

User Scenario: Medical

[Return to Part II: User Scenarios](#)

Overview

[Return to Top](#)

There are conflicting interests at work in the Medical area. The need for information about a patient in order to care for the patient versus [Data Protection](#) and the privacy concerns for patient's privacy. The following are some of the restrictions apply in California:

- [Health Insurance Portability and Accountability Act \(HIPAA\)](#)
- [General Data Protection Regulation \(GDPR\)](#)
- [Data Protection Act 2018](#)
- [California Consumer Privacy Act \(CCPA\)](#)
- [01_problem](#)
- [02_existing](#)
- [03_theory](#)

Problem Statement

[Return to Top](#)

Lilly is a 90 year old woman living in a Memory Care Facility (MCF) in San Diego, California, USA. She routinely sees her medical doctors for routine healthcare and specialists that see her for an existing heart problem, dementia, dentalcare, etc.

Lilly is a resident of the MCF because she has debilitating dementia and is in **moderate**¹⁾ to **serious decline**²⁾ and can no longer be taken care of by family and friends. She is not capable of communicating serious health issues to those around her nor remember what the medical team has told her even a few minutes before. She can not remember her insurance numbers, where she lives, her family or her current set of diagnosis.

Lilly does have a **Durable Power of Attorney**³⁾ who does not live in the immediate area and can not be available to provide the answers required by the medical team to provide the best healthcare for Lilly.

Lilly falls down in the MCF and hits her head. She appears confused but that is “normal” for her in her current state, however, it is also a sign of a concussion⁴⁾. MCF policy is that when a resident hits their head, they need to be seen by a doctor. Figure 1 outlines at a simplified, high level the course of events for Lilly and the role of medical records during the process which includes a ride in an ambulance to the emergency room, the required medical assessment of her condition. a short stay in a hospital and

rehabilitation hospital. When she is able, Lilly returns to the MCF.

Existing Simplified System without DIDO

[Return to Top](#)

The following is an extremely simplified system that is meant to provide an overarching framework for using DIDOs to solve medical problems. It is not meant to be completely accurate but is provided for illustrative purposes. Others are encouraged to use this as a starting point for more complicated reality based scenarios.

Activities

[Return to Top](#)

The following is only a simplified list of the steps involved in providing Lilly's healthcare needs that stem from a fall.

1. Lilly is a resident of the Memory Care Facility (MCF)
2. She routinely see's her doctors and the write simple diagnostic reports and prescription for her. Each doctor keeps their own records and provides a diagnostic summary and prescriptions which are recorded at MCF in Lilly's Medical Records
3. Lilly has a fall and hits her head and it is bleeding.
4. An MCF staff member helps her to the bed and looks at the wound. Determines the wound is not serious but follows MCF protocols and calls for an ambulance to take Lilly to the Emergency Room. She files a incident report and sees Lilly safely to the Ambulance where she provides some information about Lilly to the paramedics and EMT in the ambulance
5. Lilly's vital signs are checked in the ambulance and initial first aid is given with the IV and a sedative.
6. The ambulance arrives t the Emergency Room (ER) where Lilly's is transferred along with original medical records from MCF and vitals obtained while Lilly was in Ambulance
7. Medical tests and procedures are conducted to determine the severity of Lilly's injuries. She is asked some basic memory questions where Lilly appears confused. It is determined that Lilly will be placed in the Hospital for observation and to assess the severity of her fractured pelvis.
8. Lilly is discharged from the hospital and transferred to a rehabilitation hospital where she receives physical and occupational therapy
9. Lilly is finally released from the Rehab hospital and returned to the MCF.

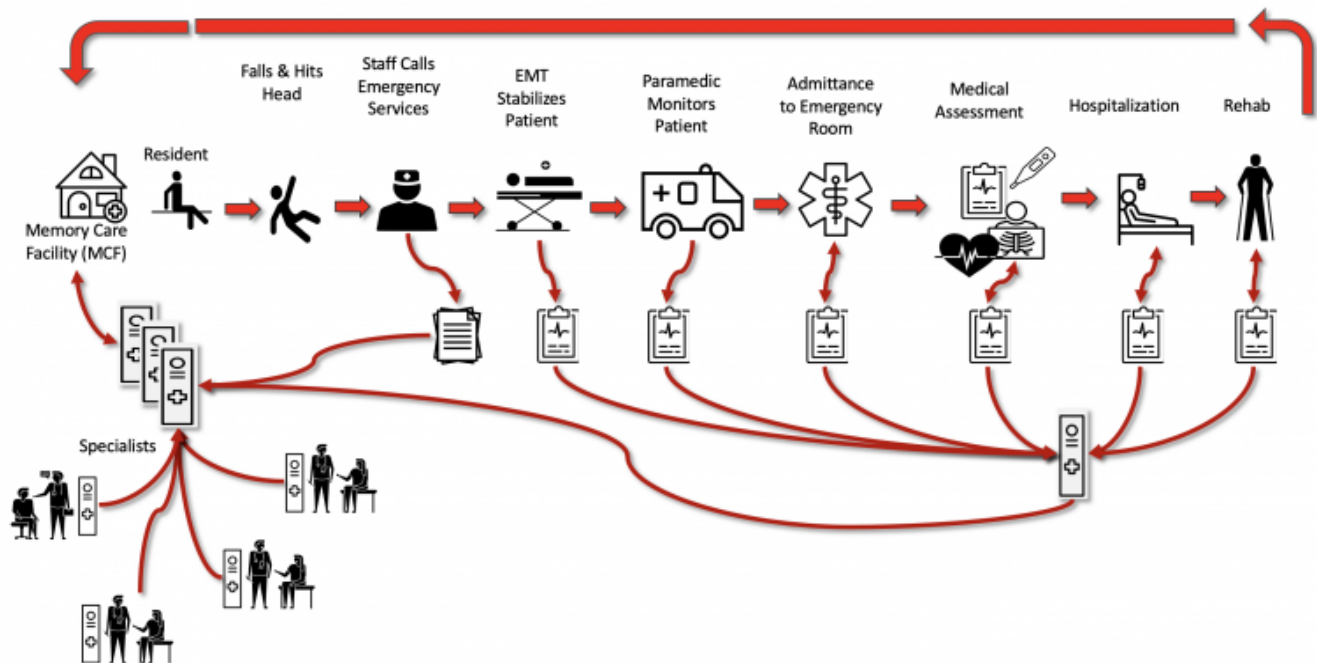


Figure 1: A simple, idealized traditional record flow for a Memory Care Resident patient incident.

Issues

[Return to Top](#)

1. Lilly's medical records are dispersed across multiple organizations and doctors offices.
2. Lilly is unable to provide a coherent personal history, allergies, medications, the list of her doctors, personal record of what happened to her, when it occurred, and what was done for her treatment.
3. This scenario does not cover all the disclosure agreements that Lilly or others have signed on her behalf.
4. This scenario is complicated by insurance, in Lilly's case social security and Medicare Part B as well as any other insurance that may cover her
5. This scenario does not cover the dissemination of medical records back to the Lilly's other doctors
6. This scenario does not include all the insurance and disclosure statements that were either signed by Lilly or by others on her behalf.

Theoretical Simplified System using DIDO

[Return to Top](#)

Activities

[Return to Top](#)

The following activities are based on the assumption that a medical records system is implemented using a DIDO. The other assumption is that the medical records belong to the patient and not the MCF, doctors,

or other institutions involved in the care of the patient.

It is only a simplified list of the steps involved in providing Lilly's healthcare needs that stem from a fall.

1. Lilly is a resident of the Memory Care Facility (MCF)
2. She routinely see's her doctors who write simple diagnostic reports and prescription for her. Each doctor keeps their own records and provides a diagnostic summary and prescriptions to a DIDO with Lilly's Medical Records.
3. Lilly has a fall and hits her head and it is bleeding.
4. An MCF staff member helps her to the bed and looks at the wound. Determines the wound is not serious but follows MCF protocols and calls for an ambulance to take Lilly to the Emergency Room. She files a incident report and sees Lilly safely to the Ambulance where she provides some information about Lilly to the paramedics and EMT in the ambulance as both a report a link to a DIDO archive containing Lilly's medical records
5. Lilly's vital signs are checked in the ambulance and initial first aid is given with the IV and a sedative. The vitals are recorded into a DIDO which does not have to be connected to the internet to record the dataa
6. The ambulance arrives at the Emergency Room (ER) where Lilly's is transferred along with original medical records from MCF and vitals obtained while Lilly was in Ambulance. The information required to access Lilly's sidechain (stream) of records.
7. Medical tests and procedures are conducted to determine the severity of Lilly's injuries. She is asked some basic memory questions where Lilly appears confused. It is determined that Lilly will be placed in the Hospital for observation and to assess the severity of her fractured pelvis. The records are added to the Lilly's DIDO sidechain (stream).
8. Lilly is discharged from the hospital and transferred to a rehabilitation hospital where she receives physical and occupational therapy. The new data is added to Lilly's sidechain (stream)
9. Lilly is finally released from the Rehab hospital and returned to the MCF where here sidechain (stream) is merged back into the main medical DIDO that contains Lilly's records

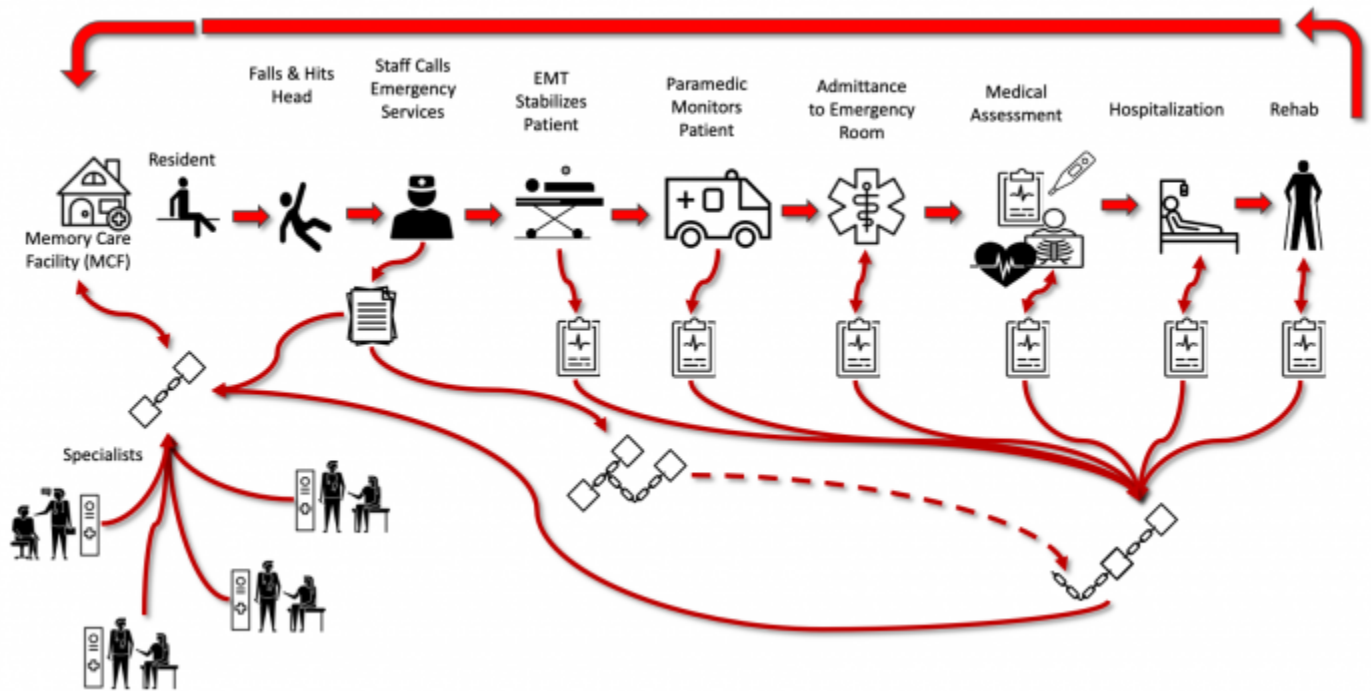


Figure 2: A simple, idealized theoretical record flow for a Memory Care Resident patient incident.

Issues

[Return to Top](#)

1. The concept of medical data ownership. Does the data belong to the patient, the medical provider or both? This is a controversial subject in the USA and every state seems to have different rules⁵⁾

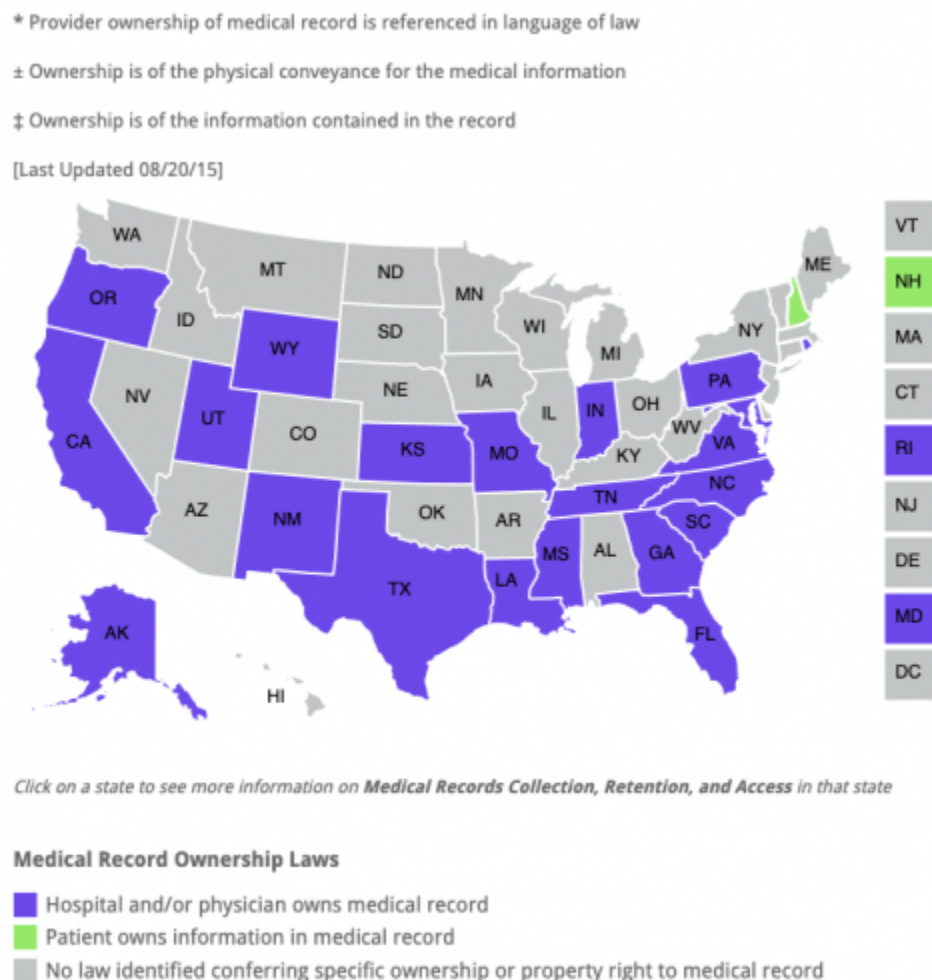


Figure 3: Map of Patients rights in the USA

Europe on the other hand has a single unified approach to patient data under the [General Data Protection Regulation \(GDPR\)](#) ⁶⁾

Table 1: Summary of patient rights within the EU.

What Right?	What does it mean for Patients?
To access one's own personal data	◦ The right to access your own personal data is part of your fundamental right to data protection ◦ The right to access your medical record is explicitly mentioned in the new Regulation ◦ If you request a copy of the personal data being processed by a data controller about you, they have to provide it to you ◦ The Regulation encourages the establishment of remote ways to provide you with access, such as electronic health records ◦ The controller has the right to check your identity before providing you with the data

What Right?	What does it mean for Patients?
Right to data portability/to transfer your data from one data controller to another	◦ When you have consented to provide your health data, and that it is in a machine readable format (e.g. in electronic form), you can request to receive a copy in order to transfer it to another entity or person, and you can also demand that it is transferred directly for you ◦ It could be positive and encourage controllers (hospitals, doctors) to ensure that data is in a format that can easily be transferred
Right to object to the processing of your data	Under the new regulation you can object to the processing of your data by a controller under these circumstances: ◦ If the processing happens for a task performed in the public interest ◦ If the processing happens for the legitimate purpose of the controller ◦ If it happens in the context of direct marketing
Right to rectification or erasure of data	You can ask for the rectification of inaccurate personal data (e.g. in your medical record) and incomplete data completed
Right to erasure (so called "right to be forgotten")	You can have your data erased. This is the so-called "right to be forgotten". This is especially the case if: ◦ you have withdrawn consent and the data controller has no other grounds for processing your data ◦ if there is no longer a purpose for processing it, in accordance with the principle of limited storage and data minimisation. ◦ if the processing is unlawful in the first place When the controller has made the information public, e.g. online, he has to take reasonable step to ensure other controllers also remove links etc. in order to implement your rights.

2. While the patient remains constant, the providers might change. For example, a patient moves and can no longer use the same doctor or the patient changes insurance companies requiring a change in provider of the medical provider. This implies an [Access Control List \(ACL\)](#) arrangement where the patient can authorize others to add new content, make updates, mark for deletion.

Note: The contents of a DIDO are immutable, therefore, traditional ACL permissions such as Write and Delete have no meaning. However, it is possible for older content to be replaced by newer content requiring the new content to point to the previous content. It is also possible to mark content as deleted.

Table 2: Potential DIDO Commands for Medical Records.

Operation	Description
CREATE NEW	This creates a new person in the Medical DIDO. For example, a new patient is added to the Medical DIDO. The CREATE NEW command adds the new patient and returns a patient specific couple of AsymmetricKeys (i.e., publicKey and privateKey). The public key is used to uniquely identify the patient within the medical DIDO and can be used to encrypt any information for that particular patient. The privateKey is used to decrypt the information in the Medical DIDO for that specific patient. The privateKey NEEDS TO BE KEPT PRIVATE! The ECHO command is used to place information onto the console log. Some of the fields used to describe a patient might be name, birthday, gender, marital status, address. There are other fields that are probably not required such as insurance id, group id, medicare number, etc. All of these fields are probably classified as Personal Identifiable Information (PII). The following is a proof of concept for creating a new patient in the Medical DIDO. <pre> patientKeys AsymmetricKeys = CREATE NEW { "patient" : { "name": "Lilly McSmythe", "birthdate": "11/25/1931", "gender" : "F", "maritalSatus" : "married" } } ECHO patientKeys.publicKey; "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E" </pre>

Operation	Description												
MANAGE ACCESS	Updates or modify the Access Control List data. The Patient Data Object (sometimes referred to as a Smart Contract) maintains its own internal Access Control List (ACL) that contains users, medical roles and access roles (i.e., READ, WRITE, etc). In this example, we add two doctors to the list: primaryPhysician, and 'cardioVascularMd'. We also grant them access roles that are traditional such as READ, UPDATE but also roles like UPLOAD and SEARCH. At this point, these roles are just conceptual in nature and need to be refined in the future. All the fields within the Patient Data Object (Smart Contract) are considered private and can only be accessed using getters and setters. The by field will be filled in by the infrastructure. <table> <tr> <th>Privilege Type</th><th>Description</th></tr> <tr> <td>READ</td><td>Granting READ privilege allows the access to all the Read attributes or operations associated with the patient</td></tr> <tr> <td>UPDATE</td><td>Granting UPDATE privilege allows the access to all the writable attributes or operations associated with the patient</td></tr> <tr> <td>UPLOAD</td><td>Granting UPLOAD privilege allows for new content to be added to the patient record (i.e., images, lab results, vitals, etc).</td></tr> <tr> <td>SEARCH</td><td>Granting SEARCH privilege allows for the Read attributes or operations to be searched for particular strings. It only returns a TRUE or FALSE. All Personal Identifiable Information (PII) can be hidden from the search.</td></tr> <tr> <td>DELETE</td><td>Granting DELETE privilege allows for the content of the patient record to be marked as deleted OR optionally for the content to be burned by destroying the private key</td></tr> </table> For example: <pre>primaryPhysician MedicalDoctor { "id" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D55555", "name" : "Dr. Jane Lee Gupta", "phone" : "1-619-555-1212", "email" : "j.l.gupta@medics.com" } MANAGE ADD { patient : { "id" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D55555", "primaryPhysician" : primaryPhysician.id } } MANAGE REPLACE { patient : { "id" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "cardioVascularMd" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2DDDDD" } } MANAGE GRANT { patient : { "id" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "cardioVascularMd" : "READ, UPDATE, UPLDAD" } } MANAGE GRANT { patient : { "id" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "primaryPhysician" : "SEARCH" } }</pre>	Privilege Type	Description	READ	Granting READ privilege allows the access to all the Read attributes or operations associated with the patient	UPDATE	Granting UPDATE privilege allows the access to all the writable attributes or operations associated with the patient	UPLOAD	Granting UPLOAD privilege allows for new content to be added to the patient record (i.e., images, lab results, vitals, etc).	SEARCH	Granting SEARCH privilege allows for the Read attributes or operations to be searched for particular strings. It only returns a TRUE or FALSE. All Personal Identifiable Information (PII) can be hidden from the search.	DELETE	Granting DELETE privilege allows for the content of the patient record to be marked as deleted OR optionally for the content to be burned by destroying the private key
Privilege Type	Description												
READ	Granting READ privilege allows the access to all the Read attributes or operations associated with the patient												
UPDATE	Granting UPDATE privilege allows the access to all the writable attributes or operations associated with the patient												
UPLOAD	Granting UPLOAD privilege allows for new content to be added to the patient record (i.e., images, lab results, vitals, etc).												
SEARCH	Granting SEARCH privilege allows for the Read attributes or operations to be searched for particular strings. It only returns a TRUE or FALSE. All Personal Identifiable Information (PII) can be hidden from the search.												
DELETE	Granting DELETE privilege allows for the content of the patient record to be marked as deleted OR optionally for the content to be burned by destroying the private key												

Operation	Description
MARK AS DELETED	Mark a person as deleted in the Medical DIDO. For Example: DELETE <pre>{ "patient" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D5555" }</pre>
UPDATE CONTENT	Update a person's information in the Medical DIDO. For example: UPDATE <pre>{ "patient" : { "id" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D5555" "maritalStatus" : "Widowed", "maritalStatusChangeDate" : "11/25/2021" } }</pre> UPDATE <pre>{ "patient" : { "id" : userKeys.publicKey, "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D5555" "DateOfDeath" : "11/25/2031" } }</pre>
UPLOAD ANCILLARY DATA	This allows for Ancillary data to be uploaded to the Patients Medical DIDO. Ancillary data is data that is associated with the patient such as vitals, images, lab result, etc. UPLOAD <pre>{ "patient" : { "id" : patientKeys.publicKey, "by" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D5555" "ancillaryData" : { "image": { "type": "xray", "view": "posteroanterior", "date": "5/7/2021" }, "image": { "type": "xray", "view": "Decubitus", "date": "5/7/2021" } } } }</pre>
ERASE	Removes the Personal Identifiable Information (PII) information from the patient in the Medical DIDO allowing the patient to be forgotten in compliance with General Data Protection Regulation (GDPR) ERASE <pre>{ "patient" : patientKeys.publicKey }</pre>

3. The [General Data Protection Regulation \(GDPR\)](#), [Data Protection Act 2018](#) and the [California Consumer Privacy Act \(CCPA\)](#) prohibit information from being “*kept for no longer than is necessary*”. How long should a medical record be kept by a medical provider? An insurance provider? Within the USA, its state-by-state, see:
<https://www.healthit.gov/sites/default/files/appa7-1.pdf>

Table 3: Example of minimum medical records retention for California and Connecticut.

State	Medical Doctors	Hospitals
California	California: Indefinitely, if possible. See CMA ON-CALL: The California Medical Association's Information-On-Demand Service, available at HealthIT.gov (accessed August 14, 2008).	Adult patients 7 years following discharge of the patient. Minor patients 7 years following discharge or 1 year after the patient reaches the age of 18 (i.e., until patient turns 19) whichever is longer. Cal. Code Regs. tit. 22, § 70751(c) (2008).
Connecticut	7 years from the last date of treatment, or, upon the death of the patient, for 3 years. Conn. Agencies Regs. § 19a-14-42 (2008).	10 years after the patient has been discharged. Conn. Agencies Regs. §§ 19-13-D3(d)(6) (2008).
EXPIRE	The Medical Record expires after a certain amount of time, after a certain date, or when an event occurs Medical DIDO. For Example: <pre> EXPIRE { "patient" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "onDate" : "20210508" } EXPIRE { "patient" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "after" : "128 hours" } EXPIRE { "patient" : "0xDC25EF3F5B8A186998338A2ADA83795FBA2D695E", "when" : "DEATH_OF_PATIENT" } </pre>	

4. A DIDO that allows that uses an ACL to control what kinds of operations that someone else can perform (see MANAGE ACCESS). Although the Medical DIDO only allows for a single owner, it allows for many participants. For example, each doctor adds information to the the patients Medical DIDO (see: UPDATE CONTENT).
5. The use of an [Archival Node](#) for the long term storage of Medical DIDO patients.
6. The idea of a sidechain or specialized stream that will be joined back to the main "chain"

1)

Moderately Severe decline They may not remember their phone number or their grandchildren's names. They may be confused about the time of day or day of the week. At this point, they'll need assistance with some basic day-to-day functions, such as picking out clothes to wear.

<https://www.webmd.com/alzheimers/types-dementia#2-6>

2)

Severe Decline They'll begin to forget the name of their spouse. They'll need help going to the restroom and eating. You may also see changes in their personality and emotions.

<https://www.webmd.com/alzheimers/types-dementia#2-6>

3)

Durable Powers of Attorney helps you plan for medical emergencies and declines in mental functioning and can ensure that your finances are taken care of. Having these documents in place helps eliminate confusion and uncertainty when family members have to make tough medical decisions.

<https://www.legalzoom.com/articles/what-is-a-durable-power-of-attorney>

4)

A **Concussion** is a traumatic brain injury that affects your brain function. Effects are usually temporary

but can include headaches and problems with concentration, memory, balance and coordination.

<https://www.mayoclinic.org/diseases-conditions/concussion/symptoms-causes/syc-20355594>

5)

George Washington University, Health Information and the Law, 20 August 2015, Accessed: 6 May 2021,

<http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison>

6)

European Patients Forum, The new EU Regulation on the protection of personal data: what does it mean for patients? Accessed: 6 May 2021,

<https://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf>

From:

<https://www.omgwiki.org/dido/> - **DIDO Wiki**

Permanent link:

https://www.omgwiki.org/dido/doku.php?id=dido:public:s_cli:05_contents:02_prt:medical:start&rev=1621551384

Last update: **2021/05/20 18:56**

