[Challenge](#_6ex8k1eidsv8)

[Goal/Proposal](#_xtr8ojh62srp)

[Existing Patient Privacy and iSanté Authentication and Confidentiality Features](#_l0tzy4y8hb8n)

[Proposed New Features To Support Confidentiality](#_m9w578yxiyd9)

[User Profiles](#_dbnluop2ofg2)

[Profile-based iSanté Web Application Elements](#_90c6dy908mlm)

[Access Reporting and Alerts](#_7becdxtlwpr4)

# 

# Challenge

# 

MSPP and CDC have expressed a concern that staff not working with HIV positive patients (i.e. primary care, ob-gyn, tuberculosis, etc.) could either inadvertently or intentionally gain access to HIV-related patient information not appropriate to their role.

However, there is also a need to support quality data, which requires providers to have knowledge of a patient’s full record.

Formal policies regarding confidentiality of medical records in Haiti do not currently exist, nor are there systems in place for monitoring or implementing consequences for inappropriate access to records. It appears unlikely that such policies, monitoring, or consequences will be developed by MSPP in the near future.

# Goal/Proposal

The statement of need: provide confidentiality and restrict access to sensitive health information for people not authorized to see it, while enabling access for providers who need it.

This document reviews existing iSanté confidentiality features and protocols, then proposes some structural modifications and enhancements to iSanté that will facilitate confidentiality for patients and monitoring of users without compromising patient care and population reporting. This analysis supports the idea that many diagnoses (not just the HIV status diagnosis) should be considered when providing or restricting access--indeed any and all medical conditions and service categories have the potential for requiring enhanced patient confidentiality. A provider treating a patient needs to be fully aware of the patient's medical history and current conditions--confidentiality policies should not restrict that appropriate access.

iSanté has a number of features in support of user authentication and confidentiality that are discussed in the next section. This proposal expands iSanté confidentiality features via:

1. User profiles
2. Application views based upon user profiles
3. Access reporting and alerts

Each of these is discussed below.

# Existing Patient Privacy and iSanté Authentication and Confidentiality Features

iSanté has always restricted access to authorized users. It uses LDAP (Lightweight Directory Access Protocol) to keep track of authorized users and to authenticate users via a password. The procedure manual for administering users in iSanté, Maintaining iSanté User Accounts, is provided separately. It contains detailed information on how to add, delete, and set access permissions for iSanté users. Its Appendix B (Haiti National Electronic Medical Record Privacy Protections for Patient Data) contains the following two sections on manual protocols relevant to the proposed access reports and alerts discussed later in this document:

Current Protocols for Managing User Access

1. Anyone with a username and password must ALWAYS be properly authorized to access patients at ONLY the site(s) where they work.
2. Only one person per clinic site should have Administrator access and therefore the ability to grant access to other users. This person must understand the 5 types of access privilege, which type of personnel require access to the EMR system, and the appropriate type of access privilege based upon personnel roles. In sum, this person must understand that they are responsible for granting access appropriately. This person must also sign a non-disclosure agreement and must adhere to it.
3. No site administrator and no site personnel should have access to more than one site, unless they perform work at more than one site.  This can easily be audited and the offending accesses removed. This type of auditing should be an ongoing monthly function of the CDC Regional Information Officers.
4. Users no longer using the system or not associated with specific sites or functions should be removed. This should be part of the regular monthly audit of user access.
5. The CDC Regional Information Officers (RIOs) should have access to only the sites within the region they serve, not all sites in the system. This should be part of the regular monthly audit of user access.

Other Current Protocols to Protect Patient Privacy

1. All users of the EMR system should sign a formal non-disclosure agreement. A draft agreement exists, and should be validated by the Ministry of Health. The signed forms should be kept in employee files at each clinic sites. Audit of the proper filing of the signed agreements should take place on an annual basis.
2. All users should lose their access and be considered for other disciplinary action, including termination of their job, if they violate the non-disclosure agreement.
3. All users should receive training on principles of confidentiality and the ethical and legal responsibilities involved in working with patient data.
4. In general, the production system (« live » EMR system) should not be used to train new users, unless training is done in conjunction with a site implementation. This will prevent trainees from seeing patient data from sites where they have no affiliation or authorization to view patient data.
5. If users must participate in a « task force » to assist other sites with catching up on backlog of data entry, they should be given temporary access to the new site. The Administrator should add authorization for the user at the new site at the beginning of the « task force » and then delete the authorization as soon as the « task force » completes its work.
6. Users with authorization for more than one site should pay strong attention to which site is currently selected from the drop down list. Users must be very careful to avoid entering patient data to the wrong site. If this happens, it means that patient’s records would be visible to authorized personnel at the wrong site, and the record would not be retrievable at the correct site.

In addition to the above, all users should follow the following standard operating procedures:

1. Never share accounts/passwords
2. Log out and exit from all browser windows after use
3. Lock computer when leaving it for even a short period of time (iSanté is considering an enhancement that would automatically log the user out after a specified period of time if the application is not used.)
4. Access only records that pertain to your work
5. Be aware that access is monitored

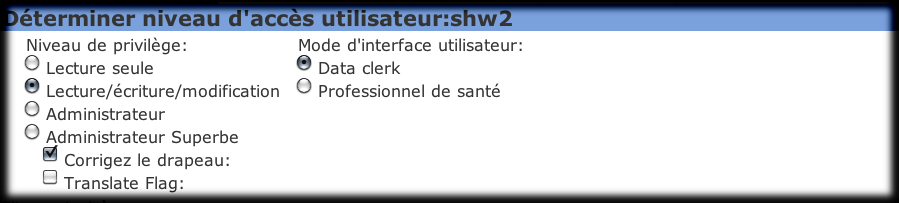
# 

# 

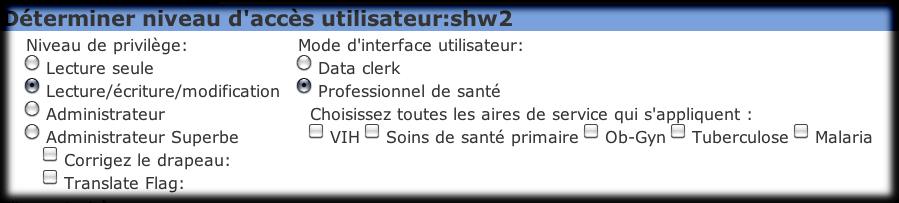
# Proposed New Features To Support Confidentiality

## User Profiles

The "user profile" refers to a characterization of the iSanté user both in terms of their duties (i.e. data entry person, provider, or administrator) and in terms of their "right" or "ability" to access a patient depending upon their diagnoses, the service area in which they are seen, the specifics of their treatment or other criteria. In general, a user need only see a patient's detailed, specific information if they provide services for that patient. Here is the current iSanté page used to specify the user access:



Registration and data clerks typically need to search for specific patients and enter specific patient encounter information into the system. Health care providers, on the other hand, need full view of all their patients' information. I-TECH proposes to modify iSanté to specify access by service area for providers as shown below:



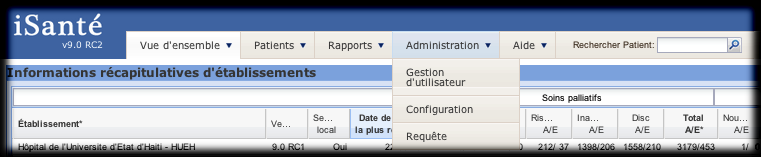
(The specific service areas listed above are estimates based on the current understanding of present and future system requirements.) The privileges, user interface mode, and service areas selected determine the iSanté elements (fields, menus, reports) that would be available to the user, as discussed in the next section. Additional criteria (patient status, patient diagnosis, etc.) can also be used for determining access, but might make access rules more confusing or complicated to be worthwhile. More sophisticated criteria could be developed later should the need arise.

## 

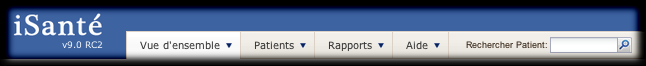
## 

## Profile-based iSanté Web Application Elements

The user profile described above can be used to determine access to iSanté elements. One existing example of using user profiles in this way is that users who are administrators have an administrator menu in iSanté:



While non-administrators do not:

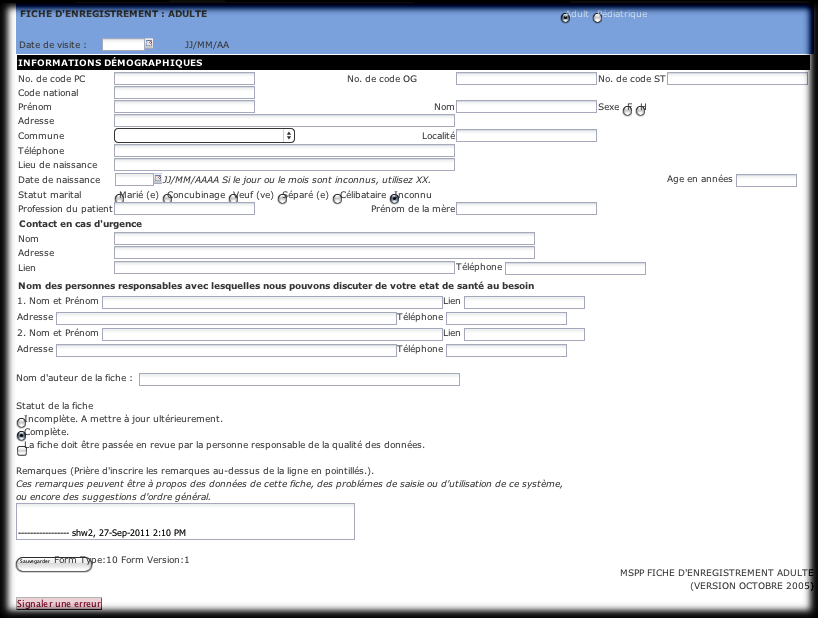


In the more robust profile I-TECH proposes, user access to iSanté elements will be further refined. For instance, users whose profile includes the areas of VIH and primary care could see the menus and reports relevant to those areas.

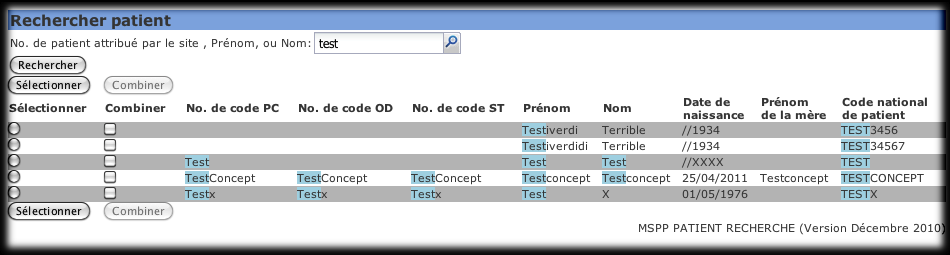
The accompanying document, Current iSanté Element-Service Area Matrix, indicates which iSanté application elements are associated with which service areas and will be the initial basis for determining access under this proposal.

It is important to note that the proposal (as indicated in the matrix) does not restrict patient search and registration-related iSanté elements by service area. To do so would invite duplicate registrations and other errors related to mis-identification of patients. For example, a patient registered in iSanté as a primary care patient should not be re-registered if making an initial ob-gyn or HIV visit, but instead should be discovered during search and have the appropriate service identifier added to their registration information along with any specific new encounter information.

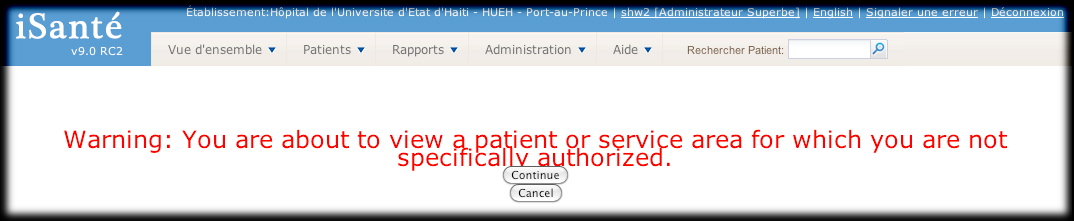
As mentioned in the first section above, all users must pledge to maintain the confidentiality of all patients, regardless of service area. Users with search and registration duties can be monitored for compliance with this policy (this is discussed further in the Alerting and Monitoring section below). The current iSanté patient registration form is common to all service areas and includes fields for entry of ST-IDs (HIV) PC-IDs (primary care), and OB-IDs (ob-gyn):



Correspondingly, users may search on name or via service area ID. A proper search should not exclude based upon service area, so search results return all matching IDs together with additional demographic information to aid with identification, as shown in the search result below:



In the example search result above, two of the found patients have IDs assigned from the primary care, ob-gyn, and VIH service areas. The usual purpose of a search is to find a patient and view their records. If the user wishes to view a patient who has been seen in a service area for which they are not authorized, they will receive an alert before proceeding, similar to this:



Alerts are discussed further in the following section.

## Access Reporting and Alerts

Since iSanté is a web application, every user/URL access is logged. This logged information can provide extensive audit information about access. In addition, since iSanté associates the user with the patient that is viewed and the encounter that is saved, it is possible to generate reports and assess and categorize time spent.

I-TECH proposes to add the following reports, which can be used to analyze access:

* User Access by Privilege
* User Access by Service Area
* User Access by Site
* Last User Access by date
* Users Who Haven't Logged On In the Last X days
* Users With Access to More than One Site
* Users Viewing Patients Not In Their Assigned Service Areas
* Number of Accesses per day, per week, per month, by user
* Forms entered per day, per week, per month, by user

As mentioned above, interactive alerting can take advantage of the user's profile information to warn about accesses outside their assigned service areas. For instance, suppose a provider assigned only to primary care is treating a patient who is HIV-positive. It is pertinent for that provider to view all of the patient's encounters related to HIV care, but probably not appropriate for the provider to create or modify a HIV encounter. The system can warn the user in this situation. Alerts could be implemented in iSanté for the following situations:

* About to view a patient who has previously been seen in service areas not in the user's profile
* About to view a form for a service area to which the user is not assigned
* About to save (or about to update) an encounter not in the user's profile

An example warning screen is shown below: