Mobile web applications download their data in a central database. The good data is not stored on a local device often for security reasons instead it stored at a central location that can be accessed by users of the application.

Because there are stored at a central location security is easier. Protect the server and the transmission (at all costs) and the data will be protected. Users only download one record or one subset of the data. They then upload a modified or new instance of the data. A security breach on a device would only compromise a limited subset of the data.

Cloud

Cloud devices are basically servers with a fancy name, often offered as a service typically, you can sign-up for space on a shared server (cheaper) or a dedicated server (more expensive)

All medical applications that use protected health information should use a HIPAA compliant cloud service. This basically means that the service uses HTTPS (using SSL) for its transmission security as well as secure authentication logins good physical security, encrypted hard drives and so on.

<https://www.imedicalapps.com/2015/10/medical-apps-103-for-physicians/#>