CVS Health®

Enterprise Person Hub (EPH) Audit

Kick-off Meeting

October 20, 2021

Agenda

Engagement Details

Key Milestones

Key Contacts

Expectations

Next Steps

Appendix

Standard Terminology
Escalation Protocol

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

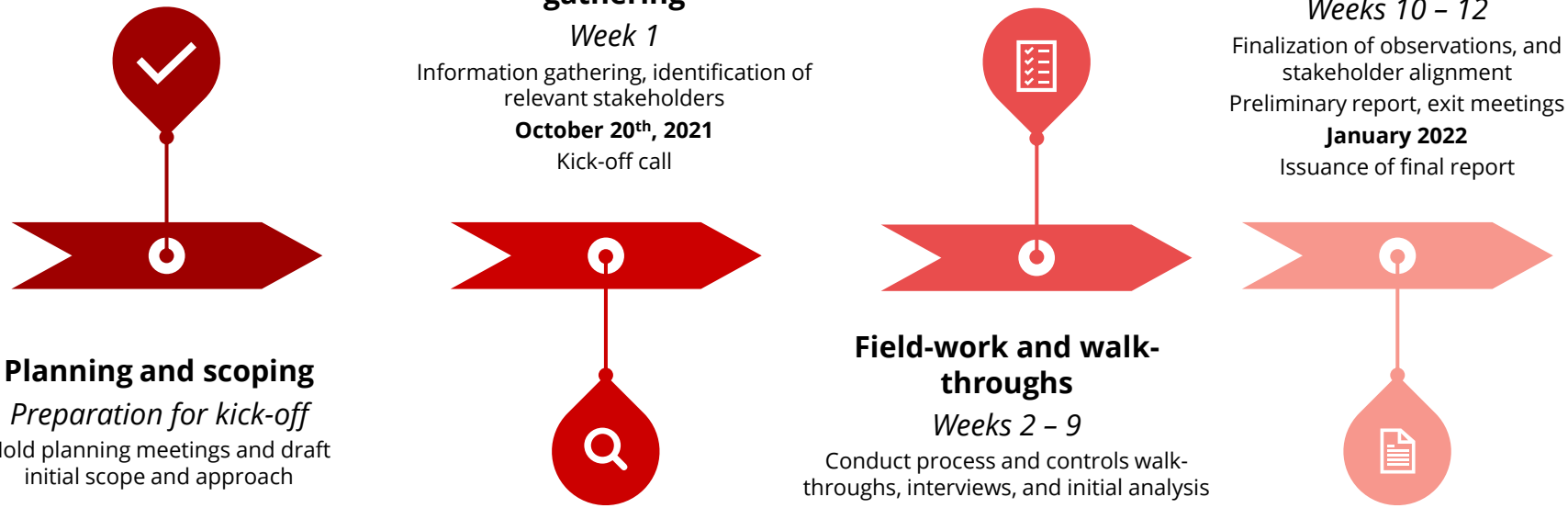
***Reflects the level of risk that exists in the absence of controls**

Engagement Details
Business Input

Input required from the Business

- Recent changes in process or organization
- Various sub-processes or multiple locations
- Any internal/external reviews (e.g. consulting, external audit, process reengineering)
- Limitations in resources or process
- Existing issues
- Other concerns

Audit Timeline



Planning and scoping

Preparation for kick-off

Hold planning meetings and draft initial scope and approach

Kick-off and information gathering

Week 1

Information gathering, identification of relevant stakeholders

October 20th, 2021

Kick-off call

Field-work and walk-throughs

Weeks 2 – 9

Conduct process and controls walk-throughs, interviews, and initial analysis

November – December 2021

Reporting

Weeks 10 – 12

Finalization of observations, and stakeholder alignment

Preliminary report, exit meetings

January 2022

Issuance of final report

Key Contacts
Internal Audit & Business Area

Internal Audit Team		
Role	**Name**	**Responsibilities**
Audit Director(s)	Lynn Atkin Ron Roy	Oversight/guidance and liaison with Business Owners
Audit Manager	Sol Vazquez	Oversight/guidance and liaison with Business Owners
Lead Auditor	Jason Nazare	Liaison with Business Owners, develop project plan and lead team
Staff Auditors	Monika Godara, Seun Mafi, Tyrell Jarrett, Terri Ann Quiambao Moriah Striegel	Liaison with Business Owners, controls analysis and test execution
Business Line Contacts		
Role	**Name**	**Responsibilities**
Primary POC Executive Management	Kathleen Kadziolka	Report Owner (VP Level or above)
Primary POC	Carmen Malangone Nadesan Wijendran Nijesh Narayanankutty David Dessommes	Transfer knowledge of key business functions, process documentation and key control evidence to the Internal Audit team; control validation and issue ownership.

Key Business Line Contacts listed are a starting point for discussion and not meant to indicate these individuals are responsible for the process, observations and/or report.

Expectations
Internal Audit & Business Line

What you can expect from Internal Audit:

- Prompt notification of concerns, such as audit issues or roadblocks
- Potential unfamiliarity with business process
- Focus on key areas of high risk
- Ongoing communication throughout the project
- Travel to primary location(s), as necessary
- Draft Audit Report will be provided for the business' review at least 24 hours in advance of the close meeting

What Internal Audit expects from your Team:

- Awareness and engagement
- All relevant documentation, including process/control documentation, policies & procedures, key reporting and dependencies be provided promptly during the planning phase
- Management and staff will make reasonable time available for interviews, provide prompt responses to follow-up questions and deliver requested support or information by agreed upon due dates
- All layers of management in your Team's organization are kept informed of identified exceptions and issues
- Management will review the Draft Audit Report in advance of the close meeting to allow for a more targeted discussion

Additional Information to Consider

AuditBoard is the audit management tool used by Internal Audit

Internal Audit may leverage this system for the following aspects of the project:

- Centrally manage and communicate requests
- Gain alignment with verbiage of Findings and Observations
  - Request Management's Remediation Plan for inclusion within the Audit Report
- Management of Findings upon the conclusion of the audit

Note: Please do not upload any PII / PHI to AuditBoard; please discuss with Internal Audit the most appropriate means to transmit any sensitive documentation requested as part of this project

Audit Surveys will be sent at the conclusion of the audit to the relevant business contacts

Audit Surveys help Internal Audit aggregate feedback on what went well during the project and areas of opportunity for the team to reflect on going forward

- Survey will be deployed from AuditBoard typically within 1-2 weeks of report issuance
- Results are gathered centrally by our Department administrative team and feedback is anonymously provided back to the respective Internal Audit team

Next Steps

- Issuance of Kick-Off deck to formalize kick-off of the project, 10/20
- Schedule walkthrough meetings with relevant business contacts starting the week of 10/25.
- Schedule periodic status meetings with the business to keep open line of communication starting the week of 11/1.

Appendix

Standard Terminology
Overall Control Environment Opinion

Effective	Overall, controls are appropriately designed and functioning as intended. Control weaknesses, if noted, do not threaten the effectiveness of the process reviewed.
Mostly Effective	Except for the issues noted, controls in place provide reasonable assurance that business risks are adequately mitigated.
Improvement Needed	One or more significant control weaknesses exist that require prompt action to prevent the process from becoming ineffective.
Ineffective	Control weaknesses are pervasive or one weakness is so severe that it impacts the entire operation under review. Immediate management attention is needed to remediate the issue identified.

Standard Terminology
Ratings & Management Action Plan

The rating of findings drives the timing of remediation and also the level of management that is responsible for developing and implementing action plans.

High	The identified risk requires the immediate attention of department and senior management to prevent the process from becoming ineffective, and an agreed-upon action plan for resolution is needed.
Medium	The identified risk requires the near-term attention of the responsible manager. There should be an agreed-upon action plan for its resolution.
Low	The identified risk does not warrant immediate attention; however, there should be an agreed-upon action plan for ultimate resolution.
Deficiency	If SOX related, rating categories will be assessed as Deficiency, Significant Deficiency, or Material Weakness. *Note: While the audit will focus on the objectives previously noted, IA has a responsibility to assess any additional risks identified during the audit, and report any issues identified. Where applicable, issues will also be evaluated against requirements for Sarbanes-Oxley or other regulatory standards.*

Each Management Action Plan requires a remediation due date which is tracked by IA.

Due Date	Reflects the date when Responsible Parties/Management will complete the agreed upon Action Plan, which includes sending data to Internal Audit to validate remediation efforts.
Remediation Date	Reflects the date when Internal Audit will have validated the implemented Management Action Plan effectively closed the issue.

Escalation Protocol

Potential Causes for Escalation

- Data requests not received within expected timeframes
- Data provided does not align with follow-up requests for clarification
- Key attendees miss walkthrough meetings following confirmed schedules
- Internal Audit is denied access to key data or people that may impact findings
- Management accepts a level of residual risk not acceptable to the organization
- Management is not aligned with identified issues, risk priority ratings and/or the overall audit opinion

Escalation Process – when one or more of the above events occur

- Convey the issue to the next level of management
- The responsible SVP / VP may be notified of causes which delay audit execution
- Escalations may be tracked and reported during recurring status meetings with management
- The CAE may discuss with Senior Management and the Audit Committee, if necessary


CVS Health®