Abett

# Lockbox™ Security Design


| | |
|---|---|
| Summary | 2 |
| Lockbox Data Management System | 2 |
| Software Description | 2 |
| Key Operational Features | 3 |
| Security Design | 4 |
| Key Security Features | 5 |
| Cloud environments | 5 |
| Lockbox Operations | 6 |
| Data Governance and Access Control | 7 |
| Protected Health Information and De-identification | 8 |
| About Abett | 9 |
| Vision and Mission | 9 |
| Information Security Organization | 9 |

## SUMMARY

As benefits plan sponsors, employers have fiduciary responsibilities to utilize the plan's operational data, both current and historical for plan administration. However, employers' utilization of that data is subject to regulatory and contractual obligations. One example is the HIPAA Privacy Rule, which prevents benefits staff who are not plan administrators from accessing certain types of data.

**The Lockbox is a Software-as-a-Service (SaaS) data-management tool designed for plan sponsors to exercise control over sensitive data, while adhering to compliance requirements and constraints.** This memorandum describes the security design principles incorporated into the Lockbox platform and explains how data is protected from unauthorized access or modification.

The Lockbox can be implemented within Amazon Web Services (AWS), Microsoft Azure, or both. The software is managed and maintained by Abett. It integrates AWS and Azure security features in fundamental ways, including technologies like virtual private clouds (VPC). The software's operation is fully controlled by the Lockbox client, subject to compliance constraints.

Herein, please note that we refer to employers, and plan sponsors generally, as the Lockbox client.

## LOCKBOX DATA MANAGEMENT SYSTEM

### Software Description

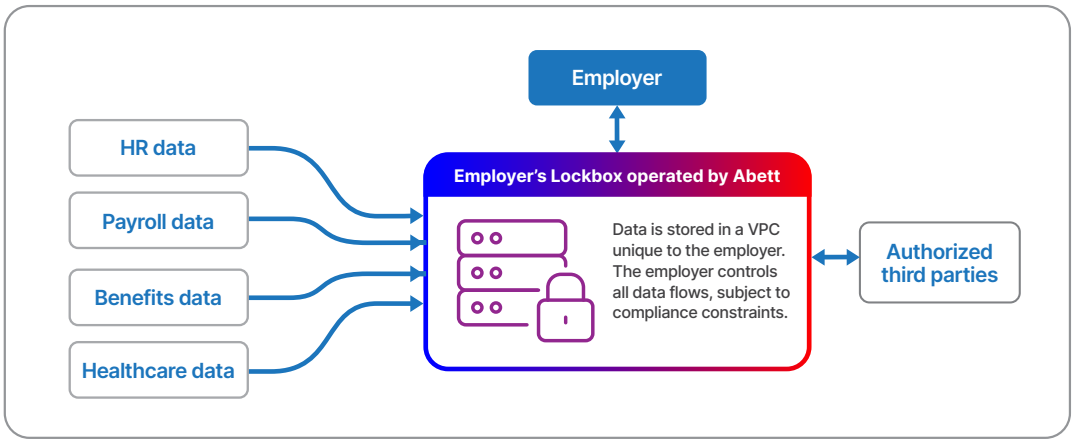
Each client is assigned a secure partition in a cloud environment, which is devoted to that client's data. This partition is colloquially referred to as a Lockbox.

- Secure and HIPAA compliant; standard BAA available. All data in this environment is encrypted both at transit and at rest with client-specific keys, among many other security measures.
- The SaaS network infrastructure incorporates features available from AWS Security Hub and Azure's equivalent services, and external tools like Sumo Logic and others that provide world-class protection against a variety of cyber threats.  All components are HIPAA compliant.
- Each Lockbox is implemented as a secure partition. Access to the public internet is tightly regulated and monitored. The VPC provides a logically isolated environment in which data can be stored and applications can be executed. For a given client, all computations are executed in private subnets of a VPC, which are not available on the public internet.

The software performs several automated tasks, including data integration and data-quality validation. It manages access control and additional security for authorized third parties.

The Lockbox's first function is to bring a client's data into a centralized, secure store. Inbound data is processed, which includes cleaning, validating and normalizing data across vendors and systems, as appropriate. To maintain fidelity, raw data is retained even after canonicalization.

Upon a plan sponsor's request, its Lockbox can be isolated in its own unique Azure or AWS account, which is an example of using "Defense in Depth" to protect sensitive data.




As illustrated above, a client may choose to share subsets of data with authorized third-party vendors. The software provides outbound (egress) APIs that enable clients to share authorized subsets of data with authorized vendors, subject to compliance constraints.

## Key Operational Features

- Only subsets of data are shared with third parties. The software adheres to the principle of "least privilege," meaning third parties receive only the smallest subset of data required to perform their commercial function. All data releases are authorized by the client.
- Outbound traffic from the private subnet is limited by firewalls and access-control lists. Abett uses Intrusion Detection Software and Intrusion Prevention Software to protect Lockbox endpoints from malicious activity.
- Outbound reports are established at the direction of the client only. Protected data, including personally identifiable data, are deidentified before being shared, whenever possible. Outbound specifications are reviewed and authorized by the client after being critically analyzed by Abett's staff to ensure the data subsets shared with third parties are appropriate.
- No data is sent outbound without first verifying that a valid, signed data authorization is on file.
- Abett requires PGP encryption on inbound and outbound data, and all data stored in the Lockbox is secured with client-specific encryption keys.

Regarding outbound APIs, the software currently supports REST API's and GraphQL queries. APIs return data in JSON, CSV, or plain-text formats. Data can be presented in standard specifications, such as EDI 834, or specifications customized for each client or third-party application.

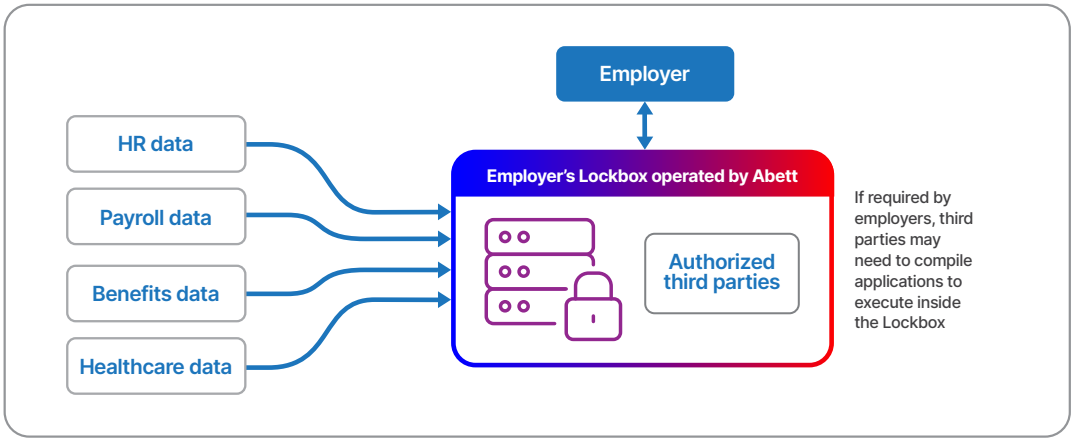
Each client application is provided with a JSON Web Token which determines which APIs, and ultimately which data, are available to the application. Therefore, no credentials or secrets are embedded in client applications. Credentials are generated when the application is launched and are short-lived. The credentials provided for each application run are specific to a single client. Validity of tokens is checked with each action taken.

The URL for the private API is also provided to the container at launch time, so the URL need not be embedded in the application, similarly to how credentials are managed.

This approach is inspired by the Twelve-Factor App methodology, which has become a standard in modern software development. It makes the Lockbox platform more flexible, as different APIs can be provided for different combinations of clients and applications.

Given the organization of the benefits industry, it is necessary to share data with third parties. However, a challenge with the arrangement is that clients lose control of that data once it is transferred to a third party. To address this concern, the software enables authorized third parties to develop applications that may execute entirely inside the Lockbox, as illustrated below.

In the scenario below, data never leaves. Rather than data traveling to a third-party vendor and its application, the application travels to the data.




Third-party vendors deliver applications via Docker, or comparable technology. The container is executed within the VPC, and specifically inside a private subnet that accesses data and other resources indirectly through APIs. Docker images have access to APIs only in private subnets in which the docker images are running.

## Security Design

The Lockbox is designed to minimize any potential attack surface while maintaining the highest security and confidentiality standards.

**Least privilege.** Abett's software developers, client account managers, and other staff are granted the minimum permission set necessary to complete their jobs. Any extra permissions requested must be logged in to a ticket with business justification, and then approved by their manager and Abett's information security organization. Abett uses Just-in-Time permissions tools such as Entra's Privileged Identity Management (PIM) system. All instances of elevated roles are audit logged and regularly reviewed.

**Separation of duties.** Abett has role-onboarding templates to specify the limited, role-specific permissions associated with new staff. As employees assume more responsibility, then they can request further access using tickets that must be approved by managers and information-security staff.

**Individual accountability.** All access to client data is audit logged. Audit logs are regularly scanned and reviewed for irregular activity.

**Change management.** All code changes and infrastructure-as-code changes must be completed by employees who have specific permissions to the relevant code, and then reviewed and approved by at least one other team member. A series of automated tests and vulnerability scans are performed during each change of the process.

## Key Security Features

**HIPAA compliance.** The Lockbox complies with HIPAA regulations regarding protected health information (PHI). It is fully compliant with the HIPAA Security Rule and the HIPAA Privacy Rule. Abett performs regular assessments against these compliance regulations, as well as the NIST Cybersecurity Framework, and follows industry leading data security and privacy best practices. The Lockbox maintains a SOC 2 Type 2 certification for the Security, Confidentiality, and Availability principles.

**Client control.** No data is sent from the Lockbox to a third-party vendor without authorization on file. Abett does not directly access a client's protected data without authorization from the client. Rather, Abett provides data management software that gives clients control while ensuring compliance with regulatory and contractual obligations.

**Architected to cloud-security best practices.** The Lockbox was built to be a secure storage system. It incorporates modern principles like least privilege, redundancy, and security by design. There is no "bolt-on" security layer. Rather, strong security design is our first principle.

**Encryption at rest and in transit.** All data is encrypted before it first reaches the Lockbox, and remains encrypted thereafter. All connections use PGP keys. Keys and credentials are client-specific with no tolerance for repeated usernames or supplier generic connections. This ensures one secure endpoint for client files.

**Full audit logging of all activity and access.** All actions taken, and all access of any kind, to client data or servers are audit logged and monitored.

## Cloud Environments

Abett uses phishing resistant FIDO2 MFA for all access to systems that hold PHI. Specifically, Abett uses Yubikeys, which stores the FIDO2 private key securely on the physical key. Authentication only occurs when the system confirms that the request came from the specific domain that registered the key.

Connections to cloud environments are only allowed via pre-approved ("whitelisted") IP addresses. Abett maintains security groups and VPCs to restrict access to client data. DDOS protection is in place through AWS WAF and API Gateway. Abett makes use of Intrusion Detection Systems and Intrusion Protection Systems to secure network access to endpoints and detect unauthorized access or suspicious activity.

Abett follows an Infrastructure as Code design pattern and maintains vetted baselines of all systems in source code. Any changes to systems must go through a code review process. Abett uses tools such as AWS Config to perform drift detection to verify that no changes are made to infrastructure outside of the vetted paths.

To connect to the production environment, Abett engineers must connect through a bastion and authenticate with Yubikeys. All client data is in client specific environments and encrypted with client-specific keys.

In most cases, information arrives at a client's Lockbox via SFTP. Access to SFTP servers is given using SSH certificates. As previously described, by policy, inbound data must be PGP encrypted. Once data lands on the SFTP server, it is immediately ingested and encrypted with a client-specific encryption key using AWS's HSM backed KMS.

All information in the Lockbox is stored encrypted at rest using AES-256.

At the client's request, specific subsets of information may be sent outbound to third-party partners and vendors. Data is delivered via SFTP, or comparable protocol. Before outbound access can be provisioned, Abett's operations team generates a specific outbound authorization form for the requested report that enumerates all data fields to be included. The client must sign the outbound form, and a record is maintained within the report pipeline. At the time that any report is generated, the software confirms that a valid authorization for that specific report is actively on file.

Abett performs cross-region encrypted backups of all client data and has disaster recovery playbooks for all systems.

- As data is ingested, inbound PGP encryption is removed using Abett's client-specific private key and then re-encrypted with client-specific encryption keys.
- Data validation software is spun up to process the newly arriving inputs. These validations confirm that the data belongs in the Lockbox that received it, and then executes a series of integrity and validation checks.
- Then, the validation services spin down, and the ingested data is securely stored.
- Outbound reports (data egress) can be scheduled to run on any cadence. When a report is due to be generated, reporting services spin up and assume a client-report-specific role. Data is decrypted only as needed to generate the report. The service checks that a valid authorization is on file for the data fields and recipients scheduled.
- Reports are PGP-encrypted at the client's request. A service connects to the destination SFTP server to deliver the report.
- At each step in the process, a specific role is assumed. Each role is generated using the minimum permissions possible and restricted to a specific client account. Audit log entries are generated throughout the process enumerating all access to the data.
- No services remain running when they are not actively working on ingestion, validation, or report generation. Lambda functions, or their equivalent, are used for these services, minimizing the amount of software needed to be maintained for each step.

**Regarding user endpoints:**

- Abett uses JAMF and inTune endpoint management software to ensure that employee devices meet security baselines. Alerts are triggered if variations are detected or if a device fails to update or connect.
- Abett uses JAMF Protect and Microsoft Defender anti-malware on Macs and Windows laptops, respectively. IT and Security staff monitor findings from these tools and remediate as needed.

**Regarding automatic log-off:**

- Abett has implemented procedures that terminate an electronic session on an Information System after a predetermined time of inactivity. Workstations and devices should terminate a session after fifteen (15) minutes of inactivity. After being locked or terminated, a session may be resumed if the Username and/or number and password are re-entered.
- Abett's interactive websites use refresh tokens to ensure that authentication materials used to render a page are constantly rechecked.
- AWS and other platforms will perform user re-authentication as needed.

**Regarding risk assessment and evaluation:**

- An annual review of Information Systems, unless required sooner, is performed to help ensure that security mechanisms are still enabled and functioning and that policies and procedures to protect ePHI are in place and functioning.
- Abett's staff periodically evaluate Abett's Information Systems, policies and procedures based upon the standards implemented under the HIPAA Security Rule and Privacy Rule, and any environmental or operational changes affecting the security of ePHI.
- Information System activity reviews and related documents are retained at least for the length of time required by the HIPAA Security Rule and other relevant regulation**s.**

## Data Governance and Access Control

When inbound data is processed by the software, it may be associated with one or more compliance constraints. In plain language, the data element may be "tagged" as being protected by one or more compliance regimes.

Outbound processes are associated with compliance regimes that govern access to data. When an outbound process attempts to access a data element, the software checks if that outbound process is associated with all the compliance regimes assigned to that particular data element. If not, then the outbound process cannot access the data.

A compliance regime can be a standardized constraint; for example, HIPAA requires Safe Harbor de-identification, which is implemented in the software. However, a compliance regime can be designed to specifically address idiosyncratic requirements of a client or data source.

For example, suppose a specific client has a contractual obligation to a plan administrator not to simultaneously share provider-identifiable information with claims-level financial information with a third party. At the direction of the client, Abett will create a compliance regime in the software that prohibits the simultaneous pairing of those data elements and assign this regime to the provider-level and financial data elements in the relevant records. Once that regime is implemented, the software will not provide that combination of data elements to an outbound process.

Regarding user access, the software enforces a series of rules based on a number of factors, including the ISO 27001 standard; general security principles; and the legal, regulatory, and contractual commitments the company has assumed, and expects to assume in the future.

All access control policies are based on the concept of need-to-know, or least-privilege.

This principle dictates that users should have access to assets only as required by their role, for business purposes. The software requires access controls to be in place on all applications, operating systems, databases, and network devices to ensure users have least privilege.

The software's access control policies apply to all users of information technology under the control of Abett, Inc. and any affiliated companies. This includes third-party vendors and subcontractors engaged by the company.

Audit logs of system access, including both general access and access to client data, shall be maintained for at least thirty-six (36) months.

At least weekly, the Access Control Officer will review audit logs of all internal staff access to client data. If the Access Control Officer is unable to complete this task during a given week, the responsibility transfers to the Chief Information Security Officer.

At least quarterly, the Access Control Officer will review each clients' user access lists. Client user accounts shall adhere to the following constraints:

- Unique User IDs are required for access.
- User IDs are not allowed to be shared across individuals.
- User IDs cannot contain data that could reveal private information about the user.
- User IDs cannot contain data that could reveal the access level assigned to the user.

Passwords shall adhere to the following requirements and constraints:

- New users are issued random and unique initial passwords. The initial password required to be reset after first sign on.
- Users are required to keep passwords confidential. Passwords should expire every 60 days, and a user account cannot use one of its previous twenty-four (24) passwords. Moreover, users must change passwords when there is an indication of possible system or password compromise, or as instructed by the Access Control Officer.
- Passwords must contain at least twelve (12) characters that include letters (both upper and lower case), numbers, and special characters.
- Finally, any vendor default passwords associated with the software must be removed, disabled, or changed prior to placing the device or system into production.

## Protected Health Information and De-identification

PHI covered by the HIPAA Privacy Rule can be de-identified following only two methods: either the Safe Harbor method, or the Expert Determination method. Abett is able to generate reports for clients via either of these methods.

Abett has contracted with established, independent experts to perform HIPAA data de-identification for data reports or exports to dashboards which cannot be de-identified under the Safe Harbor provision. Using third-party vendor de-identification software, Abett staff identifies sensitive data fields in a dataset. This software performs a series of data transformations using blurring, data perturbation, and other methods to appropriately de-identify the dataset. The independent de-identification expert then reviews the data and the rule sets applied to it. Upon successful review, the independent expert issues an opinion certification that the data is appropriately de-identified to reduce the risk of accidental re-identification.

## Vision and Mission

**Abett envisions a world in which everyone has access to high quality, affordable, and timely healthcare.**

Our mission is to deliver solutions to our clients that produce transparency and accountability. Those solutions will put power into the hands of healthcare consumers. Consumers will use that power to make our vision real.

In the US, the flow of healthcare data is complex and messy. Employers are the key consumers of healthcare, but historically, they could not access their benefits plan data, let alone leverage it to improve outcomes.

Abett solved this problem with the Lockbox, which serves as a client's system of record for benefits and healthcare data. Abett product suite will allow employers to achieve better outcomes, lower costs, and simplify experiences for benefits staff and plan members.

## Information Security Organization

Within Abett, the following named roles exist to ensure the security of the software and users' data. Each officer is responsible for regularly reviewing and updating their assigned policy, as needed, and communicating changes to appropriate constituents. Each officer is responsible for the enforcement of his or her assigned policy or policies.

| Role | Implementation Responsibility |
|---|---|
| **Chief Information Security Officer** | Overall strategy and certifications |
| **Access Control Officer** | Access Control Policy |
| **HR and Asset Management Officer** | HR and Asset Management Policy |
| **Regulatory Compliance Officer** | Regulatory Compliance Policy |
| **Security Incident Officer** | Security Incident Policy |
| **Threat Management Officer** | Threat Management Policy |

Any exception to any aspect of any security policy may be tentatively granted by mutual consent of the Chief Information Security Officer (CISO) and the officer responsible for the policy.

The CISO has several key responsibilities, including ensuring the company's information security policies align with recognized standards, including the HIPAA Security Rule and Privacy Rule, as well as the NIST Cybersecurity Framework. Further responsibilities include the annual completion of a Service Organization Control (SOC 2) report, and obtaining and maintaining appropriate security certifications, as well as performing annual HIPAA risk assessments, incident response exercises, disaster recovery, and business continuity exercises.

Learn more about Lockbox at **abett.com**