HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) is a set of US federal legislative requirements for the healthcare industry and includes, among other things, standards and requirements for the administration, management, storage and transmission of Protected Health Information (PHI).

PHI is understood to be any data that relates to a person's heALTh: for example a medical test result in isolation such as a cholesterol count is not classed as PHI but it certainly would be if it were in any way associated with, or identifiable as belonging to, an individual's heALTh record. Equally, all information about a person and their relationship to their healthcare provider(s) - such as their name, address, date of birth, billing history, etc. - is considered PHI.

Blue Prism and HIPAA

Blue Prism contains a rich set of technological and administrative features that support solution designers in creating a HIPAA compliant solution. The implementation methodology and deployment framework also help to ensure the correct governance model is deployed as part of the solution to include:

- Appropriate awareness and operational training for administrative staff
- Proper change management disciplines and record keeping
- Annual review of risk assessments

Blue Prism is optimized to enable customers to implement Robotic Process Automation as part of a HIPAA compliant solution. This document references the features and functionality that are frequently utilized as part of a solution which compliment such deployments. Additional considerations also typically include: data center location and security; as well as governance and change management frameworks which are covered comprehensively within the Blue Prism Methodology.

Blue Prism Data Governance

Data Scope

The Blue Prism Delivery Methodology provides clear structure and guidance to Process Modellers at design time, encouraging them to think carefully about what data is being collected/inspected, whether it is necessary to view that data and how the nature of that data will affect its downstream management. Clear documentation is typically generated in order to capture such design time considerations and decisions.

From a software perspective, Blue Prism provides full visibility of all data being used by a process, both from a high level input/output perspective and also as part of the in-process detail. This maximizes the opportunity to provide oversight and audit of what data is being used, why it is being used and how that data is being handled.

Data Sensitivity

Sensitive data, where used, can be handled appropriately using a variety of software options:

- **Data Masking** – Where it is necessary store the full value of a particular data item (such as a password or record number), when presenting the data on screen, data masking can be used to hide all or part of the value. Likewise the data can be hashed as it is retrieved from a source system prior to being stored, for example, Password = ********; Record Number = xx-xxxxx-879.
- **Flexible-Logging** – Granular logging controls provide flexibility to apply an appropriate level of logging based on the type of process and the sensitivity of the data being managed. For processes which include processing of sensitive data, data logging could be turned-off, or alternatively set to record the decisions and actions taken but without storing any of the data.
  Additionally any Blue Prism data items which are set to be of type password are automatically omitted from the logs.
- **Data Encryption** – Specific data items identified as sensitive can be encrypted prior to being stored for later processing, likewise entire work queues can be encrypted prior to storage.
  Where such data is stored within a work queue item, the value entered as the item key is often presented in plain-text therefore it is recommended that the key does not contain sensitive information unless it is sufficiently masked.
- **Total Encryption** – Disk encryption of the Blue Prism database and log files can be implemented using Transparent Data Encryption (TDE) on the SQL Server database.

Data Management

The data captured and treated by Blue Prism in work queues and log files can be comprehensively managed using the data archiving feature which allows the selective archiving of data according to its age and the process it relates to.

The model governance framework that surrounds a typical Blue Prism software deployment also addresses the considerations necessary to achieve the responsible downstream storage/management/disposal of that data in a secure, managed and compliant manner.

Data Security

All data – whether operational or configuration related – is stored in a centralized and secure repository provided by Microsoft SQL Server. This makes the data easy to secure and govern which is one of the core architectural principles which underpin the Blue Prism technology platform and governance.

Secure user access control to the Blue Prism platform is provided natively or via integration with Active Directory Domain Services and is implemented using role-based permissions which govern access to system features and data at a highly granular level. Administrators apply detailed control over the actions and visibility that operational employees can achieve based on their role and permissions, while user credentials are subject to password complexity (such as length, inclusion of non-standard characters, upper/lower case etc.) and expiry rules, as well as re-use frequency restrictions.

Software Features

Please refer to the companion document entitled **Blue Prism Data Sheet - Operational Audit Overview** for additional information in relation to user access control, audit, and software features that provide governance of data management and security.

Further Reading

U.S. Government Printing Office: Health Insurance Portability and Accountability Act of 1996.

Blue Prism Resources

The guides listed below provide further insight into some of the features and functionality discussed within this document:

- Data Sheet – Operational Audit Overview
- Data Sheet – Credential Manager
- Data Sheet – Active Directory Integration