医疗信息授权共享设计

存储数据内容

（A） Patient Data Reference

该数据为医疗系统中数据的一个索引，指明了一条医院数据的拥有者、提供者、访问方式以及访问权限。

1. 数据结构

   （recordId，ownerId，providerId，accessInfo，permission）

   ```
   recordId：数据的唯一编号，用以唯一标示一条医疗数据
   ownerId：数据的拥有者
   providerId：数据提供者
   accessInfo：数据获取方式信息，例如包含了查询数据的服务器地址，端口，数据的schema等
   permission：该条数据访问的权限设置(list)
        （consumer, dataItem,  query, hash, deadline）
   ```

2. 数据管理方案

数据提供者：创建该类数据，并对accessInfo拥有所有权。
数据拥有者：管理该类数据中的permission选项。

（permission可能需要设计一下）

（B） User‘s Summary

该数据用于存储与用户相关（不限于拥有或者管理关系，也包括查看关系）的PDR信息，便于用户查找到自己可以查看的数据项，相当于一个归总目录。
每个用户都将拥有一个这样的数据项，不管是医院、用户或者第三方机构。

1. 数据结构

   （userId，flag，count, [recordId1，stauts; recordId2，status...]）

   ```
   userId：用户id
   flag：用以表明该数据是否被更新过，需要user进行确认
   count：用于记录其后list的长度。
   []：该list用于记录与自己相关的所有记录，recordId即为Patient Data Referene的唯一id；sta
   tus用于表明该条是否经过用户认可。
   ```

2. 数据管理方案

数据recordId的拥有者或者提供者（即PDR的拥有者和提供者）：对list进行增加操作；（该操作是授权操作的一部分，可见用户授权部分）######

```
recordId提供者：初次创建的时候或者更改的时候可以对owner的record list进行操作，不能对非owner的record list进行相关操作；
recordId拥有者：可以将该recordId加入到任何人的list中，但是之前需要permission修改操作。
```

该数据对应的用户：对status拥有确定权。

（好像status并没有什么用处，看起来可以删掉，但是在一定程度上，是不是可以确保别人随意更改自己的summary？）

数据流转

1. 医院增加record

1. 创建数据到自身数据库
2. 将数据对应（A）record 记录到区块链
3. 将数据对应的recordId更新到数据owner的（B）User's Summary中
4. owner确认该更新

（需要更改provider的record list）

至此用户将拥有该条数据的所有权。

2. 查询数据过程

1. 用户访问自己的User's Summary，查询recordId
2. 用recordId查询数据索引
3. 用查询到索引内容发送查询请求到数据提供者
4. 数据提供者验证请求发送者以及查询recordId，验证查询权限
5. 按照权限返回数据

3. 授权数据给第三方（可以是医院，其它机构等）

1. recordId记录拥有者更改该条数据中的permission内容，对需被授权的用户进行权限设置；
2. 用于将recordId加入到被授权用户的list中；
3. 被授权用户进行确认；（是否有必要）
4. 第三方查询数据（见2）。

智能合约提供的接口

Invoke

用户增加操作

用户注册功能。

接口名称

register

传入参数

（userId)

执行操作

创建对应的userId的summary的数据项，即B。

```
设置flag为0，count为0，list内容["0"+"0"]
```

医院增加数据A

医院在每次产生新的数据的时候，都需要通过该接口提交记录到区块链。

接口名称

add

传入参数

（recordId，ownerId，providerId，accessInfo，permission）

```
recordId：唯一编号，由医院id+该条数据在医院的唯一id确定
accessInfo：获取数据方式
permission：为空?
```

执行操作

1. 检查recordId的存在性
2. 写入该条数据到state中
3. 将该条数据的recordId添加到ownerId和providerId的 （B） User's Suammry中

   ```
   ownerId：处于待确认状态，并更改status为1，更改flag为1，count递增
   providerId：处于待确认状态，并更改status为1，flag不变，count递增
   ```

医院更新数据A accessInfo

当医院数据库访问方式进行修改的时候，对该字段进行修改。

接口名称

updateAccessInfo

传入参数

（recordId，providerId, accessInfo）

执行操作

1. 权限确认，是否为该record的provider对其进行修改
2. 修改accessInfo内容

owner修改数据A权限修改permission

数据拥有者对数据进行授权操作时，需要进行权限修改。

接口名称

updatePermission

传入参数

(recordId，ownerId，[consumer, dataItem, query, hash, deadline])

```
recordId：为数据ID
ownerId：所有者的ID
[]:permission所需要给的权限设置
consumer：被授权人Id
dataItem：授权访问的数据项
query：查询语句
hash：查询得到对应的hash值
deadline：权限时限
```

执行操作

1. 确认权限，是否对owner是否对该数据项的拥有权
2. 修改recordId对应的A数据permission内容，该操作为简单增加操作
3. 修改consumer对应的B数据list内容

> 该操作需要更改内容包含B数据中flag为1，count递增，以及list。

数据B确认

在list被修改后，对其进行的确认操作。

接口名称

confirmSummary

传入参数

（ownerId，recordId，op）

```
op：对该数据项的操作为接收或者拒绝，其中ac表示同意，re表示拒绝
```

执行操作

1. 确认权限问题？？？
2. 查看状态是否处于待确认状态
3. 查询对应list并实现对应操作

   ```
   ToDo!!!!!!!
   如果op为拒绝操作，删除list中内容，如果操作者为recordId的owner，将删除相关记录，更改provid
   er方的状态!
   如果op为接收操作，更改状态，并更改provider相关状态
   ```

Query

查询权限

查询是否拥有该条数据的访问权限。

接口名称

havePermission

传入参数

（userId, recordID）

```
    userId：查询者的id
    recordId：需要查询数据的唯一id
```

执行操作

1. 获取recordId对应的permission内容
2. 筛选userId部分内容，提取query部分，进行对比

3. 返回True or False

数据索引查询

查询单条数据索引相关的内容，即A数据项。

接口名称

getRecord

传入参数

（userId， recordId）

执行操作

1. 权限确认
2. 返回数据A

用户索引查询

查询用户自己的summary内容。

接口名称

getSummary

传入参数

（userId）

执行操作

1. 查询数据B并返回