A CVS Caremark White Paper

Vendor Assessment Program

Vendors who collect, use, store, process, transmit or destroy Confidential Information on behalf of CVS Caremark must be reviewed by undergoing an assessment of the Vendor's privacy protections and security safeguards. In addition, a Vendor must undergo periodic reassessments to confirm that the vendor maintained the protections and safeguards for CVS Caremark confidential information.

Executive Summary

CVS Caremark's Vendor Assessment Program supports the process to ensure that Vendors of CVS Caremark provide appropriate and reasonable protections and safeguards for CVS Caremark Confidential Information consistent with the company's privacy and information security programs. Vendors must demonstrate an ability to protect confidential information that is collected, used, stored, processed, transmitted, or destroyed on behalf of CVS Caremark. Assessments involve evaluation of the contracted vendor as well as subcontractors providing support services for the vendor that involve CVS Caremark Confidential Information. CVS Caremark Confidential Information encompasses both proprietary information, such as business data and financial records, and personal information, such as Personally Identifiable Information (PII) and Protected Health Information (PHI), which includes information received from clients and customers.

After the initial assessment with a determination that the Vendor may handle Confidential Information, Vendors must undergo reassessment on a periodic basis to ensure appropriate protections for the Confidential Information. In addition to the periodic reviews, a data breach or security incident will prompt an immediate reassessment.

Each assessment is based on various parameters, including the type of services, type of information, and location of vendor involved. Through the assessment process, certifications, SSAE 16 SOC 2 Reports, and, most importantly, responses to the CVS Caremark Standard Information Gathering (SIG) questionnaire, are reviewed to assess the protections and safeguards for consistency with CVS Caremark policies. CVS Caremark requires each vendor to validate SIG questionnaire responses with supporting documentation. The SIG is aligned with existing standards, including ISO 27002:2005, ISO 15489:2001, PCI-DSS, NIST, NAID COBIT, and incorporates FFIEC guidance. The assessment reports are then provided to the Vendor Review Committee for voting in order for a vendor to achieve approval as a Privacy Compliant Vendor. A single denial vote will cause denial of a vendor.

The Vendor Assessment Program provides CVS Caremark with an effective method to assess vendor privacy and security controls to ensure appropriate safeguards for the Confidential Information of CVS Caremark and its clients and customers.

Overview

The Vendor Assessment Program assesses CVS Caremark Vendors' protections and safeguards surrounding the CVS Caremark Confidential Information entrusted to them. Vendors who collect, use, store, process, transmit or destroy Confidential Information on behalf of CVS Caremark must demonstrate the implementation of appropriate controls to ensure the confidentiality, integrity, and availability of Confidential Information. CVS Caremark maintains the Vendor Assessment Program to ensure that our Vendors operate consistent with CVS Caremark policies and procedures related to privacy, security, and data management consistent with the type, sensitivity, and scope of the information involved. The Vendor Assessment Program satisfies Payment Card Industry (PCI) requirements, the Massachusetts Data Privacy Law, as well as other regulatory requirements.

Technical Assessment

Foundation for the Assessment

CVS Caremark's assessment process is modeled after the BITS Shared Assessment process which was created by leading financial institutions, the 'Big 4' accounting firms, and key service providers and is aligned with existing standards including

- ISO 27002:2005
- PCI DSS
- NIST
- COBIT
- FFIEC Guidance

The Shared Assessments founding organizations recognized the need for a standardized methodology that could be used to assess providers of outsourced services. CVS Caremark holds a corporate membership in the Shared Assessments group and is an active participant on the Steering Committee.

Initiation of the Assessment Process

CVS Caremark assessors begin by contacting Business Unit management to make them aware of the assessment process and to establish joint communication with the vendor. Since the Business Unit "owns" the relationship with the vendor, Business Unit involvement is important to ensure the vendor's cooperation and responsiveness. The assessor obtains copies of pertinent documentation, such as:

- Contract or proposed Contract
- Statement of Work
- Non-disclosure Agreement
- Business Associate Agreement
- Certifications
- SSAE 16 SOC 2 reports.

Assessment Scope

Assessments include

- Kick-off meeting/notification to Business Unit and Vendor
- Review of scope of services and location where services are provided
- Evaluation of confidential data types involved

- Review of contract/statement of work, non-disclosure agreement, and business associate agreement (if PHI)
- Evaluation of SIG questionnaire and investigation of responses
- Network vulnerability assessment
- Review of policies, procedures, and standard documents
- Preparation of report of observations

SIG

Standard Information Gathering (SIG) questionnaires are a key component of the data gathering to begin the assessment process. The SIG questionnaire contains questions in several categories to assist in establishing the security controls and level of maturity of the security programs of the vendor. SIG categories include:

- Risk Management
- Security Policy
- Organizational Security
- Asset Management
- Human Resource Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Information Systems Acquisition and Maintenance
- Business Continuity and Disaster Recovery
- Compliance

The SIG is based on the BITS Shared Assessments Group Standard Information Gathering (SIG) tool originally promulgated by the financial industry and is modified to incorporate healthcare requirements for security controls. Vendors are required to respond to all questions on the SIG. The assigned assessor reviews the responses and obtains documentation from the vendor to validate responses.

Subcontractors

Vendors are required to disclose any subcontractors used, with explanation of the services provided in support of the CVS Caremark contract, as well as locations of any subcontractor services. This information is evaluated in conjunction with the primary vendor assessment.

Assessor Assignments – Contiguous United States and Offshore

CVS Caremark recognizes the unique circumstances associated with protection of data in offshore environments. In these cases, onsite assessments are done on an annual basis. Offshore assessments may be performed by our internal assessors, or through carefully selected external assessment vendors with qualified staffing in the offshore regions used by CVS Caremark. Our external assessment partners are required to use assessors who are Certified Information Systems Security Professionals (CISSP) or Certified Information Systems Auditors (CISA), with work reviewed by a second layer of management within the external assessment firm. The final report is then reviewed by Vendor Assessment Program management at CVS Caremark prior to committee voting.

The Assessment Report

A confidential report is prepared by the assessor detailing the assessment process and the results of the assessment, with a determination regarding the vendor's acceptability for handling confidential information. The report is provided to the Vendor Review Committee for voting to approve or deny the vendor. Reports are treated with confidentiality based on Non-disclosure Agreements between the vendors and CVS Caremark.

Vendor Review Committee

Assessment results are entered into the management system and initiate appropriate automated notifications. Committee members review the assessment report and conclusion, then vote to approve or deny use of the vendor. Vendor Review Committee Members include representatives from Compliance, Privacy Office, Information Security and Corporate IT Shared Services encompassing representation at the Director level, Vice President or above.

A single committee denial vote causes the vendor to be denied. Denials when related to reassessment of an existing vendor may initiate a process to cease business with the vendor if deficiencies cannot be promptly resolved.

Reassessments

Each vendor approved for use as a Privacy Compliant Vendor undergoes reassessment on a scheduled basis to reaffirm that the vendor continues to maintain the necessary control environment to provide adequate protection for CVS Caremark confidential information. The reassessment schedule is based on the VARR score, with high risk vendors being assessed on an annual basis. Vendors with offshore locations and vendors who impact Payment Card Industry (PCI) data are also assessed on an annual basis, regardless of VARR score.

Conclusion

CVS Caremark's Vendor Assessment Program provides comprehensive controls and reporting mechanisms to keep abreast of vendor relationships supporting CVS Caremark to better safeguard the confidential information of our clients.