PUBLISHED

Simple: Digital Principles

Principles on data ownership, sharing, and privacy for deployments of Simple, the hypertension control app.

Data ownership

- ❏ Countries determine how data are owned and housed. All Simple deployments follow all country principles, regulations, and guidance.
- ❏ The deploying entity control how the data are shared and who has access to it. Individual patient data and personally identifiable information should never be shared other than as authorized by the treating health care provider and according to national regulations.
- ❏ The entity deploying the app (e.g., state or national government) owns the program data. No program data will be published identifying the deploying entity, or with identifiable data from the deploying area, without the area's expressed consent.

Privacy & security

- ❏ If RTSL deploys Simple, it will follow the data hosting requirements of the entity that is deploying the app. Simple encourages government-approved, cloud-based data storage, as managing the app requires software installation, ongoing server maintenance, and reliable support for data center outages and issues. Simple stores all of its server data in an encrypted manner inaccessible to cloud providers, and all cloud provider account details will be owned by the entity deploying the app. If necessary, Simple can be deployed on servers in a government facility, but the above requirements still apply.
- ❏ In RTSL-supported deployments, the need-to-know Simple administrators will have access to metadata (e.g. how long users take to enter patient information) and will use this information to further optimize the app. Metadata does not include any personally identifiable information, nor does it include any actual data (e.g. blood pressure, medications) entered into the Simple app. At all times, RTSL will abide by the Simple Privacy Policy and any other data protection and privacy policies of Vital Strategies.
- ❏ In RTSL-supported deployments, select members of the Simple database engineering team (fewer than 5 engineers) will have access to the complete database for purposes of app implementation and support. A list of all people with access to data will be maintained and shared with state/country authorities; an audit trail of data access will be maintained and made available to the deploying entity on request.
- ❏ Any program can "fork" the Simple codebases and deploy them as independent software. In this situation, neither the Simple tech team nor anyone else at RTSL will have any access to any type of data from the deployment. We ask that those who deploy the app follow the principles of data ownership here.

Software development

- Resolve to Save Lives (RTSL) is committed to providing the best possible digital tool to support health workers and patients to improve hypertension control. The Simple software is developed in accordance with the Principles for Digital Development.
- The Simple app is, and will always remain, open source and free of cost. Each instance of Simple deployment will be the responsibility of the deploying entity to manage (e.g., rules for who can access the data).
- Simple is a digital tool. It does not confer any right or authority to any individual to prescribe or dispense medications or to request laboratory tests.
- As is standard with digital development, RTSL may conduct frequent optimization tests such as:
  - A/B tests of different aspects of the app
  - Qualitative usability testing and observational analysis of software use
  - User satisfaction reviews (e.g. interviews of health care workers to learn how to improve the app).

Data sharing

- RTSL may disseminate anonymized or de-identified information about uptake of the app (e.g. number of deployments, number of users, number of patients covered, time efficiency, number of blood pressure measurements, etc.).
- No program data will be published in medical literature unless the implementing entity consents.
- Anything that reports a specific country/jurisdiction data needs to have the consent of that country.
- As noted above, in no case would patient health information or other individual identifying information be released.