# SECURING PATIENTS MEDICAL RECORDS

A Major Hospital Complex Protects its Thin Client farms running Citrix™

**This hospital complex is specialised in psychiatry and has 1,200 employees. The Information System comprises 45 Windows servers, SANs, two AD directories, 20 Citrix™ servers and several hundred Wyse thin terminals. The request came from the doctors themselves: they wanted to secure their patients' medical records beyond the level provided by law.**
***«The law states that only holders of a health professional card can access this data. However, this only protects access to the data and does not directly protect the data itself»,*** **the IT Manager explained. The hospital wanted to go further in this area and also protect against data theft and leaks. From the point of view of the architecture, the Hospital's networks are already partitioned, separating administrative and medical data. The network isolates data within the hospital according to the role of each employee. Therefore, all that remains is the protection of the data itself and this encryption is the only solution.**

## ZONECENTRAL

## Requirements

**« Multi-user Citrix™ based encryption and encryption procedures are as close as possible** to each profession to protect medical records » this statement summarises the Hospital's requirements for which performance and workload requirements are critical on its servers.
Indeed, the new Information System is based on thin and compact clients (Citrix clients) installed all over the hospital very close to Doctors and Nurses right down to operating rooms. These terminals have a smartcard reader to authenticate caregivers and give them access to patients' confidential records. The entire workload therefore relies on Citrix™ server farms that host the user sessions simultaneously.
These sessions, although running on the same servers, must enable the information to be cryptographically partitioned based on each user of each session, regardless of the resource accessed and including the SAN arrays.

## Solution

*«Single-user encryption worked well, but multi-user access to shared data posed problems with all off-the-shelf products. Yet this was essential criterion for us»*, the IT Manager explained. Then he discovered **ZoneCentral** from Prim'X and his team found that the product perfectly met their multiuser encryption requirements.
**ZoneCentral** is compatible with the Citrix™ architecture : « *The solution has proven to be perfectly stable despite* **scalability peaks of up to 120 simultaneous users in the same encryption zone** », the IS director said, « *We were afraid that the encryption load would be very heavy but in fact the* **impact on server resources is quite low** ».

## Experience

The hospital complex has implemented a series of procedures to ensure all functions are separated across the entire encryption chain.
« *The IT director manages the certificates required for encryption and the medical department manages the users who will have to encrypt the data. The two parties are independent. As an IT manager, I have access to encryption zones to maintain them but I don't have access to the encrypted data they contain*», said the IT director.
**Recovery**, a crucial step in encryption, **is also very closely controlled**. No administrator can decrypt their users' data by themselves. For this, it is necessary to involve the IT department (to access recovery data), the medical department (which holds the PIN code of the recovery card) and Management (which holds the card but not the code).

## Benefits

Not only can the hospital comply with the obligation to control access to medical data, but it can also go further by securing this data through perfect role separation and strong encryption. The data is only accessible to staff authorised to consult it, and they have total control in its handling.