dimagi

Data Confidentiality & Security Overview

Dimagi has designed its software and infrastructure to ensure that we can fully maintain the confidentiality and security of our clients' data. Data collected by Dimagi's mobile solutions is often sensitive, including protected health information. To best protect this data, Dimagi employs many layers of data security, and prioritizes the integrity and safety of data hosted on our systems. There are numerous components that contribute to Dimagi's ability to maintain confidentiality and security. This document provides an overview of these components, and of the technical requirements and processes Dimagi uses to safeguard patient, process, and outcome data.[1] This document is most relevant to projects that use Dimagi's cloud or an actively managed server.

Overview

1 *Dimagi's projects involve two components: a cloud server ("CommCare") and mobile phone-based component ("CommCare Mobile")*

1. Operational Security

Physical Security – Data Center

In order to create the most secure cloud environments, Dimagi partners with the best available data centers for managed local instances. All of our cloud environments require ISO 27001 compliance, and we seek providers that provide increasing levels of security. This has resulted in two public locations our clients can select from: one located in the United States (the default location for new users) and one located in India.

Both in the US and India, our data center provider is Amazon Web Services (AWS). Data does not move between locations after a location has been selected.

AWS: AWS has a designated security organization that is responsible for their security policy, asset management, human resources security, physical and environmental security, information security incident management, and security vulnerability reporting. AWS carries out the security objectives as defined by the best practices set out in ISO 27001. This standard is recognized globally as the most comprehensive framework for establishing and maintaining information security best practices within an organization.

AWS also adheres to the following information security and related certifications and standards: ISO 27001, ISO 27017, ISO 27018, PCI-DSS Level 1, SSAE16, SOC1, SOC2, SOC3, Safe Harbor, and Content Protection Standard (CPS). For more information on AWS's standards, please see the following: https://aws.amazon.com/compliance/programs/.

AWS's data center also maintains keycard protocols, biometric scanning protocols, and around-the-clock interior & exterior surveillance. Thorough background security checks of data center employees and access to facility only for those with proper clearance.

Table 1: Information about Dimagi's Data Center Providers

Physical Security	• Access limited to authorized data center personnel — this means that no one can enter the production area without prior clearance and an appropriate escort. • Every data center employee undergoes thorough background security checks. • Utilizes keycard protocols, biometric scanning protocols, and around-the-clock interior and exterior surveillance.

Precision Environment	• In the event of an HVAC system failure, N+1 redundant HVAC (Heating Ventilation Air Conditioning) system ensures a duplicate system immediately comes online every 90 seconds. All air is circulated and filtered to remove dust and contaminants.
	• Utilizes an advanced fire suppression systems.
	• Conditioned power, including:
	  • UPS (Uninterruptible Power Supply) for all servers.
	  • N+1 redundant UPS power subsystem, with instantaneous failover if the primary UPS fails.
	  • If an extended utility power outage occurs, onsite diesel generators will take over and run indefinitely.

Table 1: Information about Dimagi's Data Center Providers	
Connectivity	• High bandwidth performance • Multiple ISP redundancies • Fully redundant, enterprise-class routing equipment only • Network topology and configuration automatically improves in real time • Network and security teams must be certified and thoroughly experienced in managing and monitoring enterprise-level networks
Hardware	• Hardware replacement SLA. Ideally less than 1 hour for hardware failures.
Application Backups	• Full daily backups to multiple locations • Continuous backups of transaction data • Secure streaming of transaction data to remote disaster recovery center

Servers

In the event of a hardware failure, Dimagi has a service-level agreement with our data center to provide one-hour replacement. For auditing purposes, all sensitive interactions with the server will be logged by user, date, time, and location. Administrative access will be restricted solely to Dimagi and associated sub-vendors. All system level access will be fully logged for auditing purposes.

2. Application Security

Application security is a combination of secure design practices and regular audits. Dimagi has invested significant resources to ensure our software is highly secure. We regularly use internal and external audits to ensure we have secure applications. Dimagi recently completed the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. Dimagi regularly supplies documentation to clients for security and information technology audits as well. Audits may include penetration testing, security testing and source code review. Dimagi will continue to work with security experts to discover, test, address and validate any security concerns.

Mobile Application Security

CommCare mobile applications have several security core security features, including the following:

- **Password protected access:** Each CommCare application will be enabled with password protection to restrict unauthorized access. Each user can have a unique username and password so that they can only access their own set of data.
- **Data Encryption:** Encrypted data storage on Android devices (AES 256-Bit Symmetric Encryption, fully HIPAA compliant). Data is obfuscated on Java devices, but is not encrypted.
- **Data Retention:** Data is erased from phone after submission to the server. However, during the app design process, an organization can specify a subset of registration data (also called case data) required for future home visits to be retained on the mobile device. This data is removed from the mobile device when the case is closed.

3. User Security

CommCare provides numerous role-based access and security features for users.

Access

The only users that have access to a CommCare project space and data are authorized users and Dimagi technical administrators. User management is available to your CommCare web administrators, so that adding and removing users is completely in your control. If a user is no longer authorized in your system, simply remove them and they will no longer have access to content stored in CommCare.

Authentication

Dimagi ensures your authentications are secure by using the following measures:

- User logins are secured by HTTPS.
- User accounts are validated by user email to prove identity.
- Dimagi requires robust, entropy-based passwords for use by each individual user.
- Passwords are stored hashed and encrypted and no Dimagi employee or contractor has access to plain text passwords. Plain text passwords are never stored by Dimagi.
- Any CommCare user can enable two-factor authentication to provide additional security to his/her login. Additionally, CommCare project administrators can require two-factor authentication of all project users if they so choose.

Roles & Permissions

With CommCare, each CommCare user can have different levels of access to a project space. For example, one person can be given access to view only reports on worker performance, while another person may have access to all data collected. As a project administrator, it is also possible to customize different levels of access.

Mobile users will only have access to the data that they have collected. Depending upon the configuration of an application they may have access to that data for an extended period on their phone, or the data may cease to be available as soon as it is submitted.

Security Policy Enforcement

CommCare enables administrative users to tailor security settings based on the level of security that is required to protect the information that exists within a project space. The following options may be enabled by a project administrator:

1. Require that all users in a project space enable two-factor authentication for logins.
2. Shortening a user's session time limit to 30 minutes, and requiring re-authentication after that period of time.

4. Data Security

Data Governance and Privacy

Data enters CommCare via mobile submissions, APIs, and direct upload via the website. If you use CommCare, you own your data. Only authorized users of your project space have access to data or user information stored by Dimagi. Other CommCare users do not have access to the data in your project unless you explicitly give them access. Dimagi's technical staff and system administrators may access data to provide operational support to your project space.

If desired, you may request that Dimagi technical staff not be able to access to your data; this may impact your ability to receive timely and relevant technical assistance from Dimagi.

Data Source Security

In addition to providing a secure environment to host data, CommCare is also designed to ensure that all data that is submitted is protected and cannot be changed.

Once submitted into CommCare, all raw data has a date of creation recorded and cannot be altered. Any changes to a record can be tracked and audited over time. Furthermore, all submissions can be traced to user and time and date of entry into the phone and submission to the server, helping with data auditing. Furthermore, while reporting in CommCare is designed to give users different access levels to different reports, CommCare does not support portioning actual data within a project. This guarantees that users always see the full picture of the data from reports they are given access to.

De-Identified Data

CommCare also has a feature which allows partners to de-identify data prior to export from the servers. Organizations may want to de-identify data in order to protect users' identities, or to better conduct de-identified datasets for research.

Dimagi Terms

To use our services, you are required to review and agree to our Terms. Our Terms consist of our Privacy Policy, Terms of Service, Business Agreement and Acceptable Use Policy. Our Terms are designed to ensure data rights are retained by our clients, while enabling Dimagi to provide and improve our services.

5. Transmission (Network) Security

Encryption

All data transfers to and from the Dimagi server will be conducted over industry standard transmission encryption (HTTPS). All access to the cloud infrastructure is protected behind a firewall and require unique VPN access permissions. Data is transferred through channels that are monitored by intrusion monitoring systems.

Transmission of SMS/IVR Messaging

Dimagi provides software to support projects that exclusively use text messaging, as well as projects that use text messages as an adjunct to a mobile phone based project. Text messaging can be a very useful medium for reaching many people, but there are several caveats worth considering that relate to data security and confidentiality:

- Dimagi sends messages through third-party SMS aggregators, and cannot guarantee the security of those messages.
- SMS is not a guaranteed medium; there is no way for Dimagi to know whether a message was actually sent from the SMS aggregator to the end recipient. Dropped messages, while rare, are a regular occurrence.
- Once a text message is received on a phone there is no guarantee of confidentiality. In general, anyone with access to the phone can read any message.
- SMS messages are sent in plain text, they are not sent in an encrypted format.

6. Conclusion

Dimagi has a robust, SOC 2 Type 2-certified security model, as well as 24/7 monitoring. Security is of the highest priority for our customers, so it is for us as well. For questions about Dimagi's data confidentiality and security policies, please email us at info@dimagi.com.

About Dimagi

Dimagi is a global social enterprise that powers impactful frontline work through scalable digital solutions and services. Since 2002, Dimagi has been guided by a vision of a world where everyone has access to the services they need to thrive. Dimagi is most well-known as the makers of CommCare, the most widely-deployed digital platform for enabling Frontline Workers. Governments and organizations across all sectors use customized mobile, web and SMS applications built on CommCare to deliver services at the frontline. Dimagi is a certified Benefit Corporation with teams in the United States, India, South Africa, Senegal and around the world.