Orange Card-based Secure Medical Record Storage System

History of Medical record storage systems:

Google health and Microsoft health vault are two of the prominent Medical Record storage systems that have been developed over last decade.

Google Health was under development from mid-2006. In 2008, the service underwent a two-month pilot test with 1,600 patients of The Cleveland Clinic. Starting on May 20, 2008, Google Health was released to the general public as a service in beta test stage.

On September 15, 2010 Google updated Google Health with a new look and feel.

On June 24, 2011 Google announced it was retiring Google Health in January 1, 2012; data was available for download through January 1, 2013. According to Google, the project was terminated due to lack of widespread adoption.

Google Health was a personal health information centralization service (sometimes known as personal health record services). The service allowed Google users to volunteer their health records – either manually or by logging into their accounts at partnered health services providers – into the Google Health system, thereby merging potentially separate health records into one centralized Google Health profile.

Privacy concerns

A personal health record, or PHR, is a health record where health data and information related to the care of a patient is maintained by the patient. This stands in contrast to the more widely used electronic medical record, which is operated by institutions (such as hospitals) and contains data entered by clinicians or billing data to support insurance claims. The intention of a PHR is to provide a complete and accurate summary of an individual's medical history which is accessible online. The health data on a PHR might include patient-reported outcome data, lab results, data from devices such as wireless electronic weighing scales or collected passively from a smartphone.

PHRs can contain a diverse range of data, including but not limited to:

- allergies and adverse drug reactions
- chronic diseases
- family history
- illnesses and hospitalizations
- imaging reports (e.g. X-ray)
- laboratory test results
- medications and dosing

- prescription record
- surgeries and other procedures
- vaccinations
- and Observations of Daily Living (ODLs)

There are two methods by which data can arrive in a PHR. A patient may enter it directly, either by typing into fields or uploading/transmitting data from a file or another website. The second is when the PHR is tethered to an electronic health record, which automatically updates the PHR. Not all PHRs have the same capabilities, and individual PHRs may support one or all of these methods.

In addition to storing an individual's personal health information, some PHRs provide added-value services such as drug-drug interaction checking, electronic messaging between patients and providers, managing appointments, and reminders. Addition of analytics of patient's medical data will allow a patient to investigate other data resources that can shed important light on patient's past history and history of other members of family to formulate future steps for patient as well as patient. This is an important shift in paradigm for patient, physician interaction where in the past only the physician had access to all the records and had limited time to analyze a patient's history considering that the physician normally meets a patient when patients is not well. In the new paradigm with patient having free access to all his records and easy analytic tools and plenty of time, the patient can consult with the physician as and when the patient feels the need.

Image-X's Orange Card system provides personal health record repository that uses its patented Secure Document storage method outlined in US Patent # 8613105. Orange card system technology offers a secure way to store a patient's personal medical records. The technology is secure and compliant with the new Health Information Portability and Accountability Act of 2014 (HIPAA). The document storage and retrieval process uses advanced encryption for secure and easy access for physicians or other health professionals attempting to access a patient's Health Care Directive. Orange card based eSecureDox is a good introductory step for a hospital attempting to apply an overall Health Information Exchange or an Electronic Medical Records System. eSecureDox system is interoperable with larger companies Health Information Systems. In addition the Secured Document Repository is already integrated with MEDICITY's HIE for universal credential verification.

How the Orange Card System Works:

The Orange Card system offers easy access to patient's healthcare records. Once the Orange Card is printed and given to the patient, this acts as one of the "keys" in the two key authentication process. From one end, the doctor is able to use his login information to verify himself as a certified health professional. From the other end, the patient's Orange Card contains a 27 digit pin that uniquely identifies the patient with his or her Personal Medical Records. Once both are input, the doctor is able to access the patient's document and see the

documents from anywhere, at any hospital. If the patient is not conscious, his records are still available to the doctor simply by the doctor having in his possession the patient's Orange Card and the doctor verifying himself as a healthcare professional. Every time a medical record is retrieved, the patient receives a secure e mail via CMAmedmail, a secured e mail process developed by Image X. CMAmedmail also sends an intimation on users normal e mail e.g. g mail, outlook etc.

Three Perspectives: Technologist, Patient, Physician

Technical Perspective:

Data security and personalization is an extremely difficult and expensive proposition for most technologists. The easiest method for the securing and personalization of data for a single user is simple - we do it every day when we log-in to a system with a username and password. However, if we want to share this system data with someone else, we need to share our log-in username and password. In regards to health records this becomes an issue of confidentiality, particularly if it provides the other viewer access to all public or private data. To solve this issue, data must be separated into shareable and non-shareable partitions. Unfortunately, healthcare data is generally not considered 'shareable.' Patients only want physicians to have access to the information, and upon their individual consent.

Patient's Perspective:

All perspectives agree the patient is the owner of his medical information, but realistically he is not in control of his medical records. Traditionally, medical records are stored by the physician at the hospital or clinic where medical service are provided. Because of this, most patients have never seen or read their medical records. Asking a patient to store medical records in his or her possession is nearly impossible, and the need to upload medical records to a shared repository is difficult for both patients and physicians. As a result, a system is needed in which medical records can be uploaded by a third party, such as hospital or clinic workers, after securing approval from the patient. Once the records are in the shared repository, a method must be devised to separate the information so anyone with access to the system cannot view or randomly search all records. What if the patient loses his Orange Card? Address the security in place to account for the lost card. If a card is lost the user can get a new card after authentication and the lost card will be deactivated

Physician's Perspective:

Physicians are responsible for providing patient care. They do not have the time to remember multiple passwords to a system that requires substantial effort to retrieve a patient's records, especially in the case of an emergency. Anyone who is familiar with the situation at an Emergency Room (ER) can imagine how difficult it would be to design a shared repository for ER

physicians. However, with other staff members available, the records could be accessed and presented to the appropriate physician quickly and electronically, even from his/her mobile device.

Summary

In summary Orange card system has been developed to overcome the problems associated with other document sharing systems to provide a secure medical record sharing system that:

- Electronically stores Personal Medical Records, and is HIPAA compliant
- Allows secure retrieval by physicians 24/7 in case of emergency
- Can be filled out online while maintaining privacy and confidentiality
- Prints an “Orange Card” with a unique identifier for secure electronic retrieval from anywhere on multiple devices.