Devolutions

Devolutions Password Hub

HIPAA SECURITY RULE ASSESSMENT

April 2022

INTRODUCTION

Password Hub

Password Hub Business is a secure and cloud-based password manager for teams. It empowers organizations to easily and securely vault and manage business-user passwords, along with other sensitive information, through a user-friendly web interface that can be quickly, easily and securely accessed via any browser.

HIPAA Security Rule

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a United States federal statute that regulates the privacy and the security of electronic Personal Health Information (ePHI). Covered Entities must implement security controls to protect ePHI that are consistent with the requirements of HIPAA's Security Rule.

HIPAA's Security Rule describes controls that apply to Covered Entities and to Business Associates who process ePHI on their behalf. Password Hub does not process ePHI but may be used to grant access to systems containing ePHI. Following an analysis of the applicability of the Security Rule's requirements, some controls have been carved out of this assessment as the do not apply to Password Hub's service offering.

HIPAA's Security Rule is not prescriptive: security control requirements refer to current industry standards without providing specifications. Security controls described herein reference the United States Department of Health and Human Services' Security Rule guidelines.

Object

This document is divided into two sections:

- **The first section, «Devolutions»**, consists in a review of Devolutions Inc.'s information security management program, internal security practices and information security controls' consistency with applicable industry standards, as defined by the National Institute of Standards and Technology Special Publication 800-53 r.5 Security and Privacy Controls for Information Systems and Organizations (NIST-SP-800-53r5).

- **The second section, «Password Hub»**, consists in a review of Password Hub's security controls' consistency with applicable industry standards, as defined by the National Institute of Standards and Technology Special Publication 800-53 r.5 Security and Privacy Controls for Information Systems and Organizations (NIST-SP-800-53r5).

	Control requirement - Reference	Validation
Organizational Requirements		
	Policies and Procedures - ¤164.316(a)	Devolutions has implemented and maintains an information security program plan and policies. The plan details roles and responsibilities, including security and privacy functions, security controls and procedures, and a review process. Policies and procedures are consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.13 Program Management
	Documentation - ¤164.316(b)(1)	Devolutions maintains documentation regarding its information security program, as well as records of actions and activities that affect its services, such as access logs and security incidents. Documentation is reviewed and updated annually, and relevant records made available to customers. Documentation is consistent with industry standards, as defined by NIST SP 800-53r5 Ð3.13 Program Management.
Administrative Safeguards		
	Security Management Process - 164.308(a)(1)	Devolutions has implemented a comprehensive incident management plan that is managed by the Chief Security Officer. Policies and procedures have been implemented to prevent, detect, contain, and correct security violations. The program governs the implementation of reasonable and appropriate controls that comply with industry standards.
	Risk Analysis (R) - 164.308(a)(1)(ii)(A)	Devolutions has implemented risk analysis and reporting procedures. Controls are in place to monitor and detect potential risks, and procedures to mitigate or remediate identified risks are implemented. Roles and responsibilities are defined, and the program is managed by a senior executive. Risk analysis policies are consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.13 Program Management and 3.16 Risk Assessment.
	Risk Management (R) - 164.308(a)(1)(ii)(B)	Devolutions has implemented risk management policies. Controls are in place to monitor and detect potential risks, and procedures to mitigate or remediate identified risks are implemented. Roles and responsibilities are defined, and the program is managed by a senior executive. Findings are presented to executive management. Risk management policies are consistent with industry standards, as defined by NIST SP 800-53r5 Ð3.13 Program Management and 3.16 Risk Assessment.
	Sanction Policy (R) - 164.308(a)(1)(ii)(C)	Devolutions has implemented a sanction policy. Employees are made aware of policies and procedures, including sanctions for non-compliance. Employees receive training and must acknowledge policies and procedures. Sanction policy is consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.2 Awareness and Training.
	Information System Activity Review (R) - 164.308(a)(1)(ii)(D)	Devolutions conducts information system activity reviews. Devolutions correlates user activity logs with information from targeted systems, periodically reviewing records of activity and security events. Discrepancies are addressed in accordance with policies. Information system activity reviews are consistent with industry standards, as defined by NIST-SP-800-53r5 Ð3.3 Audit and Accountability.
	Assigned Security Responsibility - 164.308(a)(2)	Devolutions conducts information system activity reviews. Devolutions correlates user activity logs with information from targeted systems, periodically reviewing records of activity and security events. Discrepancies are addressed in accordance with policies. Information system activity reviews are consistent with industry standards, as defined by NIST-SP-800-53r5 Ð3.3 Audit and Accountability.
	Authorization and/or Supervision (A) Ð 164.308(a)(3)(ii)(A)	Devolutions has assigned information security and privacy resources with sufficient authority to govern the information security program. Policies document roles and responsibility regarding information security procedures and activities. Assigned security responsibility is consistent with industry standards, as defined by NIST-SP-800-53r5 Ð3.13 Program Management.
	Information Access Management - 164.308(a)(4)	Devolutions leverages zero knowledge principles to ensure customer data is not accessible without authorization. Access controls leverage role-based access principles and IaaS provider security features to restrict access to the platform. Information access management is consistent with industry standards, as defined by NIST-SP-800-53r5 Ð3.1 Access Control and 3.19 System and Information Integrity.

	Access Authorization (A) - 164.308(a)(4)(ii)(B)	Devolutions leverages zero knowledge principles to ensure customer data is not accessible without authorization. Access controls leverage role-based access principles and IaaS provider security features to restrict access to the platform. Access authorization is consistent with industry standards, as defined by NIST-SP-800-53r5 Ð 3.1 Access Control and 3.19 System and Information Integrity.
	Access Establishment and Modification (A) - 164.308(a)(4)(ii)(C)	Devolutions leverages zero knowledge principles to ensure customer data is not accessible without authorization. Access controls leverage role-based access principles and IaaS provider security features to restrict access to the platform. Access establishment and modification is consistent with industry standards, as defined by NIST-SP-800-53r5 Ð 3.1 Access Control and 3.19 System and Information Integrity.
	Security Awareness and Training - 164.308(a)(5)	Devolutions has implemented a security awareness and training program. Employees receive training upon hiring and yearly thereafter and must acknowledge policies and procedures. Security awareness and training is consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.2 Awareness and Training.
	Security Incident Procedures - 164.308(a)(6)	Devolutions has documented and implemented security incident procedures that include measures to prevent, detect, contain, and correct security events. Roles and responsibilities are defined, and the program is managed by a senior executive. Security incident procedures are consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.8 Incident Response and 3.13 Program Management.
	Response and Reporting (R) - 164.308(a)(6)(ii)	Devolutions has implemented response and reporting procedures, derived from a documented risk management policy. Controls are in place to monitor and detect potential risks, and procedures to mitigate or remediate identified risks are implemented. Roles and responsibilities are defined, and the program is managed by a senior executive. Findings are presented to executive management. Response and reporting procedures are consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.13 Program Management and 3.16 Risk Assessment.
	Contingency Plan - 164.308(a)(7)	Devolutions has implemented contingency controls that are based on backup and restore capabilities and leverage IaaS high availability and redundancy mechanisms for additional security and reliability. Business continuity and backup procedures are reviewed and tested annually. Devolutions does not have a formal disaster recovery plan to respond to potential disruptions, should IaaS mechanisms fail. Contingency plan is partially consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.6 Contingency Planning.
	Evaluation - 164.308(a)(8)	Devolutions undergoes multiple evaluations on a yearly basis to determine the effectiveness of its information security program. Evaluations are consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.4 Assessment, Authorization, and Monitoring and 3.13 Program Management.
Physical Safeguards		
	Facility Access Controls - 164.310(a)(1)	Devolutions leverages third party infrastructure to host the service. Facilities access controls are included in the service agreement with the IaaS. Microsoft Azure provides documentation regarding its compliance with various industry standards: https://azure.microsoft.com/en-ca/overview/trusted-cloud/compliance/.
	Workstation Use - 164.310(b)	Devolutions has implemented an Employee Manual. Employees are made aware of policies and procedures, including proper use of corporate assets (i.e. workstations). Employees receive training and must acknowledge policies and procedures. Workstation use is consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.2 Awareness and Training.
	Workstation Security - 164.310(c)	Devolutions has defined and implemented configuration management policies and procedures, including workstation security requirements. Encryption and endpoint management ensure that access to workstations is restricted, minimizing endpoint risk. Administration rights are restricted, minimizing the risk of privilege escalation. Workstation security is consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.5 Configuration Management.
	Device and Media Controls - 164.310(d)	Devolutions leverages third party infrastructure to host the service. Device and media controls are included in the service agreement with the IaaS. Controls include media disposal and sanitization procedures. Microsoft Azure provides documentation regarding its compliance with various industry standards: https://azure.microsoft.com/en-ca/overview/trusted-cloud/compliance/

	Data Backup and Storage (A) - 164.310(d)(2)(iv)	Devolutions has implemented data backup and storage procedures that leverage IaaSÕs backup and replication mechanisms for additional security and reliability. Backup procedures are reviewed and tested annually. Data backup and storage are consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.6 Contingency Planning.
Technical Safeguards		
	Unique User Identification (R) - 164.312(a)(2)(i)	Devolutions ensures that accounts are unique, and that users can be properly identified and authenticated. Access is further controlled through the use of MFA and encryption to establish privileged access. User identification controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Automatic Logoff (A) - 164.312(a)(2)(iii)	Automatic log-off controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Audit Controls - 164.312(b)	Devolutions maintains comprehensive audit controls that correlate user activity logs, security events, and change logs with information from targeted systems. Access rights and logs are monitored and periodically reviewed. Discrepancies are addressed in accordance with policies. Audit controls are consistent with industry standards, as defined by NIST-SP-800-53r5 Ð 3.3 Audit and Accountability.
	Integrity - 164.312(c)(1)	Devolutions leverages zero knowledge principles to ensure customer data is not accessible without authorization. Access controls leverage role-based access principles and IaaS provider security features to restrict access to the platform. Integrity controls are consistent with industry standards, as defined by NIST-SP-800-53r5 Ð 3.1 Access Control and 3.19 System and Information Integrity.
	Person or Entity Authentication - 164.312(d)	Devolutions ensures that accounts are unique, and that users can be properly identified and authenticated. Access is further controlled through the use of MFA and encryption to establish privileged access. Person or entity authentication controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.

	Control requirement - Reference	Validation
Administrative Safeguards		
	Risk Analysis (R) - ¤164.308(a)(1)(ii)(A)	Risk analysis, reporting, and notification features are consistent with industry standards, as defined by NIST SP 800-53r5 Ð 3.16 Risk Assessment.
	Information System Activity Review (R) - 164.308(a)(1)(ii)(D)	Correlation of user activity logs with information from targeted systems facilitates improves review capabilities and may be used as evidence. Content of records is consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Assigned Security Responsibility - 164.308(a)(2)	Assignment of security responsibilities within the platform facilitates information security program management by notifying and informing relevant personnel of potential security incidents. Security responsibility assignment features are consistent with industry standards, as defined by NIST-SP-800-53r5 3.13 Program Management.
	Authorization and/or Supervision (A) Ð 164.308(a)(3)(ii)(A)	Authorization is managed via Password Hub`s user and user group permissions, which requires authorization be granted to access information assets. Supervision is managed via Password HubÕs user activity event logs. Authorization and supervision controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control and 3.3 Audit and Accountability.
	Workforce Clearance Procedure (A) - 164.308(a)(3)(ii)(B)	Access to information is managed via user and user group permissions. Account provisioning logs can be audited. Workforce clearance controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Termination Procedures (A) - 164.308(a)(3)(ii)(C)	User accounts can be terminated by administrative users within the Administrative Console of the platform, facilitating compliance with termination procedures. Termination controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Access Authorization (A) - 164.308(a)(4)(ii)(B)	Access authorization controls are robust and facilitate segregation of duties and compliance with the least privilege principle. Vault-based access and user group permissions enable the implementation of role-based access policies. Dual authorization and single use credentials are robust measures of access enforcement. Access authorization controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Access Establishment and Modification (A) - 164.308(a)(4)(ii)(C)	Access establishment is protected by three layers of security controls: access requires users to be authenticated; access requires users to have permission to use credentials; access requires users to be granted rights to the vault hosting the credentials. Use of shared credentials are logged as user activity events. Access modification requires administrative permissions and are logged as system events. Access establishment and modification controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Password Management - 164.308(a)(5)(ii)(D)	Password Hub facilitates password management enforcement. Shared password is managed by system administrators and permissions are controlled at the user or user group level. Password management controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Response and Reporting (R) - 164.308(a)(6)(ii)	Password Hub facilitates the correlation of security incident information with other systems. Audit logs are sufficiently detailed to allow for correlation with event logs from other systems and reporting functions draw attention to potential incidents. Response and reporting controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.8 Incident Response.
	Data Backup Plan (R) - 164.308(a)(7)(ii)(A)	Password Hub provides industry standard backup functions that leverage IaaS high availability and redundancy mechanisms for additional security and reliability. Data can be exported by customer via API for additional safeguards. Data backup controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability, 3.6 Contingency Planning, and 3.18 System and Communications Protection.

Physical Safeguards		
	Data Backup and Storage (A) - 164.310(d)(2)(iv)	Password Hub provides industry standard backup functions that leverage IaaS high availability and redundancy mechanisms for additional security and reliability. Data can be exported by customer via API for additional safeguards. Data backup and storage are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability, 3.6 Contingency Planning, and 3.18 System and Communications Protection.
Technical Safeguards		
	Unique User Identification (R) - 164.312(a)(2)(i)	Password Hub ensures that accounts are unique, and that users can be properly identified and authenticated. User identification controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Automatic Logoff (A) - 164.312(a)(2)(iii)	Automatic log-off controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.1 Access Control.
	Encryption and Decryption (A) - 164.312(a)(2)(iv)	Password Hub uses cryptographic measures to protect data by utilizing industry standard protocols that encrypt data at rest and hash highly confidential values. Encryption and decryption controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.18 System and Communications Protection and 3.19 System and Information Integrity.
	Audit Controls - 164.312(b)	Audit controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.3 Audit and Accountability.
	Integrity - 164.312(c)(1)	Password Hub provides basic integrity control functions. Restricted write functions prevent modification and change logs document change events, but Password Hub does not provide versioning or data restoration functionality. Integrity controls are partially consistent with industry standards, as defined by NIST-SP-800-53r53.19 System and Information Integrity.
	Person or Entity Authentication - 164.312(d)	Password Hub enforces entity authentication in a layered manner: To access the platform, users must first be authenticated. To access integrated systems, users must be granted permissions to access the credentials. Authentication controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.7 Identification and Authentication.
	Transmission Security - 164.312(e)(1)	Password Hub uses cryptographic measures to protect data by utilizing industry standard ciphers that encrypt data in transit. Transmission security controls are consistent with industry standards, as defined by NIST-SP-800-53r5 3.18 System and Communications Protection and 3.19 System and Information Integrity.