CVS HEALTH
INFORMATION SECURITY CONTROLS

CVS Health offers security and privacy controls and programs to ensure the confidentiality, integrity and availability of client and member data. Our programs provide the framework for the protection of corporate information assets through established policies, procedures, controls, and programs. Our Information Security policies and procedures regarding information confidentiality provide for protection against unauthorized access, disclosure, modification, or destruction of sensitive and pertinent computerized data files.

The following will provide an overview of the many programs in place at CVS Health. We employ effective security and privacy programs, standards and procedures in support of stringent industry standards, such as NIST 800-53, ISO 27000, and PCI-DSS.

The controls and programs address the following:

- Regulatory and Industry Mandates:
  - SOX
  - PCI-DSS
  - HIPAA
  - SOC2 Type II (Security & Confidentiality)
- External Customer Requirements:
  - Clients
  - Members
  - Health care professionals
- Internal Customer Needs:
  - Business operations
  - Legal/Corporate Compliance
  - HR/Employees
  - IT/Sales and Marketing.

THE RISK ASSESSMENT PROCESS

The Risk Assessment process includes:

- Vulnerability Scans of the Internal and External Network
- PCI Scans of the Perimeter Network
- Pre-production Vulnerability Scans
- Web Application Scans
- Penetration Testing
- Vulnerability Classification and Management
- Wireless Rogue Testing
- Change Management and Scan Notification

TREATING SECURITY RISKS

The Business Unit Leader is ultimately accountable for the risk or vulnerability that exists on that Business Unit's Technology Resource or Information Asset. The Business Unit Leader may delegate the documentation or resolution of that risk or vulnerability to an appropriate designee, but is ultimately accountable for the remediation of risk. The designee or remediation owner documents the effort required to resolve each identified risk or vulnerability. The expected effort required, including specific project details and timelines for remediation, is specified on the eGRC Archer ISRM Risk Observation record.

THIRD PARTY RISK MANAGEMENT

CVS Health maintains a comprehensive Third Party Risk Management program. All third parties that store, process, transmit, or destroy sensitive or personal information are assessed to ensure minimum CVS Health security and privacy requirement are in-place. Assessment are performed at a defined frequency based upon the risk profile assigned by CVS Health.

INTERNAL AND EXTERNAL PENETRATION TESTING

Penetration testing occurs at varied frequencies, but occurs at least annaully. The scope of testing includes PBM and Retail Environments, social engineering, web applications and physical security. The Information Security Organization (ISO) identifies suitable resources to have these services performed under their strict oversight. Appropriate Change Tickets shall be in place and management approval shall be obtained prior to conducting these penetration tests. Vendor shall document and submit the findings to ISO Security Operations for certification.

PATCH MANAGEMENT PROGRAM

The patch management process includes each of the following:

- **Detect** - Automated tools will be implemented to scan operating systems for missing Security Patches; detection will trigger the patch management process
- **Assess** - Assessing the criticality of the security patch will determine if it is necessary to install the patch. The severity of the issue will be balanced against any mitigating factors (e.g., current security measures already address or diminish the risk) to determine the overall threat to CVS Health, which will drive the timing for implementation of the security patch.
- **Acquire** - If the vulnerability is not addressed by existing security measures, the relevant Security Patch should be identified for implementation.
- **Test** - Security patches will undergo a testing process to identify any ramifications before being rolled out in a production environment.
- **Deploy** - The security patch will be deployed to relevant systems. There will also be confirmation that the system operation is not affected, including whether a rollback or backup-restore plan is needed.
- **Maintain** - Monitoring of vendor communications and appropriate channels will be maintained regarding the release of security patches and the timely identification of new patches.

ANTI VIRUS, ANTI SPAM AND ANTI SPYWARE PROGRAM

All Windows based computers have standard CVS Health managed antivirus software installed. Our AV update system is automated. A schedule is established whereby antivirus definitions are downloaded from the vendor's website to central distribution servers.

ENFORCEMENT OF MINIMUM SECURITY BASELINES

CVS Health has defined Minimum Security Baselines (MSB) for all hardware platforms that store, process and/or maintain sensitive or personal information. These established baselines are reviewed at least annually and are updated as relevant threats or risks are detected. Auditable reports are produced on a defined frequency and Information Security works with IT for any remediation that may be required. After remediation, validation reports are run to ensure compliance.

WORKSTATION SECURITY

Workstation security controls include, but are not limited to:

- Administrative privileges are prohibited and granted by exception only. All Workstations are built using a secured image defined by the minimum security baseline requirements
- Storing media in a secure and controlled space (e.g., locked cabinets or desks for removable media)
- Maintaining a "clear desk", "clear screen" for media and computer screens
- Locking computing sessions via password protected screen savers
- Securing laptops and remote/mobile devices after business hours via cable locks or in locking cabinets
- Using screen covers when working with ePHI in common work areas.

24X7 NETWORK MONITORING

Logging and monitoring network devices, systems and application assets is accomplished by collecting logs from operating systems, databases, applications, and Network Devices. Authentication logs and Application logs which record events, exceptions and other security-relevant events from critical systems will be collected by ISO. These event logs include, at minimum, the following:

- User identification
- Type of event
- Date and time
- Success or failure indication
- Origination of event
- Identity or name of affected data, System component, or resource.

The Security Operations Center (SOC) is responsible for providing centralized computer security logging and correlation. Alerts can be set up to notify the management of any undesirable activity. Logs are routinely reviewed by dedicated staff. Comprehensive Security Information and Event Management (SIEM) tools used within CVS Health include:

- Splunk – Application logging
- ArcSight – Core Security logs and monitoring
- Digital Guardian – DLP & Desktop logging
- Guardiam – Database monitoring (PCI cardholder data)
- Cisco Sourcefire – IDS/IPS
- Symantec – Anti-Virus
- FireEye – Advanced Malware Detection and Containment

INTERNET CONTENT FILTERING

CVS Health employs controls to manage access to Internet based resources using commercially reasonable vendor supported solutions. Preventative controls are designed to minimize the risk of malicious software and prevent access to Internet resources as governed through the CVS Health Acceptable Use policy.

WEB APPLICATION SECURITY PROGRAM

CVS Health maintains a Web Application Security program for development of both new and existing applications. The topics covered in this program include, but are not limited to, authentication, authorization, session management, data security, secure coding practices, secure web server configuration, and general guidelines.

DEVELOPER TRAINING PROGRAM

All CVS Health developers must attend required annual security training that incorporates security checks into each phase of the software lifecycle. In addition, the system engineering process policy (required for all software projects) provides specific quality checkpoints to ensure readiness for moving forward in the project lifecycle.

INFORMATION FORENSICS SUPPORT

CVS Health has developed a program to provide information forensics support if needed. If required, the team would:

- Participate in response activities as directed by the SOC or CSIRT-IH
- Collect forensic evidence in accordance with CVS Health procedures
- Advise the CSIRT on appropriate courses of action during an incident.

TWO-FACTOR AUTHENTICATION

CVS Health Information Security has implemented two (2) factor authentication for all administrative and remote access to Health's internal assets and network.

FIREWALL AND NETWORK MANAGEMENT

A formal Firewall and Perimeter Network management standard is designed, implemented and maintained for the evaluation, control and reduction of risks to CVS Health. The components of this standard address the management and access of the firewall architecture, management of the perimeter network; and the establishment of standards-based rules that govern the firewall.

DATA LOSS PREVENTION

CVS Health's Data Loss Prevention (DLP) program is maintained to continually evaluate the safeguards in place for unstructured sensitive information including, but not limited to, confidential and proprietary information, present in our computing environment.

INFORMATION ASSET STEWARD (IAS) PROGRAM

CVS Health has a program dedicated to asset management and policy.

The IAS has primary responsibility for Information Assets associated with the IAS's functional authority. They are responsible for ensuring:

- All Information Assets are assigned an appropriate classification
- The classifications of all Information Assets are periodically reviewed to determine if they should be changed
- All Information Assets that require access controls are identified and accounted for and the appropriate access controls are followed
- Information Assets and Removable Electronic Media containing Information Assets are appropriately labeled or marked
- Information classifications and requirements are properly communicated to, understood by, and adhered to by employees within the IAS' business unit and vendors used by the business unit
- Inventories of material Information Assets are conducted at least annually

ACCESS MANAGEMENT

A formal access request management system is in place with a dedicated team responsible for provisioning and de-provisioning access. Access is granted only after a formal access request is submitted to Identity Access Management, including all requisite approvals by management and by data stewards. Access is granted on a Minimum Necessary

basis, as determined by the approving manager equivalent, whereby the minimum amount of access (using the information security principle of least privilege) will be granted to an employee based on their job function.

USER ACCESS REVIEW

CVS Health maintains a Periodic Access Review procedure for Applications, Operating Systems and Databases compliant Regulatory and Industry Mandates for SOX, PCI and SOC2 Type II, and SSAE 16/SOC1 audit requirements.

QUARTERLY PRIVILEGED USER REVIEW

Users granted elevated privileges to claims adjudication systems where client data is stored are reviewed on at least a quarterly basis.

FILE SYSTEM INTEGRITY MONITORING AND PROTECTION

File Integrity Monitoring is maintained to alert personnel to unauthorized modification of critical system files, configuration files, or content files for all systems classified assets in scope for the Payment Card Industry Data Security Standard (PCI-DSS) or SOX compliance.

WIRELESS SECURITY PROGRAM

Wireless Access Points (WAPs) are maintained in accordance with the Payment Card Data Security Standard.

SEGREGATION OF DUTIES REVIEW

As part of CVS Health's overall SOX Compliance, the company focuses on Security Administration and User Access. Controls are in place to ensure that only authorized persons have access to financial data and applications, and then only to perform specifically defined functions. CVS Health performs a Segregation of duties (SOD) analysis at least annually as part of a Periodic Access Review against role codes assigned to business critical applications.

ENCRYPTION STANDARDS FOR DATA AT REST AND IN MOTION

Appropriate procedures and measures are in place to encrypt sensitive data transmitted over public networks in conformance to the specifications of FIPS 140-2 and to encrypt PHI and PII at rest in compliance with all applicable regulatory requirements and standards so that it cannot be accessed by unauthorized persons.
CVS Health employs strong encryption technologies with minimum key lengths of 128-bits for symmetric encryption and 1024-bits for asymmetric encryption. A documented policy for the management of the encryption keys and associated processes adequate to protect the confidentiality and privacy of the keys and passwords used as inputs to the encryption algorithm is in place.

Per the Payment Card Industry Data Security Standard, CVS Health encrypts all payment card information in accordance with the requirements and current version of the regulation.

All CVS Health laptops and desktops are encrypted using full disk encryption. By default, CVS Health prohibits the use of removable media through the enforcement of technical controls, unless required for a business operation and approved by management.

MOBILE DEVICE SECURITY STANDARDS

A formal standard is in place that provides companywide direction to CVS Health Agents on the acceptable standard for configuration and use of mobile computing devices. These devices include but are not limited to iOS or Android devices, iPads, iPods, iPhones, smartphones, tablets, etc. System administrators are responsible for the configuration and maintenance of the Mobile Device Management (MDM) server and all device profiles configured on it.

INCIDENT RESPONSE PROGRAM

A formal information security event reporting procedure exists that provides uniform instructions for CVS Health employees who provide support in the event of a potential or actual Security Incident.

These work instructions include details with respect to the appropriate and consistent response to security incidents and resolution of security incidents which must be implemented in order to reduce losses, minimize potential vulnerabilities and the effect of vulnerabilities, protect the affected Information Assets, Technology Resources and any other affected assets, protect the reputation of CVS Health, and ensure the continuity of our business in the event of a Security Incident.

EMPLOYEE TRAINING

A comprehensive Security Awareness Training Program is maintained at CVS Health. New hires are required to complete HIPAA Privacy and Security Training and Security Awareness Training within 12 days of hire and annually thereafter. Information Security (IS) provides regular awareness updates and communications to all employees and contingent workers and performs periodic simulations to test colleague awareness.

We employ the policies, procedures, and security measures described above to ensure the highest possible levels of protection against breaches of confidentiality.