Zaptic
Compliance with FDA CFR Part 11
Introduction

This document outlines how Zaptic can be used for the digitisation of records which are subject to FDA compliance. We are committed to providing a solution that will be used in-line with Current Good Manufacturing Practice (CGMP) as outlined by the FDA and see Zaptic as a solution to help customers comply with the regulatory requirements without stifling pace of innovation.

This document outlines the functionality within Zaptic that enables customers to comply with CFR part 11. This document is provided as a guide, the ultimate responsibility of compliance rests with the customer. This document outlines what we consider to be Zaptic responsibility, and what we expect our customers to assume responsibility for.

Approach

This document is created based on FDA CFR part 11 (1997), with clarification provided from the FDA in the document titled “Guidance for Industry” published August, 2003. We take a collaborative approach with our customers and rely on feedback from regulated customers as to how we can improve or clarify our compliance.

Compliance

This section follows the structure as laid out in CFR part 11, 1997 requirements.
11.1 Scope
Because the core of Zaptic is a no-code authoring platform which allows customers to configure a large range of use cases, we rely entirely on customers to decide which use cases fall under the scope of FDA requirements.

11.3 Definition
Through this document Zaptic follows the definitions laid out in CFR part 11.3. Additionally, we use the following definitions for concepts within Zaptic:

Procedure
A folder in Zaptic that organizes tasks, training, guides and files under a heading.

Flow
A task or training that has been configured using Zaptic’s no-code authoring capabilities.

Report
A completed task or training that contains data records submitted by a user.

App
The mobile application available on iOS/Android/Windows which users can use to complete tasks and submit records.

11.10 Subpart B
We rely on customers to decide whether Zaptic is classed as an open or a closed system, though typically it is considered an open system. This section covers requirements for closed and open systems.

A) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Zaptic follows principles outlined in the ISO9001 quality management standard to ensure Zaptic delivers a quality product. All changes are made using an industry standard development, test and release process with rigorous processes for ensuring system stability.

Additionally, customers will typically perform and document their own validation of the system using standard input/output tests. The Zaptic helpdesk can support in answering any queries that come out of these tests. Zaptic can also offer additional validation services as required, such as early access to new releases in a test environment.

(B) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Person should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

It is ultimately the customers responsibility to identify how any records which are required to be submitted to the FDA are done so. Zaptic provides a number of formats in which records can be exported, namely:

- PDF documents
- CSV files
- Excel reports

Additionally, it is always possible to physically print these records and submit them on paper.

(C) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Zaptic’s standard SLA guarantees a 99.5% uptime of the system. We have multi-availability zone back-ups of data and a 24 hour RPO.

Additionally, Zaptic supports a full CSV export of data using the web portal. Customers may elect to use this to download the data on a fixed frequency to a on-site back-up.

(D) Limiting system access to authorized individuals.

Zaptic provides a number of tools to limit access to the system for record creation, system configuration and record access:

User Accounts: Only individuals with a valid user account can access the system. We recommend connecting this to Single Sign On to enforce a 1 account per person policy.

Permissions structure: Only users with the correct permissions can access the admin/configuration interfaces of the solution.

Collaborators: Only users who are made a collaborator of a procedure are able to make edits to tasks within it. This can be managed on a use case by use case basis.

Teams: Tasks are assigned to specific teams of users. Only a user in that team is able to create records.
(E) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Every value that is entered into a report (a record) is tracked against the individual that made that entry. Each audit event is timestamped, with the previous value and new value being recorded.

This audit trail is kept for the length of our contract with the customer, and available to download upon termination. Each report that is submitted has a timeline where the history of that record can be viewed, which includes any changes in status, clarifications, edits and follow up actions that were created:
(F) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Flows in Zaptic can be configured to have mandatory questions, as well as routing which enforces a logical and correct answering of questions. Every field can be configured to be mandatory, with validation to ensure that operators enter a valid value.

Configuration:
(G) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Users can only access the platform by authenticating using a valid account. Via SSO we support multi-factor authentication, key authentication or even biometric authentication. This can be enforced on a device with a mandatory log out after a period of inactivity.

When creating tasks in Zaptic there is in-built digital signature functionality that can be enabled for each quality critical work process. When enabled, this will force the user to re-enter their email and password before submitting the information on screen. This digital signature will be kept with the record for the entire retention period.

It’s also possible to add a ‘Sign on the glass’ signature capability into any flow for quality critical records:
(H) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

We rely on customers to complete specific device checks.

(I) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Training for users of the compliant system is the ultimate responsibility of the customer. Zaptic does support the creation of training modules that can be assigned to personnel to assist with this, that is tracked in a training matrix.

Zaptic also supports the ability to embed work instructions directly into flows to guide users through correctly entering data.

(J) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

This is a customer responsibility, which Zaptic can support with our skills module to track who has completed mandatory policy training.

(K) Use of appropriate controls over systems documentation including:

This is a customer responsibility.
Subpart C Electronic Signatures

This section further details how Zaptic can comply with electronic signature requirements for both closed and open interpretations of the requirements:

11.1 1) Employ at least two distinct identification components such as an identification code and password.

Zaptic has inbuilt authentication that uses email/password. Users are required to enter their own password when they create an account, and are able to self-manage password resets should they forget it.

Zaptic also supports Single Sign On, which may mean that the user is not prompted to enter their password each time they log in. This is defined by the authentication provider, not by Zaptic so this most likely can be configured by the customer. Within Zaptic, users are always prompted to enter their email before being redirected to single sign on. In this scenario, entering the email is the first component. The second component would be the Single Sign On token stored on the user’s device.

11.1 2) Be used only by their genuine owners;

Our policy is that there must be one user for each account, therefore fulfilling the requirement for 2 identification components for each authorized individual.

11.1 3) Be administered and executed to ensure that attempted use of an individual’s electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Zaptic doesn’t currently have functionality that allows for users to sign records on behalf of others. Each action is associated to the authorized user only.
Record Retention

All records created in Zaptic are stored for the length of the contract with no archiving policy in place. At the end of the contract period, this data can be made available to customers in CSV format.

When employees leave, it’s possible to ‘soft delete’ them. This means that their user account will be deactivated and unable to be used anymore - however information pertaining to their actions is still visible. This means that if a user leaves, their user can be deleted however their name and signature will still be visible on legacy records.

If in Europe, this of course needs to be considered alongside GDPR regulations. Given the provisions in GDPR for legal obligations being exempt from the ‘right to be forgotten’ provisions, then Zaptic suggests that the soft deleting of users approach be taken for individuals responsible for quality compliance. Soft deleting a user will ensure that their details are still visible next to records, however other information such as their skills matrix will no longer be available.

To fully comply with the right to be forgotten, Zaptic also supports the ability to hard delete users which will entirely remove their details. If this is done for users who have completed quality records then the record will be shown as being created by a ‘deleted user’.

For each new customer Zaptic will work with them to define what the offboarding process should look like for users and ensure that a strategy is developed to comply with GDPR and their CFR part 11 strategy.

Change control and future developments

Zaptic is committed to supporting customers in achieving FDA CFR part 11 compliance. We rely on our customers to help us understand and further our support of these requirements. Please send all comments, ideas or corrections to support@zaptic.com as we endeavor to keep this document up to date.