HIPAA Compliance

This page provides HIPAA compliance guidelines for organizations that store health-related data in Service Edge.

**Related Topics**

HIPAA is the United States Health Insurance Portability and Accountability Act of 1996. Among many other subjects, HIPAA sets strict requirements for the storage and transmission of electronic protected health information (e-PHI). For example, it requires organizations to:

- Store and transmit e-PHI in ways that are available only to authorized users
- Prevent inadvertent or deliberate access by unauthorized users
- Ensure the integrity and accuracy of e-PHI
- Provide backups and mechanisms that safeguard e-PHI against disasters and system failures

If your organization uses Service Edge to support health-related services, you must ensure HIPAA compliance of the data that you store and process in Service Edge, or compliance with similar laws that exist in other countries. For example, an organization that provides home nursing care might use the ClickSchedule application of Service Edge to schedule the nurses' visits to patients. It might use ClickMobile to communicate with the nurses in the field. It might use ClickAnalytics to view summary reports of the nurses' activities. This data is likely to be subject to HIPAA requirements. The e-PHI is likely to include Task and Assignment objects, which record the home visits. It might include other data such as Calendar objects, which specify when the patients are available for visits. Object properties that store medical history or images are likely to be especially sensitive.

Service Edge is compliant with HIPAA rules, following the implementation of instructions from the customer. The customer is the covered entity under HIPAA, and is responsible for the risk analysis and management of e-PHI. The article HIPAA Compliance for Customers contains valuable information for customers who are required to protect health information that they store in Service Edge, to ensure their full compliance with the HIPAA rules as a covered entity.

The Service Edge multitenant architecture strictly isolates each organization's data from all other organizations. Communication between the server and the UI, the API, and external applications is by the TLS protocol. The infrastructure provides many mechanisms for enforcing the HIPAA rules, for example:

- Setting user roles and permissions that enable each user to view only the appropriate objects and to perform only appropriate operations on the objects
- Restricting the status transitions that users can perform on objects
- Backing up and restoring data
- Password management policies
- Viewing the history (audit trail) of data updates
- Integrating securely with external systems
- Setting security options of the Service Edge UI
- Securing and encrypting the data that ClickMobile stores on mobile devices

For example, suppose you permit all your users to view Task objects. You permit only specific users to view a custom Task property called PatientMedicalRecord. You can implement this in the following way:

1. **Define** the Task.PatientMedicalRecord property with a data type of Key, referencing a PatientMedicalRecord business-object collection. Store the sensitive data in the PatientMedicalRecord objects.
2. **Configure** the user groups so that only the authorized users can view both the Task objects and the PatientMedicalRecord objects. For the other users, permit access to the Task objects. Deny permission for the PatientMedicalRecord objects.
3. **For the authorized users**, configure the Task form of the Service Edge UI and the ClickMobile UI to display the Task.PatientMedicalRecord property. Optionally, for the other users, configure the Task form not to display the property. Even if you display the property to these users, they cannot view the property values because they do not have permission for the PatientMedicalRecord objects.

We encourage you to coordinate with ClickSoftware about these and other HIPAA aspects. If you send test or development data that contains health-related information to ClickSoftware, consult with ClickSoftware about how to send it in a protected sandbox environment. If it is forbidden for the ClickSoftware staff to view the patient data, scramble or falsify the patient names and identifying information.

**Caution**

The following security guidelines are recommended in order to comply with HIPAA rules:

- By default, saving login credentials on a mobile device or browser is not enabled. In order to comply with HIPAA rules, do not enable saving the user's login credentials.
- By default, an inactive user's session expires after 4 hours. In order to comply with HIPAA rules, the amount of time until an inactive user's session expires should not exceed 8 hours.
- Use the Logout functionality in ClickMobile Touch, or the Sign Out functionality in the Service Edge Mobile app, every time you leave the app.
- Use the Multi-Factor Authentication (MFA) method, which enables confirming the users' claimed identity by utilizing their password and a second factor such as a code that they receive via their mobile device.

**Related Topics**

Business Objects Reference
HIPAA Compliance for Customers
User Management
Configuring a Generic Status Flow
Backing Up and Restoring Tenants
Accessing Service Edge
History of a Business Object
Integrating Click Field Service Edge with External Systems
General Settings for the Service Edge UI
Configuring ClickMobile Touch Security Settings
Custom Collections and Properties
Managing User Groups
Configuring Forms of the Service Edge UI
Editing ClickMobile Touch Forms
Configuring Multi-Factor Authentication
Configuring Session Timeout
General Settings for the Service Edge UI
Accessing ClickMobile Touch and Using the Menu
Using the Settings in the Service Edge Mobile App