Data Storage 1

When data is stored, locally or centrally, the way the data is stored is important. Personal, sensitive or medical data need to be stored securely, meaning encryption.

To store data securely, you need to implement:

- Secure encryption algorithms, chosen from the FIPS 140-2 cryptographic algorithms list
- The correct encryption method depending on the type of information. A password must use a one-way encryption using a hashing algorithm and random generated number (salt). Medical data must be encrypted symmetrically in the database.
- A way to manage the encryption key lifecycle
- Sufficient random number generation

OWASP has a cryptographic storage cheat sheet where you can learn more about the rules we listed above.

On a mobile application, you must ensure that encryption keys are stored in the keychain and that the mobile device is able to do encryption. Most of the time, a device access code is needed to enable encryption on a mobile device.