



Vestigo® Specification Sheet

2026



Contents

Vestigo® Specification Sheet.....	1
2026	1
Overview	4
Data Center Facilities	4
Data Backup and Disaster Recovery	4
Data Encryption and Security.....	6
Privacy.....	6
Information Supplied by End Users	6
Information McCreddie gets from the client’s use of the Application	6
Use of the Information Collected.....	7
Sharing of the Information Collected.....	7
Data Ownership	7
Authentication and Authorization	7
Password Policy.....	7
Session Length Policy	7
Lockout Policy	8
Access Control for External Users.....	8
Audit Trails	8
Logical Data Model	9
Connection to Application	9



Requirements for Client Workstations	10
Requirements for Label Printers.....	10
Resources Required from Client for Implementation and Support.....	10
Compliance	10
Code of Federal Regulations 21 Part 11.....	11
Social Security Numbers	11
Patient Financial Information	11
Further Information	11



Overview

Vestigo® is a web-based application providing automation tools for an Investigational Drug Service. The application features protocol management, electronic virtual inventories, automated drug accountability, dispensing and labeling of prescriptions, and automated protocol billing. Vestigo® was commercially released in 2004 as WebIDS. The product was renamed Vestigo® in 2012. The application is hosted and offered by McCreddie Group Software LLC (McCreddie), Ann Arbor, Michigan. McCreddie is annually audited for compliance with SOC2 Type II requirements.

Data Center Facilities

McCreddie uses secured data center facilities to operate the hosted version of Vestigo®. The data centers employed are physically located within the United States. McCreddie reserves the right to move client's data from one physical location to another as long as the following standards and processes are met.

- Data center must maintain compliance with SAS-70 or SSAE 16/SOC auditing.
 - Audit report available with a signed NDA
- Data center must provide redundant power, networking, cooling and 24x7x365 support for any issues.
- All servers are dedicated to McCreddie and are not used by any other entity.
- All servers owned or used by McCreddie will be dedicated server class machines including:
 - RAID-configured disk arrays
 - Redundant power supplies
 - Error correcting memory
 - Redundant fans
 - Built in encryption at rest
- All servers are behind a dedicated firewall (FortiGate).

McCreddie currently contracts with MS Azure for hosting the Vestigo® application.

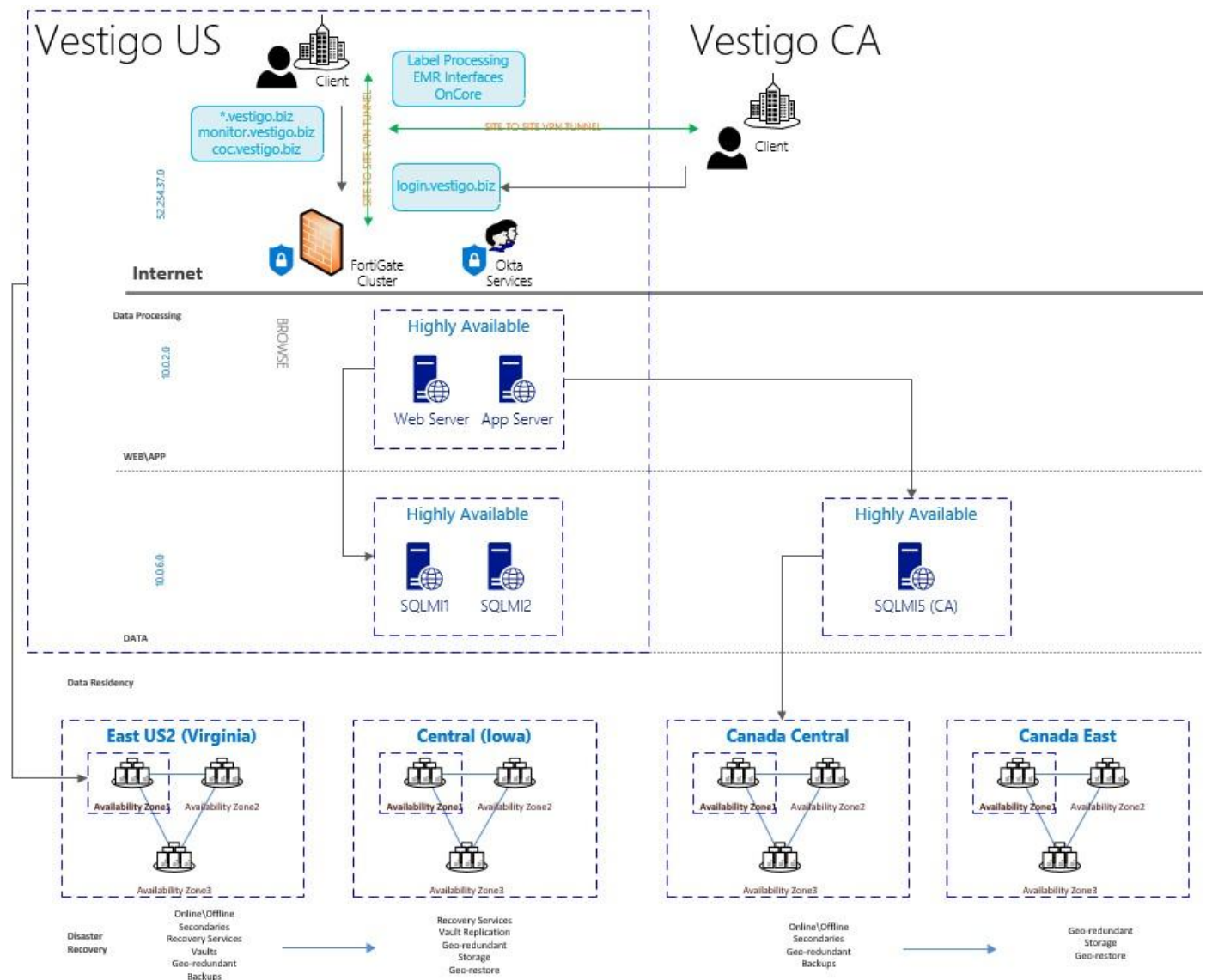
Data Backup and Disaster Recovery

- All production databases have a full back up once every 24 hours. Each backup is encrypted and transferred to a second data center (geo-redundant storage accounts).
- All production databases have an hourly transaction log backup. Each backup is encrypted and transferred to a second data center (geo-redundant storage accounts).
- All production databases have a monthly backup. Each backup is encrypted and transferred to a second data center (geo-redundant storage accounts).
- Transaction logs are stored until a successful daily backup is complete.
- Daily backups are stored for 14 days.



- Monthly backups are stored for five years.
- McCreddie maintains 24x7x365 emergency support for data recovery.
- In the event that the data center needs to be moved, McCreddie will work with the client to update any VPN tunnels/IP addresses to allow access by client to the application.

The data center model used by Vestigo® is as follows:





This data center model provides security and redundancy of client data via separation of data center facilities, internet and power providers to ensure consistent availability and decreased risk of downtime or loss of data. Data is stored geographically according to the country of residence (i.e., USA clients are stored in Vestigo® US and Canadian clients are stored in Vestigo® CA). Vestigo® is a multi-tenant solution with logical controls to separate data, and every client has their own database instance.

Data Encryption and Security

- Access to the application and underlying data is secured via either a VPN tunnel or 256-bit SSL connection.
- All data is encrypted at rest.
- All backup data is encrypted using 256-bit AES encryption.
- Data is never stored outside of a secured data center and never stored on portable devices.
- Data will not be sent via e-mail.
- Only secured FTP will be used to transmit files, if needed.
- Clients will not have direct access to the database and can only access data via the provided web interface and application reports.
- Printing of labels to the client is routed through an encrypted VPN tunnel.
- Annual completion of third-party penetration and vulnerability test.

Privacy

McCreddie Group collects information two ways:

Information Supplied by End Users

Vestigo® is a transactional system and collects many data elements supporting the research operations of the client. This data includes protocol information, participant information, financial information for interdepartmental billing and user information including names, email addresses, physical addresses, and other contact information.

Information McCreddie gets from the client's use of the Application

McCreddie may collect information about the use of the application to assist in improving the application. Information includes the browser and operating system used, user's IP address, pages visited in the application and certain error codes that the application emits. The application utilizes cookies to help maintain sessions. Log information from the server is also collected.



Use of the Information Collected

McCreddie uses the information collected to service the application and identify error conditions to assist in improving the application.

Sharing of the Information Collected

The information collected by McCreddie is used solely to support the application and provide services to the client. Information is not to be shared with any external party with the potential exception of the client's technical support team in the process of resolving a technical issue related to the application's use at that client.

If a legal request for information sharing is presented, McCreddie will contact the client's Compliance Office prior to the release of any client information to any third party.

Data Ownership

- Client data is owned by the client.
- Upon termination of agreement with client, the client's data will be downloaded and supplied to the client in a secure manner if requested or as indicated in the MSA; client's data will then be permanently purged from the servers in accordance with the MSA.
- McCreddie will only access the data for purposes of user support and application maintenance and upgrades.

Authentication and Authorization

The application only allows authenticated and authorized access beyond the login screen. All authentication and authorization is controlled by the application. Vestigo® authentication utilizes the Okta IdP platform. Usernames must be unique per user. The use of shared or common accounts is not allowed. Vestigo® supports SAML 2.0 for clients who wish to integrate into their identity management systems.

Password Policy

The default password requires at least eight characters including one character that is not a letter or a number. Users may change their own passwords at any time. Client-specific password policies will be applied, if required.

Session Length Policy

The default session length policy is to time out the application after 29 minutes of inactivity. Client-specific network policies be enforced on the desktop that impact browser time out. In the absence of such policies, the timeout value of desktop screen saver locks may be adjusted per client preference.



Lockout Policy

The application will automatically lock an account after five unsuccessful attempts at login. Accounts are unlocked by using the Okta to revalidate the user.

Access Control for External Users

Vestigo® provides pathways for users to add new users. A McCreddie team member conducting site implementation will grant client System Administrator access to the site's director/manager and/or designees. McCreddie will assist in setting up additional user accounts for new or existing clients with appropriate change request documentation. Once the client has completed implementation, the client has the ability to grant access, remove or modify access. McCreddie will not grant additional access to the system without written authorization.

Audit Trails

Vestigo® maintains several audit trails to meet compliance and practical needs. All remote access to the servers is logged via Windows Server event logs.

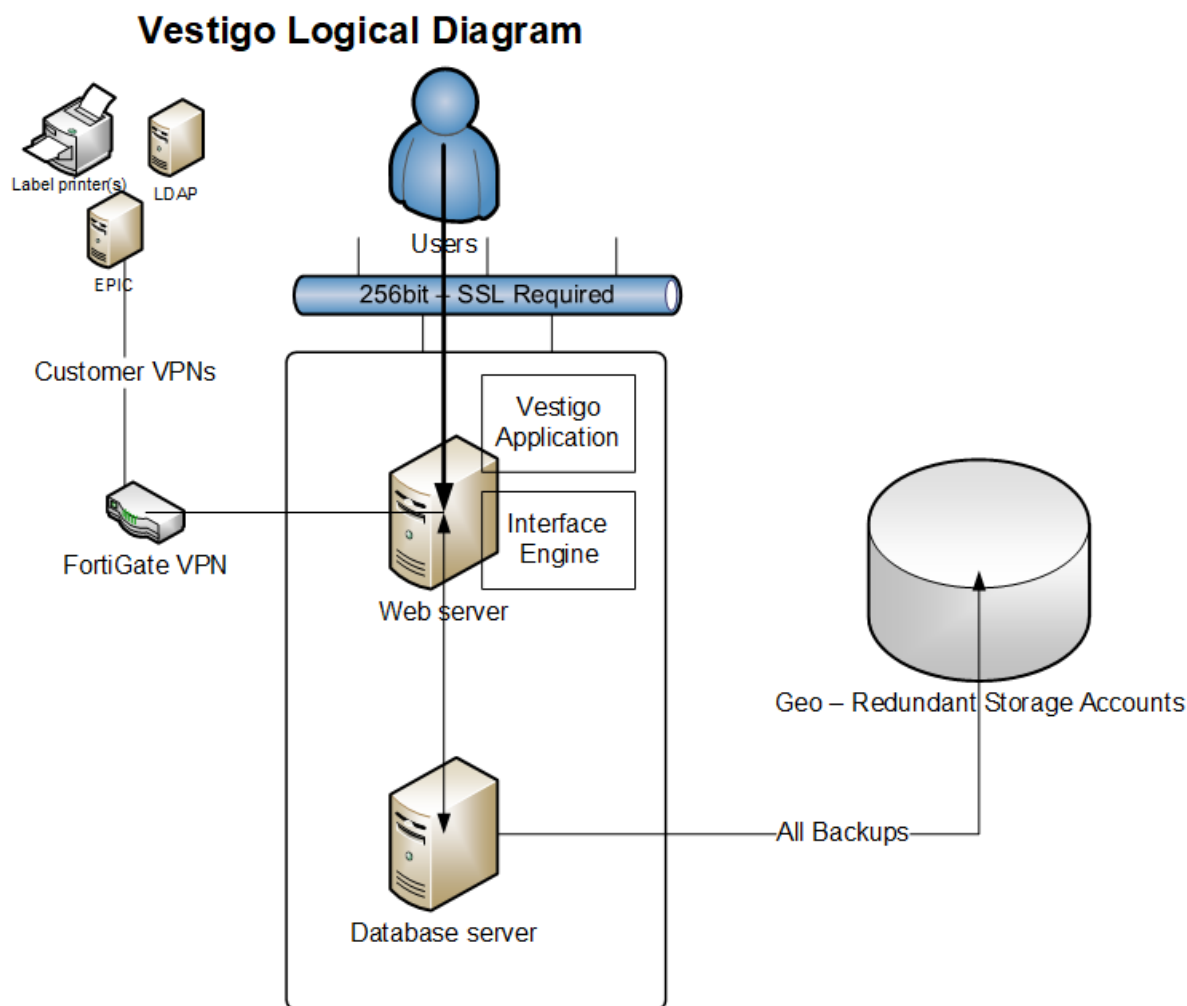
Within the application, the following logging occurs:

- Logins – all successful and failed logins are recorded.
- Access of participant-identifiable records – a participant access report is maintained and can be viewed by an administrative-level user of the application.
- Changing of data – all data regulated by 21 CFR Part 11 (please see 21 CFR Part 11 Policy) is recorded in the audit log.
- Billing – edits of records affecting client use of Vestigo® for protocol billing are audited.
- Deletion of data – deletion of data is not permitted in the application.



Logical Data Model

Vestigo® uses the following logical model. All data center facilities shall be located within the United States.



Connection to Application

The hosted version of Vestigo® involves client workstations connecting to McCreddie servers to access the application. The application is accessed over a 256-bit SSL-encrypted public web address. A VPN tunnel between a private address with McCreddie and the label printer(s) must be established. McCreddie supports all standard VPN encryption methods and will attempt to use a setting that is



commonly used by the client. McCreddie utilizes FortiGate firewall equipment. The detailed specifications and creation of a shared key is conducted via a joint conference call.

Requirements for Client Workstations

- Windows 11 operating system with a screen resolution of 1024 X 768 minimum
- Microsoft Edge, Firefox and Chrome browsers supported
- Adobe Acrobat Reader for viewing pdf reports
- Microsoft Excel for viewing Excel reports
- Workstation should be able to print to a standard laser printer as needed for reports

Requirements for Label Printers

- Printer requires an Ethernet port and a fixed IP address.
- Printer hardware is supported locally by the client; McCreddie supports the software used by the Vestigo® product.
- Zebra and Intermec printer models are the most commonly used printers by our current clients
 - Note: The Zebra ZM400 printer, the model currently in use in most Vestigo® user sites, has been discontinued and replaced by Zebra Technologies' ZT410.
 - Other printer models can be supported.

Resources Required from Client for Implementation and Support

- Ensuring that appropriate workstation resources are available for users.
- Network port with fixed IP address for label printer(s)
 - Network engineering resources to establish private VPN tunnel for label printer(s)
 - Conference call to setup VPN tunnel
- Available help desk support and network engineering resources to troubleshoot any VPN tunnel issues including inability to connect or network performance concerns
- McCreddie provides 100% of the end user support for application functions and training.

Compliance

Sensitive Information/PII

McCreddie provides an investigational drug accountability software called Vestigo®. In providing its customers with access and use of Vestigo®, McCreddie is not a business associate, is not performing HIPAA-covered functions on behalf of its customers, and the information uploaded and processed in Vestigo® is not Protected Health Information. Clinical research activities conducted by users of Vestigo® are outside the scope of standard medical care and treatment services regulated by HIPAA. Apart from the end-user credentials for Vestigo® users, the identifiable information created, received, or accessed through Vestigo® is limited to information pertaining to research subjects who have been consented and enrolled in a research study. Therefore, as the provider of



Vestigo®, McCreddie Group does not function as a Business Associate and a BAA is not applicable. Executing a BAA for a business relationship that does not fall within HIPAA imposes HIPAA compliance obligations on both parties where not applicable. In addition, if the information were Protected Health Information, our customers would be restricted in how such information could be used or disclosed, which is not aligned to the uses for research purposes. Although a BAA is not applicable, we take security seriously and maintain physical, administrative, and technical safeguards to protect the confidentiality, integrity and availability of data in Vestigo®. We maintain annual SOC 2 Type II reports and have regular penetration testing performed by 3rd parties, amongst our other security measures.

Code of Federal Regulations 21 Part 11

Vestigo® is an application to manage the Investigational Drug Service. As such, it performs record-keeping functions subject to 21 CFR Part 11. The regulations require electronic features and controls, as well as user policies and practices. The Vestigo® Statement of Compliance with 21 CFR Part 11 document is provided to clients for use with their study sponsors. Each client is responsible for maintaining their policies related to 21 CFR Part 11.

Social Security Numbers

Vestigo® does not provide a field for the storage of social security numbers and explicitly prohibits the storage of such information within the application for any reason.

Patient Financial Information

Vestigo® does not provide a field for the storage of patient financial information and explicitly prohibits the storage of such information within the application for any reason.

Further Information

Detailed data infrastructure diagrams and security information, including SOC 2 Type II audit reports are available upon a signed Master Services Purchasing Agreement (MSA) or a signed Non-Disclosure Agreement (NDA).