**VeriWrite Persistence Key Stores**

**Author(s):**

**K.S.Venkatram, Gap Analyst, AOEC 2021**

**@sign: @iceclimbingzany**

**Dates of documentation:**

**10/07/2021: Draft created**

**11/07/2021:**

**Hackathon:**

[**FHIR @hack 2021**](https://devpost.us2.list-manage.com/track/click?u=4812d3b2b48f57c38070d62e7&id=801e6f8890&e=861c76b535)

**Problem statement:**

Healthcare providers regularly collect sensitive medical information about their patients.

This forces clinicians to spend excessive amounts of time on data entry, and burdens hospitals with the responsibility of organizing, maintaining, and protecting a massive database of confidential patient records.

Develop a solution that prioritizes patient/clinician experience.

**At the idea level**

**The VeriWrite Persistence Key Store**

As SMART Phones may be preferred by practitioners and clinicians in independent clinics or businesses, the problem solving could be extended to

1. Create a separate @persistence keystore that can be used by practitioner or clinician to prescribe and share diagnostic summaries with a patient

2. Create a separate @persistence keystore that can be used to read, write, update, delete “Companion card data” where this data may be complete card information or may be key hole specific card information

3. Create a separate @persistence keystore that can be used to read, write, update, delete “Health Policy data” where this data may Health Policy information or may be Claim information

4. Associate Data sharing and privacy with these keystores, where the access to each data record could be

* **public:** keystore data (like LineIcon card data) that can be read by anyone without need for authentication
* **shared:** keystore data (like Prescriptions, Diagnostic summaries and Vital health data + Confidential & Sensitive card data) that the owner has explicitly granted the right to some entity to read it after proving they are who they claim to be
* **private:** keystore data (like Healthcare Policy data) that is only accessible to the owner (requires authentication)

4. Add a notification verb for the keystores containing “Prescription”, “Diagnostic Summary”, “Line Icon data”, “Vital health + C-S data” to alert the @Platform VeriWrite application when new data shared by others is available

5. Incorporate the monitor verb to create a persistence connection to the keystores to access / update data

6. Enable new Vital HealthCare Applications that are certified as @protocol compliant (@pps) to access and diagnose data stored in the @persistence keystores for prescriptions and diagnostic summaries

.

7. Enable new VeriSafe Healthcare Applications that are certified as @protocol compliant (@pps) to access and infer data stored in the @persistence keystore for Companion Cards like protected Vital health data + Confidential & Sensitive card data or public LineIcon data

.