CVS Health®

Enterprise Person Hub (EPH) Audit

Scope & Objectives

Engagement Details
Executive Summary

Enterprise Person Hub (EPH) is intended to provide consistent and seamless knowledge of an individual's identity across multiple lines of business that will improve the constituent experience and increase business agility. EPH has assigned and currently manages over 592M CVS IDs, 1.9B source records, 3.6B transactions per year, and 8.1M searches per day over 40+ Enterprise consumers across PBM, Retail, Specialty, Aetna, Digital, IPP, A4L, and HCB.

EPH consumes data from 13 source systems to resolve a person's identity based on demographic and other identifiable data. EPH matches source records using probabilistic matching techniques and identifies the same "individual" within/across source systems. EPH data is only used for matching and search functions and access to the data is protected by system enforced security controls.

Audit Scope: Ensure technical controls in place are designed and operating effectively to support CVS IDs creation and management within Enterprise Person Hub.

Engagement Details
Objectives & Inherent Risks

Objective Area	Related Inherent Risk*	Key Areas of Focus
Controls are in place to ensure ID creation is managed adequately.	CVS IDs may unintentionally be created, updated, or deleted resulting in erroneous data in EPH.	• CVS IDs are created, updated/edited, and deleted completely and accurately, and to ensure duplicates do not exist
Data integrity controls are in place to ensure data entering EPH is complete and accurate.	Data integrity and daily balance controls between the source systems and EPH are not in place and the data does not reconcile for completeness and accuracy	• Data validation checks are performed between the source systems and EPH • Data integrity alerts are communicated and remediated timely per defined SLAs

Access controls are in place to ensure access to the database is appropriately managed by authorized individuals	Access to the database may not be adequately restricted or monitored, resulting in unauthorized access and changes	• Access to IBM MDM is restricted adequately
		  • Provisioning
		  • Recertification
		• Access activities are logged and monitored

***Reflects the level of risk that exists in the absence of controls**

Engagement Details
Objectives & Inherent Risks

Objective Area	Related Inherent Risk*	Key Areas of Focus

Data protection controls are in place to ensure data is secured in transit and at rest	Data in transit and at rest is not secure to prevent unauthorized access to confidential, proprietary, or otherwise sensitive data	• Ensure data in transit and data at rest is encrypted in accordance with company standards
		  • Encryption/masking methods are used for protecting data stored in IBM MDM
		  • Encryption methods are in place for data in transit

Scalability and availability controls are in place to support large volumes of data	Technology infrastructure supporting EPH is unable to support large volumes of data	• EPH is measured and monitored to ensure the technology infrastructure is scalable to support large volumes of data

***Reflects the level of risk that exists in the absence of controls**


CVS Health®