Information Security and Privacy Policy

December 10, 2012

What framework will be established by COHBE to appropriately protect the confidentiality, integrity, availability, and privacy of the COHBE information assets?

Goals/Objectives of COHBE

Unauthorized modification, deletion, or disclosure of information assets can compromise COHBE business operations, violate individual privacy rights, and possibly constitute a criminal act. Efforts are needed to ensure:

- Confidentiality of personally identifiable information and other sensitive data.
- Integrity of data stored on or processed by COHBE information systems.
- Availability of information stored on or processed by COHBE information systems.
- Compliance with applicable laws, regulations, and COHBE policies governing information security and privacy protection.

Background

COHBE is committed to protecting the privacy, confidentiality, integrity, and availability of information assets owned, leased, or entrusted to the entity. The COHBE information security and privacy program promotes and encourages appropriate use of information assets and is not intended to prevent, prohibit, or inhibit the sanctioned use of information assets as required to achieve business objectives. COHBE will establish an information security and privacy program with responsible risk management at its core. COHBE recognizes that no solution is perfect and that residual risks should be identified, managed, and regularly reviewed instead of being waived. In addition to being an appropriate business practice, this policy satisfies the requirements for an Information Security Program Policy as specified in the Centers for Medicare and Medicaid Services (CMS) Minimum Acceptable Risk Standards for Exchanges (MARS-E) requirements. The MARS-E baseline was established in a collaboration between CMS, the Internal Review Service (IRS), and other key stakeholders and is based on the National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53) and IRS Publication 1075.

Scope

This policy applies to the equipment, technology, and data for which COHBE is responsible and all individuals who come in contact with the systems either logically or physically. Contracts and other agreements with 3rd Parties involving COHBE information assets must include compliance with this policy directly or by reference. Implementation efforts regarding personnel vetting, authorization, and training will be done in coordination with and support of responsible human resource and personnel staff.

COHBE reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include,

but is not limited to: monitoring communications across COHBE network services, monitoring actions on the COHBE information systems, checking information systems attached to the COHBE network for security vulnerabilities, disconnecting information systems that have become a security hazard, or restricting data to/from COHBE information systems from access by people, devices, and other systems and across network resources.

Organizationally, we will refer to "COHBE" and the "Exchange" to distinguish activities between the business entity (COHBE) and the technology, call center & back office (the Exchange). This policy may be supplemented and tailored, but not superseded, by additional policies, procedures, and standards adopted by the above individual business units.

Policy Maintenance

This policy shall be reviewed annually and updated to reflect changes in COHBE's business, administrative, or technical environments, or applicable federal/state laws and regulations. The COBHE CEO is responsible for overseeing the review of this policy.

Compliance Requirements

COHBE must at a minimum comply with:

- NIST SP 800-53 for general security
- CMS MARS-E for Exchange specific security
- CMS Health Insurance Portability and Accountability Act (HIPAA) requirements[1]
- IRS Federal Tax Information (FTI) protections based on IRS Pub 1075
- PCI-DSS for payment card transactions
- Applicable privacy requirements from states where COHBE data may reside[2]
- Other statues and regulations which may become applicable based on the actual Exchange implementation

Verification and Validation Requirements

To ensure the COHBE achieves appropriate security and privacy, the program shall integrate the testing of security and privacy controls (physical, technical, and administrative) into routine development and operational processes. The results of the testing must be part of decisions to deploy and manage on going risk.

Periodic independent testing shall be used to avoid blind spots caused by system familiarity and threat advancements.

Reporting and Incident Response Requirements

To ensure appropriate visibility and accountability, the program shall institute routine reporting of threat, risk, attempted attacks, suspected breaches, and actual breaches in accordance with applicable laws, statutes, regulations, and COHBE policies and practices.

Responses to potential security and privacy breaches shall be pre-planned, routinely exercised, and involve data owners.

Responses to actual security and privacy breaches shall be prompt, deliberate, and seek to minimize impacts and loss; balanced with the needs of law enforcement.

[1] Under its current business model, COHBE will be a Business Associate and not a Covered Entity with regard to HIPAA.

[2] At this time the COHBE data may reside in the following states: Colorado, Pennsylvania, Arizona, Alabama, Texas, Illinois, and California.

Roles and Responsibilities

COHBE CEO

The COHBE CEO is ultimately responsible for security and privacy within the organization. The CEO ensures appropriate oversight and resources are made available to implement and operate the COHBE Security and Privacy program. The CEO conducts an annual review of the adequacy and effectiveness of the Security and Privacy Program.

COHBE COO

The COHBE COO is responsible for the development, implementation, and maintenance of operational practices consistent with the COHBE Security and Privacy Program and its associated implementation documents.

COHBE CFO

The COHBE CFO is responsible for overseeing the COHBE Security and Privacy Program; ensuring adequate resources are made available. The CFO will periodically review the status of Security and Privacy Program and the associated performance metrics.

COHBE Security Officer

COHBE will have a Security Officer (SO) designated by the CEO to direct the development, implementation, and maintenance of the COHBE Security and Privacy Program. The COHBE SO will report directly to the CFO with the ability to elevate issues or concerns directly to the CEO; this is a job functionality that may be incorporated within another employee's role.

The SO will be the primary advisor to the organization and the primary representative for COHBE on security and privacy matters to external organization. As such, the SO is expected to stay informed of evolving regulations, statues, threats, risks, technology, and recognized best practices and to regularly coordinate with counterparts at CMS, NIST, and other security authorities.

The SO will develop and implement the COHBE Security and Privacy Risk Management Program[3].

The COHBE Security Officer will review and approve the Exchange Plans of Action and Milestones (POA&M).

CGI Security Officer

The CGI Security Officer is responsible for the development, implementation, and maintenance of operational practices for the Exchange consistent with the COHBE Security and Privacy Program and its associated implementation documents. The CGI Security Officer is responsible to the COHBE COO for the proper daily operation of the Exchange as specified in the Exchange Operations contract.

CGI Security Manager

The CGI Security Manager is designated by the CGI Security Officer to lead and direct the development, implementation, and maintenance of the Exchange Security and Privacy Program. The CGI Security Manager will

[3] As required by CMS MARS-E.

report directly to the CGI Security Officer with the ability to elevate issues or concerns directly to the COHBE Security Officer.

The CGI Security Manager will develop and maintain the Exchange Plans of Action and Milestones (POA&M)[4]

Security Policy Implementation

This policy will be translated and refined into greater detail using the following framework to ensure appropriate review, approval, and oversight.

COHBE Security Business Processes

These documents provide the basic guidance for how routine business will be conducted; consistent with the COHBE Organizational Policies. Security Business Processes may be developed in response and support of an Organizational Policy or as determined by the COHBE Board of Directors or CEO. Security Business Processes are intended to be long lasting direction as to how COHBE and the Exchange are to operate and conduct business in a manner that preserves security controls.

COHBE Security Business Procedures

These documents provide the remaining details regarding the who, what, when, where, and how operations and business related to security are to be conducted. Security Business Procedures support and are consistent with Security Business Processes and may be supplemented with other items such as working aides, checklists, memos, and guidelines. Business Procedures are reviewed, refined, and updated as determined by the COHBE COO based on business and operational needs or in response to changes in Business Processes. COHBE Security Business Procedures may be limited in scope to an individual business unit.

CGI Security Policies

These documents provide high level direction for the operation of both COHBE and the Exchange. CGI Security Policies support and are consistent with and supportive of COHBE's Security Business Processes and Procedures. Exchange Security Policies are developed in response to required compliance activities and as needed to provide high level operational guidance. Exchange Security Policies are created and maintained as determined by the CGI Security Officer based on business and operational needs or in response to changes in superior governance documents.

CGI Security Business Procedures

These documents provide the remaining details regarding the who, what, when, where, and how Exchange security operations are to be conducted. Exchange Security Business Procedures support and are consistent with Exchange Security Policies and may be supplemented with other items such as working aides, checklists, memos, and guidelines. Exchange Security Business Procedures are reviewed, refined, and updated as determined by the CGI Security Officer based on operational needs or in response to changes in Exchange Policies.

[4] As required by CMS MARS-E.

Program Elements

The COHBE Security and Privacy program will at a minimum address the following elements.

- Access Control
- Awareness and Training
- Audit and Accountability
- Security and Assessment Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity
- Program Management

And other elements as may be identified by the CEO or CFO or through application of risk management.

Exceptions:

Exceptions to this policy may be authorized by the Board of Directors or CEO upon recommendation of the COHBE Security Officer. Exceptions will be reported to the Board of Directors and reviewed annually by the CEO. The Security Officer will develop plans for resolving exceptions in coordination with the CFO.