Two independent methods ensure uniqueness of User and sample ID codes or UUID (Unique User ID). within the application. Below we have provided an in-depth explanation of where and how we guarantee uniqueness and security of UUIDs in the application.

## Cryptographic security

First, uniqueness of the UUID is ensured by a pseudo-random number generator (PRNG). PRNGs are a method for generating sequences of numbers that appear random to an outside observer, typically they rely on multiple permutations of an input value, the seed. Our application implements the Python PRNG, based on the Mersenne Twister, which produces pseudo-random values. While the default PRNG implementation is deterministic – that is, if the initial seed is known the entire permutation is computable – we reinitialize the PRNG with a non-guessable random value derived from the current system state and additional bits of entropy via a secure cryptographic primitive for each user. The resulting values are cryptographically secure, meaning in practice they are impossible to guess or compute. We use these secure values to produce a 16-character alphanumeric string, containing the upper- and lower-case alphabet and numbers 0-9 for 1636 possible outcomes (≈7.95×1024).

## Software-enforced uniqueness

Secondly, because we must store these values, i.e. in a database, we enforce a uniqueness constraint on the stored values. This means that if the application were to try to assign two users the same UUID (e.g. in the case of an implementation error or bug in the application), the database would reject such data. The unique constraint is enforced by the database itself and not the application and the application cannot override errors.

## Automated generation

Finally, UUIDs are not user customizable or settable. A UUID is generated when a participant registers on the website and is not influenced by any participant input. Only database administrators (e.g. the application developer(s) and IT staff) and individuals approved by study administrator (Dr. Greg Gibson) have the ability to link UUIDs to PII. While this does not prevent study participants from sharing their UUID information with others, the cryptographic safety guaranteed by (1) ensures that participants cannot “guess” the UUID of others.

We also note that the application is accessible only over HTTPS (SSL/TLS), which encrypts traffic between the application and user. Participants emails, passwords, UUIDs and other PII are never transmitted unencrypted. Additionally, staff will verify participants identity at time of collection ensuring the accuracy of results for contact tracing and follow up by Stamps Health Services.