# Data Lockbox: Security Whitepaper

January 2023

âbett

# Table of Contents



# Summary

As health-plan sponsors, employers have fiduciary responsibilities to utilize the health plan's operational data, both current and historical. However, employers' utilization of that data is subject to regulatory and contractual obligations, including contractual obligations to insurance carriers and others.

The Data Lockbox is a Software-as-a-Service (SaaS) data-management tool, specifically designed to provide employers control over sensitive data, while adhering with the associated compliance constraints. This security paper describes the security by design principles that are incorporated in the Lockbox and explains how your data stored in the Lockbox is protected from unauthorized access or modification.

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

Abett is not a traditional healthcare services vendor. It does not access or utilize an employer's protected data, per se. Rather, Abett provides data-management software. Its SaaS product enables employers to utilize sensitive data while ensuring compliance with regulatory and contractual obligations.

*Abett enables employers to utilize sensitive data while ensuring compliance with regulatory and contractual obligations.*

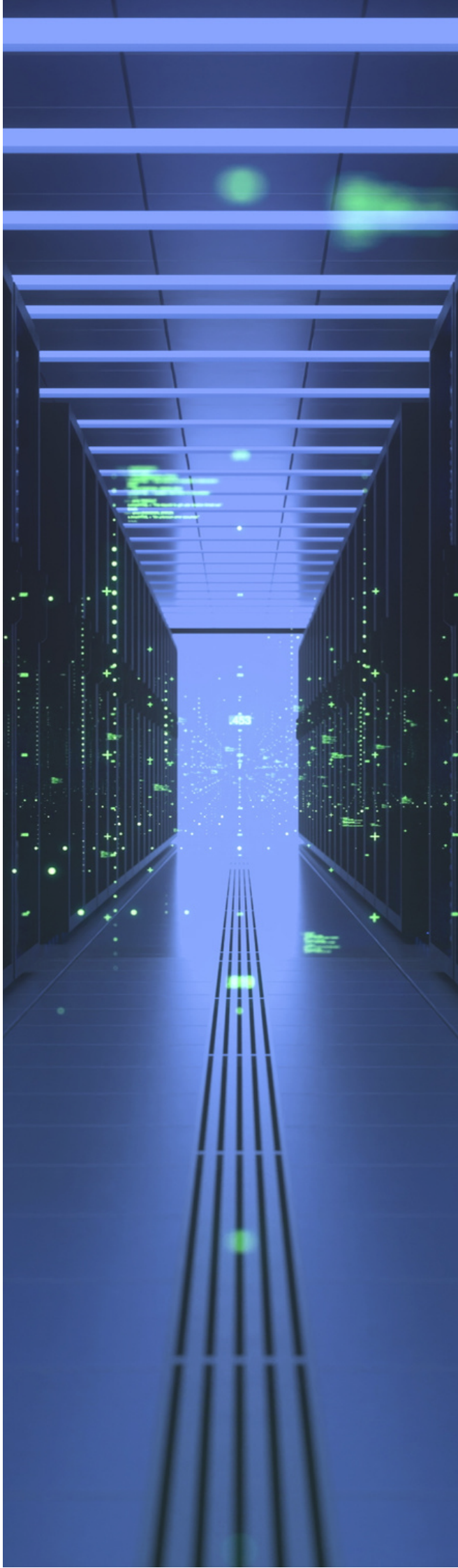
# Key Security Features

## Key Feature 1:

HIPAA compliance. The Lockbox complies with HIPAA regulations regarding protected health information. The Data Lockbox 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 following industry-leading data security and privacy best practices. The Data Lockbox also maintains a SOC 2 Type 2 certification for the Security, Confidentiality, and Availability principles.

## Key Feature 2:

The Employer controls data flows. No data is sent out of the Lockbox to a partner without an authorization on file from the owner of the data.



# Key Security Features


Architected from the ground up to follow cloud security best practices. The Data Lockbox was built from the start to be a secure storage SAAS, following modern principles of 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 Employer data is encrypted from the moment it first reaches the Lockbox. Keys are customer specific.


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

# Software Description

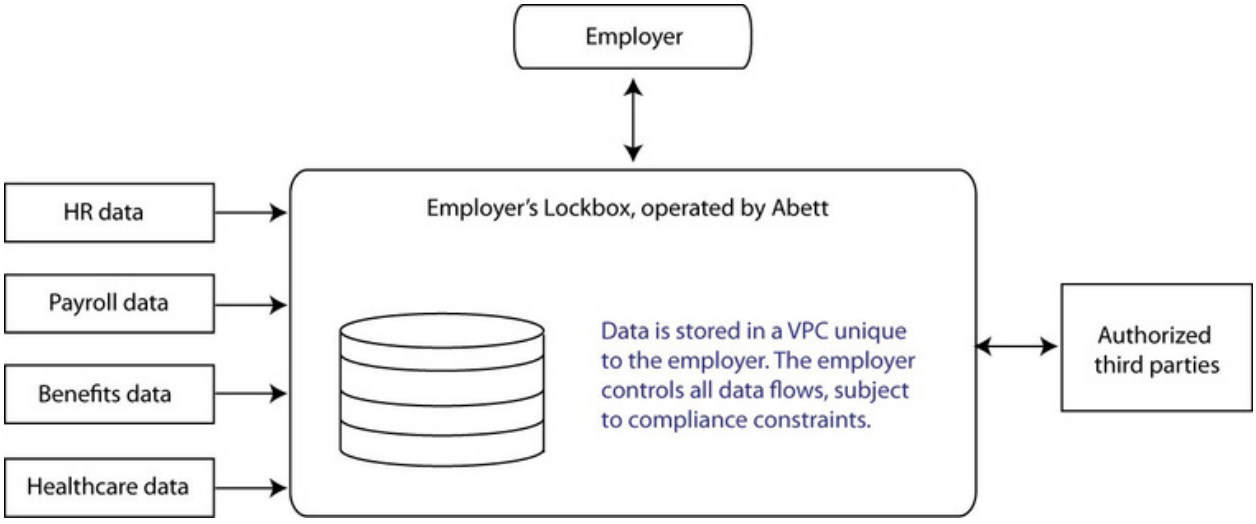
Each employer is assigned a secure partition in an AWS cloud environment, devoted to that employer's data only. This partition is colloquially referred to as a Lockbox.

- Secure and HIPAA compliant; standard BAA available. All data in this environment is encrypted both at transit and at rest, among many other security measures.
- The SaaS network infrastructure incorporates not only features available from AWS Security Hub, but also external tools like Sumo Logic and others that provide world-class protection against a variety of cyber threats. All AWS components used are HIPAA Compliant.
- Each Lockbox is implemented as a secure partition within AWS. 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 execute. For a given employer, all computations are executed in private subnets of a VPC, which are not available on the public internet.
- The SaaS software performs a number of automated tasks, including data integration and data-quality validation, and managing access control and additional security for authorized third parties.
- Employers control the Lockbox configuration and how data is used. Abett does not access an employer's data, per se, and it does not control how it is used. Rather, Abett provides a software tool that gives employers control over data flows, subject to compliance constraints.

# Software Description

The Lockbox's first function is to bring an employer's data into a centralized, secure store. Inbound data is "processed," which includes cleaning, validating, and normalizing data across vendors and systems, as appropriate.

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

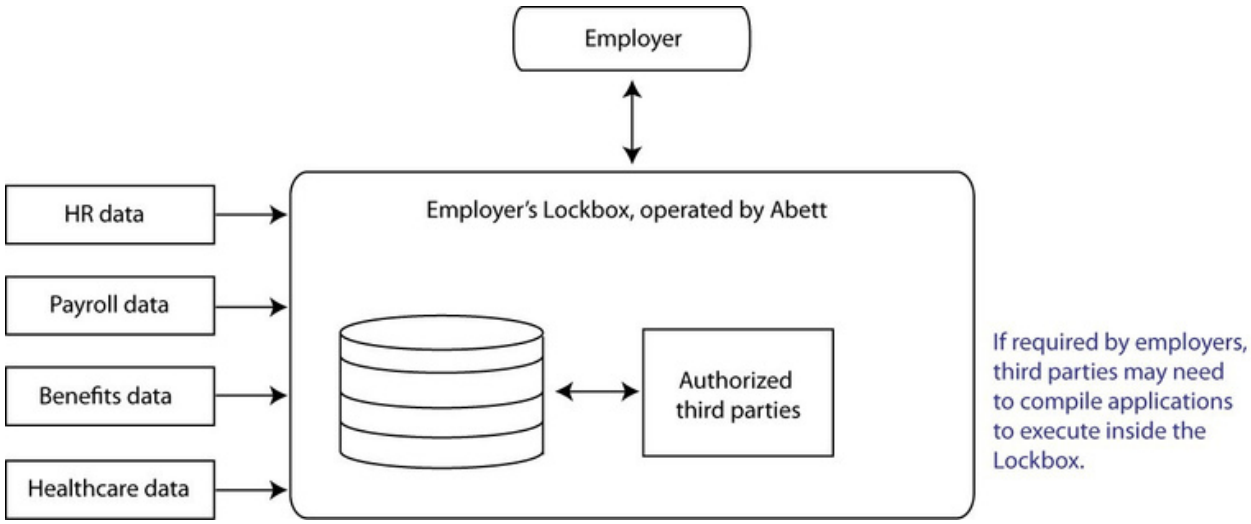



As illustrated above, an employer may choose to share a subset of data with third-party vendors with which it chooses to do business. The software provides "outbound" APIs that enable employers to share subsets of data with authorized vendors, subject to compliance constraints.

- 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 business function.
- Outbound traffic from the private subnet is limited by firewalls and access-control lists.
- Outbound APIs are established at the direction of the employer only. Protected data, including personally-identifiable data, are deidentified before being shared, whenever possible. The configurations of outbound APIs are regularly reviewed by the employer and 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 HIPAA data authorization is on file.

# Software Description

While there is a business case to share data with third parties, a challenge with this arrangement of “handing off data” is that employers 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.




**Rather than send data to a vendor, the vendor must send its application to the employer.**

In this scenario, third-party vendors build their applications via Docker, or comparable technology, and then share the resulting container with Abett. The container is executed within the VPC. Third-party applications will execute inside a private subnet that can access databases and other resources indirectly through APIs. Specifically, Docker images have access to APIs only in private subnets in which the docker images are running.

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 employer or third-party application.

# Software Description

Each client application is provided a JSON Web Token which determines what APIs and ultimately what data is 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 employer. 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 handled.

This approach is inspired by the Twelve-Factor App methodology, which has become a standard in modern software development.

***This approach makes the Lockbox platform more flexible, as different APIs can be provided for different combinations of employers and applications.***

# 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 most closely associated with 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 Framwork.

Further responsibilities including 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.

# 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 of 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 an employer or data source.

For example, suppose a specific employer has a contractual obligation to a medical insurance carrier not to simultaneously share provider-identifiable information with claims-level financial information with a third party. At the direction of the employer, Abett will create a compliance regime in the software that prohibits the simultaneous paring 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 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 its 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 customer data, shall be maintained for at least thirty-six (36) months.

# Data Governance and Access Control

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

At least quarterly, the Access Control Officer will review each employers' user access lists. Employer 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 constituents are issued random or 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 eight (8) 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.