

Personal Identifiable Information

You must protect personal identifiable, sensitive and medical information of the user. There are different measurements that you need to take to ensure that this type of information is secure:

- Client-side caching must be clear of personal identifiable, sensitive and medical information
- Logging and error messages must be clear of personal identifiable, sensitive and medical information
- Protection of data in transit
- Protection of data in rest (see data storage section)

For the protection of data in transit, you must ensure:

- To implement it using industry standards (TLS)
- Certificates need to be checked for validity and correct chaining
- That you only use secure ciphers and don't allow to downgrade to less secure ciphers

On a mobile app, you need to ensure:

- Keyboard caching is disabled on fields with personal identifiable, sensitive and medical information
- The clipboard is disabled on fields with personal identifiable, sensitive and medical information
- That personal identifiable, sensitive and medical information is removed from views when the app is send to the background