casebook
Person-centric Purpose-built

cb: admin

Casebook | Security

The Casebook Platform Security follows and implements best practices for securing SaaS Application on the Cloud. Casebook's product, technology, and data decisions are based on first validating all security standards and approaches.

Casebook Platform has three tiers of Security:

- Tier 1: Hosting with Cloud Hardening
- Tier 2: SaaS Application including Secure Application Architecture
- Tier 3: Applications' Access based on Least Access Policy

Tier 1: Hosting with Cloud Hardening

First Security Tier provider SaaS Platform availability, scalability, and defense against cyber and DDoS attacks. Since Casebook Platform is Cloud-native architecture, self-healing microservices, auto-scaling configuration, triple data-redundancy are all inherent.

Casebook Platform hosting network topology provides Logical Access Control. This allows complete Database lockdown, giving no internal or external party direct database access. Additionally, four layers of hosting environment networking configuration, provides open access only through the application gateway, while all other networking layers are accessible only from the internal services.

Tier 2: SaaS Application including Secure Application Architecture

In 2013, Case Commons (now Casebook PBC) retained Epstein Becker & Green and Fidelis Technology Consulting Group, experts in security practices associated with protecting Protected Health Information (PHI) and Personally Identifiable Information (PII), to conduct an outside audit, vulnerability assessment and to provide feedback and analysis on the degree to which Casebook PBC had implemented appropriate practices and policies to meet the standards of HIPAA and HiTech. The external audit was completed in keeping

with Casebook PBC's commitment to meeting the highest security standards and protocols. The review included all aspects of our operations: from the physical plant to technology infrastructure, to personnel policies & practices. The firm's finding was that Casebook PBC had implemented very strong operational, management and technical NIST controls and was largely compliant with the HIPAA Security Rule. The firms provided a handful of recommendations about policy changes to be considered. Two examples of recommendations from the audit, both of which were implemented, are described below:

- Better document the chain of command and related procedures in the event of a catastrophic event that disrupts operations (which is now part of the Casebook PBC Disaster Recovery Plan and Protocol)
- Hold annual training on internal security practices around issues such as computer security, password standards, and storing data (which is now provided to all employees annually, complementing the training upon hiring which has always been conducted).
- Deployed on AWS, the Casebook platform benefits from the industrial-strength AWS security infrastructure. AWS provides HIPAA compliance as well as PCI DSS compliance out of the box, addressing all stated State security requirements including logging, data center security, encryption, antivirus, network security, access and identity management and data handling.

Tier 3: Applications' Access based on Least Access Policy

This Tier of Casebook Platform Security provides a fine-tuned identity management and access control system along with powerful system-wide security features to keep all data secure and accessible only to explicitly authorized individuals using the principle of least privilege. The security features enable administrators to control which data and application functionality a given user role can access. For example, a user group may have read-only access to certain data elements but write access to others. Access can be controlled at entity, record or field level. The Casebook Platform comes with a set of predefined roles to serve as a jumpstart for the Department with the ability to add additional roles and edit others if desired. System-wide security features are of paramount importance and are at the core of the system architecture. Some highlights of the Casebook security features include:

- **Security services**
  Our philosophy relies on multiple layers of security, starting with design and carrying through the operations and management of the system as a whole. The security services layer is responsible for application-level security.

- **Single sign-on via identity federation**
  Casebook can integrate with external identity providers, such as Active Directory, Oracle LDAP and IBM RACF, via identity federation services using connectors. This allows users to sign-in to the platform using their enterprise credentials.
- **Authentication & Authorization**
  The platform uses standards-based authentication/ authorization using OAuth2.0 and OpenID Connect. JWT tokens are used which are based on open standard (RFC 7519) that defines a compact and self-contained way for securely transmitting information between parties as a JSON object. This information can be verified and trusted because it is digitally signed using a secret (with the HMAC algorithm) or a public/private key pair using RSA or ECDSA.

The Casebook platform uses JWT tokens to verify all communication with data services. In authentication, when the user logs in a JWT is generated which is passed by the client to the application with each API request. By default, the expiration is set 6 hours from login and refreshed on each successful interaction with a service.

- **Role-based security**
  Authorization and application rights are managed by a role-based authorization framework. The Casebook platform currently supports ten different user roles, including read-only users. Specifics of roles and capabilities can be customized during implementation.
- **Data protection**
  Within the platform, all data is encrypted in transit. The Casebook platform also encrypts data at rest with limited usage of cache and CDN capabilities.