, identification of threats, risks, & likelihood, & the mitigation of risks. Policies address risk inherent within the environment & mitigating the risk to an acceptable & reasonable level. Marketware, Inc. has a Sanction Policy that has sanctions for employees not adhering to certain policies, & for specifically violating HIPAA rules. Policies & procedures address the requirements of monitoring & logging system level events & actions taken by individuals within the environment. All requests into & out of the Marketware, Inc. network are logged, as well as all system events. Marketware, Inc., has implemented multiple logging & monitoring solutions to track events within their environment & to monitor for certain types of behavior. Log data is regularly reviewed. Additionally, proactive alerts are enabled & triggered based on certain suspicious activity.

Assigned Security Responsibility - 164.308(a)(2)

Standard	Description
Assigned Security Responsibility (Req)	Identify the security official who is responsible for the development & implementation of the policies & procedures required by this subpart for the entity

Marketware, Inc., Inc. has formally assigned & documented its security officer. Our security office is Benjamin Bartel. He can be reached by email at ben.bartel@marketware.com

Workforce Security - 164.308(a)(3)(i)

Standard	Description
Authorization &/or Supervision (A)	Implement procedures for the authorization &/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.
Workforce Clearance Procedure (A)	Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.
Termination Procedures (A)	Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [Workforce Clearance Procedures] of this section.

Marketware, Inc., Inc. has policies in place that require workforce members requesting access to ePHI to submit an authorization form that is signed & acknowledges their responsibility of safeguarding ePHI. The form must also be approved by the Security Officer. Once signed & approved, then the individual will be provisioned access to systems deemed business necessary. All Access to ePHI is based on minimum necessary requirements & least privilege. Marketware, Inc. cannot access ePHI unless customers explicitly grant access.

Marketware, Inc. policies define the immediate removal of access once an employee has been terminated, with the Security Officer responsible for terminating the access. Once HR initiates the termination process the termination checklist is referenced to ensure necessary actions are taken to remove systems & facilities access

Information Access Management - 164.308(a)(4)(i)

Standard	Description
Isolating Health care Clearinghouse Function (Req)	If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies & procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.
Access Authorization (A)	Implement policies & procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.
Access Establishment & Modification (A)	Implement policies & procedures that, based upon the entity's access authorization policies, establish, document, review, & modify a user's right of access to a workstation, transaction, program, or process.

Marketware, Inc., Inc. does not perform the functions of a Healthcare Clearinghouse so aspects of this section are not applicable. The security officer determines the roles necessary for each system & application. When access is needed to Marketware, Inc. infrastructure, a request & acknowledgement form is signed & then approved by the Security Officer. Marketware, Inc. has a formal process for requesting additional access to ePHI, & again Marketware, Inc. customers must approve all requests concerning ePHI.

Security Awareness & Training - 164.308(a)(5)(i)

Standard	Description
Security Reminders (A)	Periodic security updates to all members of Marketware, Inc
Protection from Malicious Software (A)	Procedures for guarding against, detecting, & reporting malicious software.
Log-in Monitoring (A)	Procedures for monitoring log-in attempts & reporting discrepancies
Password Management (A)	Procedures for creating, changing, & safeguarding passwords.

Marketware, Inc. has a Security Awareness training policy in place that requires new employees & current employees to conduct training upon hire & annually thereafter. Minimum training is done annually, with informal security & compliance training done as needed.

Marketware, Inc. proactively assesses & tests for malicious software within their environment, both infrastructure & workstations. Members of the Marketware, Inc. team monitor bug & vulnerability lists to assure they remain up to date. Marketware, Inc. is monitoring & logging successful & unsuccessful log-in attempts to the servers within its environment & policies are in place requiring audit logging, which includes login attempts. Password configurations are set to require that passwords are a minimum of 8 character length, 90 day password expiration (Customer Admin Configurable), account lockout after 5 invalid attempts, & account lockout after 20 minutes of inactivity (Customer Admin configurable up to 60 minutes).

Security Incident Procedures - 164.308(a)(6)(i)

Standard	Description
Response & Reporting (Req)	Identify & respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; & document security incidents & their outcomes.

Marketware, Inc. has implemented a formal incident response plan (IRP), which discusses the procedures for identifying, responding to, & escalating suspected & confirmed security breaches. Marketware, Inc. has implemented an incident response team for the purposes of dealing with potential security breaches. The IRP has specific types of incidents to look out for, as well as some common types of incidents that are monitored for within the environment.

Contingency Plan - 164.308(a)(7)(i)

Standard	Description
Data Backup Plan (Req)	Establish & implement procedures to create & maintain retrievable exact copies of electronic protected health information.
Disaster Recovery Plan (Req)	Establish (& implement as needed) procedures to restore any loss of data.
Emergency Mode Operation Plan (Req)	Establish (& implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic PHI while operating in emergency mode.
Testing & Revision Procedure (A)	Implement procedures for periodic testing & revision of contingency plans.
Applications & Data Criticality Analysis (A)	Assess the relative criticality of specific applications & data in support of other contingency plan components.

Marketware, Inc., Inc has a formal Backup & Recovery Policy that defines the data backup strategy including: schedule, associated responsibilities, & any risk-assessed exclusion to the backup schedule.

Marketware, Inc. has a formal Disaster Recovery plan to ensure the efficient recovery of critical business data & systems in the event of a disaster. The DR plan includes specific technical procedures necessary to reinstate the infrastructure & data to allow critical business functions to continue business operations after a disaster has occurred. Additionally, the Marketware, Inc. DR plan includes requirements for performing annual testing of the DR plan to ensure its effectiveness.

Marketware, Inc. has a DR plan, or a Business Continuity Plan (BCP), to aid in the efficient recovery of critical business functions after a disaster has been declared. The BCP goes into effect after facility outage of 24 hours. The BCP identifies critical information necessary to resume business operations such as: Hardware/software requirements, recovery time objectives, forms, employee/vendor contact lists, alternate working procedures, emergency access procedures, & a data & application criticality analysis. The BCP includes an Emergency Mode Operations Plan that addresses the access & protection of ePHI while operating in emergency mode.

The DR & BPC plans are reviewed & tested annually or whenever significant infrastructure changes occur. Marketware, Inc. has a performed an applications & data criticality analysis that details what systems & application need be recovered & their specific order in the recovery process.

Evaluation - 164.308(a)(8)

Standard	Description
Evaluation (Req)	Perform a periodic technical & non-technical evaluation, based initially upon the standards implemented under this rule & subsequently, in response to environmental or operational changes affecting the security of electronic PHI that establishes the extent to which an entity's security policies & procedures meet the requirements of this subpart.

Marketware, Inc., Inc. has formal internal policies & procedures for conducting periodic technical & non-technical testing. These define procedures for performing quarterly internal & external vulnerability scanning, as well as annual penetration testing. Vulnerability scanning is performed regularly on a weekly basis & with any major changes in infrastructure. Additionally, non-technical evaluations occur on an annual basis to ensure that the security posture of Marketware, Inc. is at the defined level, approved by management, & communicated down to Marketware, Inc. employees.

Business Associate Contracts & Other Arrangement - 164.308(b)(1)

Standard	Description
Written Contract or Other Arrangement (Req)	A covered entity, in accordance with Â§ 164.306 [Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with Â§ 164.314(a) [Business Associate Contracts or Other Arrangements] that the business associate will appropriately safeguard the information. Document the satisfactory assurances required by paragraph (b)(1) [Business Associate Contracts & Other Arrangements] of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of Â§ 164.314(a) [Business Associate Contracts or Other Arrangements].

Marketware, Inc., Inc. has a formalized template, as well as policies in place regarding Business Associate Agreements & written contracts. Marketware, Inc. has engaged a third party provider for hosting responsibilities & has written attestations of safeguarding its data. Additionally, Marketware, Inc. performs due diligence in assuring that third party providers they select go through their due diligence process & provide services consistent with Marketware, Inc.'s security & compliance posture.

Physical Safeguards (see 164.310)

This one is pretty straight forward - physical measures, policies, & procedures to protect a covered entity's electronic information systems & related buildings & equipment, from natural & environmental hazards, & unauthorized intrusion. Data center security is typically easier to address than office security, though at Marketware, Inc. we address both.

Facility Access Controls - 164.310(a)(1)

Standard	Description
Contingency Operations (A)	Establish (& implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan & emergency mode operations plan in the event of an emergency.
Facility Security Plan (A)	Implement policies & procedures to safeguard the facility & the equipment therein from unauthorized physical access, tampering, & theft.
Access Control & Validation Procedures (A)	Implement procedures to control & validate a person's access to facilities based on their role or function, including visitor control, & control of access to software programs for testing & revision.
Maintenance Records (A)	Implement policies & procedures to document repairs & modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, & locks).

Marketware, Inc., Inc. infrastructure supporting its environments is hosted at AWS (Amazon Web Services), which provides hosting & recovery services for the infrastructure. Marketware, Inc.'s headquarters also has many written policies & procedures for safeguarding the corporate location, which includes workstations with access to the environment, from unauthorized physical access. Smart locks are used to track access & all visitors are logged & escorted.

The Marketware, Inc. environment is entirely hosted & built on hardware components provided by AWS which Marketware, Inc. would never have access into.

Workstation Use - 164.310(b)

Standard	Description
Workstation Use (Req)	Implement policies & procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, & the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.

Marketware, Inc., Inc. has policies in place that define the acceptable uses in place for workstations within the environment. These policies define the acceptable & unauthorized uses of personnel that provided workstations with access to systems potentially interacting with ePHI. These policies are enforced on all workstations. All internal email uses HIPAA compliant vendors.

Workstation Security - 164.310c

Standard	Description
Workstation Security (Req)	Implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.

Marketware, Inc. has a formal Workstation & Portable Media Security Policy that identifies the specific requirements of each device. The policies define the requirements for using &/or restricted specific actions while engaged with any ePHI. Additionally, workstations are secured appropriately to limit exposure to breaches. Firewalls & hard disk encryption are used on all workstations. Actions & events are monitored & controlled, with user restrictions on downloading or copying any ePHI without documented approval & business justification. Additionally, all file storage internally at Marketware, Inc. utilizes HIPAAcompliant cloud-based vendors (currently Dropbox).

Device & Media Controls - 164.310(d)(1)

Standard	Description
Disposal (Req)	Implement policies & procedures to address the final disposition of ePHI, &/or the hardware or electronic media on which it is stored.
Media Re-use (Req)	Implement procedures for removal of ePHI from electronic media before the media are made available for re-use.
Accountability (A)	Maintain a record of the movements of hardware & electronic media & any person responsible therefore.
Data Backup & Storage (A)	Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.

Marketware, Inc. has policies & procedures for all workstations that interact with & may potentially become exposed to ePHI. These policies have requirements for secure media disposal so that ePHI cannot be recovered from these systems. Marketware, Inc. has Media re-use requirements for the workstations, despite the fact that these workstations do not have access to & interaction with ePHI.

Technical Safeguards (see 164.312)

This section of HIPAA outlines the technology & the policy & procedures for its use that protect electronic protected health information & control access to it. It is important to note that these requirements are not prescriptive, & there is flexibility in implementation. The key is that measures that are reasonable & appropriate are implemented to safeguard ePHI.

Access Control - 164.312(a)(1)

Standard	Description
Unique User Identification (Req)	Assign a unique name &/or number for identifying & tracking user identity
Emergency Access Procedure (Req)	Establish (& implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
Automatic Logoff (A)	Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity
Encryption & Decryption (A)	Implement a method to encrypt & decrypt electronic protected health information

All users within the Marketware, Inc. environment are issued a unique user name & password. All accounts are local & unique. General/shared accounts are not in place & root access is restricted & monitored.

Marketware, Inc. has procedures & a process for obtaining access to ePHI should an emergency or disaster occur.

Marketware, Inc. systems settings on all of its servers have session timeout features enabled & configured to terminate sessions after a period of 60 minutes or less. Marketware, Inc. encrypts all stored data in its environment using 256-bit AES encryption. Additionally, all data in transit is encrypted end to end (more below).

Audit Controls - 164.312(b)

Standard	Description
Audit Controls (Req)	Implement hardware, software, &/or procedural mechanisms that record & examine activity in information systems that contain or use ePHI.

Marketware, Inc., Inc. has policies in place addressing audit trail requirements. Systems within the its environment are logging to a centralized logging solution, New Relic, which is monitoring system level events & contains user id, timestamp, event, origination, & type of event. These logs are constantly monitored for suspicious events & alerts are generated to any type of behavior that is suspicious.

Integrity - 164.312c(1)

Standard	Description
Mechanism to Authenticate Electronic Protected (A)	Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.

Marketware, Inc. has employed a centralized access control system for authenticating & accessing internal systems where ePHI resides. Currently, Marketware, Inc. employees access a bastion host using an SSH-2 connection to access internal systems. Accounts on the internal database are restricted to a limited number of personnel, with logging in place to track all transactions.

Person or Entity Authentication - 164.312(d)

Standard	Description
Person or Entity Authentication (Req)	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.

Marketware, Inc., Inc. has a formal policy that describes the process of verifying a person's identity before unlocking their account, resetting their password, &/or providing access to ePHI.

Transmission Security - 164.312(e)(1)

Standard	Description
Integrity Controls (A)	Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection.
Encryption (A)	Implement a mechanism to encrypt ePHI in transit.

All data in transit with Marketware, Inc. is sent over internet connections through an TLS1.2 encrypted mechanism. Transmissions of the data to the application servers occur via an encrypted connection using the TLS protocol. Additionally, none of the internal application servers, database servers, & log & monitoring servers are accessible via public internet. All internal servers must be accessed via bastion host which are not accessible from the internet.

Organizational Requirements (see 164.314)

These requirements simply outline the need for business associate agreements (BAAs) between covered entities & business associates. This requirement has recently been extended to require business associate agreements between business associates & all subcontractors. That linking, chaining together of BAAs, has created for new & interesting legal & business questions. Basically, each layer in the chain of BAAs takes on certain responsibilities & certain risks as part of HIPAA, & there needs to be consistency. We've taken a proactive approach to BAAs to mitigate risk for our customers & assure consistency along the chain of BAAs.

Business Associate Contracts or Other Arrangements - 164.314(a)(1)(i)

Standard	Description
Business Associate Contracts (Req)	The Implementation Specifications for the HIPAA Security Rule Organizational Requirements "Business Associate Contracts or Other Arrangements" standard were evaluated under section 164.308(b)(1) above.
Other Arrangements (Req)	Rules to engaging with additional 3rd parties, like subcontractors.

Marketware, Inc. has a formalized policy & process is in place concerning BAAs. BAA templates are in place & BA contracts are reviewed for consistency. All paying customers on Marketware, Inc. have BAAs in place. Marketware, Inc. has a formal policy & process in place for performing due diligence with any third party or vendor before engaging them. Additionally, contracts are retained that detail the responsibility of safeguarding any information to which the provider may have access, as well as creating consistency for Marketware, Inc. & Marketware, Inc. customers.

Policies & Procedures & Documentation Requirements (see 164.316)

Policies & Procedures - 164.316(a)

Standard	Description
Policies & Procedures (Req)	Implement reasonable & appropriate policies & procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in Â§ 164.306(b)(2)(i), (ii), (iii), & (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart.

Marketware, Inc. has a formalized Policy Management program that ensures that policies are developed, implemented, & updated according to best practice & organization requirements. In the words of our auditors, this is a policy about our policies.

Documentation - 164.316(b)(1)(i)

Standard	Description
Time Limit (Req)	Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.
Availability (Req)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
Updates (Req)	Review documentation periodically, & update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.

Marketware, Inc. retains the necessary policies & documentation for a minimum of 6 years. All policies & procedures are available & distributed to personnel on the company shared drive (currently Dropbox). Marketware, Inc. has an update & review process for reviewing all policies & procedures & updating them as necessary. Additionally, Marketware, Inc. tracks & maintains revision history, approval signature, & timestamps to ensure policies are reviewed & updated according to organization requirements.

HITECH Act & Omnibus Rule: IT Security Provisions

These were updates made to strengthen the Privacy, Security, & Breach Notifications rules within HIPAA. These updates went into effect in 2013 & were the driving force for many existing IaaS vendors to begin signing BAAs

Notification in the Case of Breach - 13402(a) & 13402(b)

Standard	Description
In General	A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.
Notification of Covered Entity by Business Associate	The requirements for the HITECH Act Notification in the Case of Breach - Notification of Covered Entity by Business Associate - Uses & Disclosures: Organizational Requirements “Business Associate Contracts” standard are located in the “BA Requirements” worksheet.

Marketware, Inc. has a formal breach notification policy that addresses the requirements of notifying affected individuals & customers of a suspected breach of ePHI. These policies outline the relevant & responsible parties in case of a breach, forensics work to discover extent of breach, reason for breach, correction of infrastructure to prevent future breach, & requirements of notifying customers of a breach within 24 hours. Marketware, Inc. is a defined Business Associate or subcontractor according to HIPAA regulations & the specific customer relationship.

Timeliness of Notification - 13402(d)(1)

Standard	Description
In General	Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay & in no case later than 60 calendar days after the discovery of a breach by the covered entity involved (or business associate involved in the case of a notification required under subsection (b)).

Marketware, Inc. has a breach notification policy that addresses the requirements of notifying the affected individuals or customers within 24 hours of a breach.

Content of Notification - 13402(f)(1)

Standard	Description
Description of Breach	Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following: (1) A brief description of what happened, including the date of the breach & the date of the discovery of the breach, if known.
Description of EPHI Involved	(2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).
Actions by Individuals	3) The steps individuals should take to protect themselves from potential harm resulting from the breach.
Contact Procedures	(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

Marketware, Inc. has Breach Notification policies in place & they include a brief description of the breach, including the date of the breach & the date of the discovery of the breach, if known. Marketware, Inc. breach notification policies include a description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of PHI were involved) & what the source of the breach was. Our breach notification policies include steps the individual should take to protect themselves from potential harm resulting from the breach. Our policies also provide the contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.