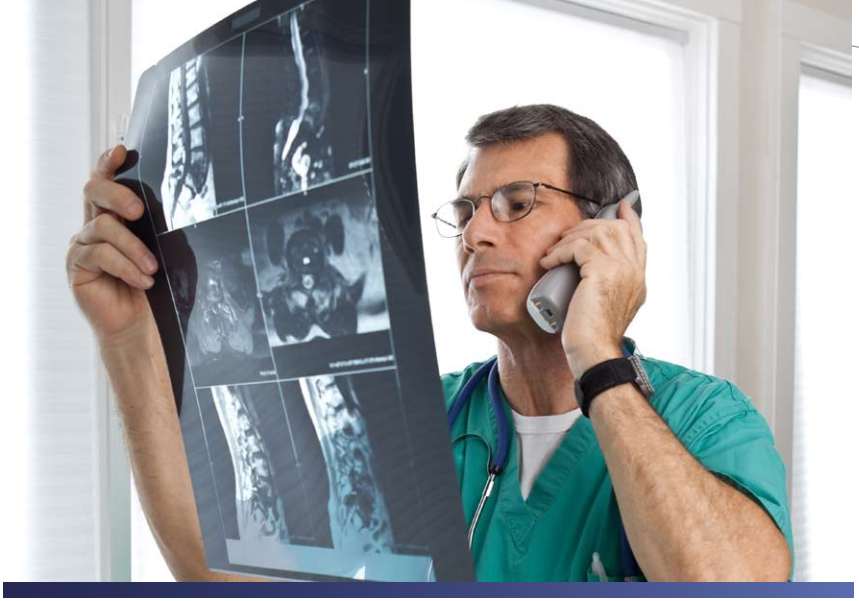
UCOPIA
COMMUNICATIONS

UCOPIA FOR HOSPITALS AND HEALTHCARE INSTITUTIONS

www.ucopia.com

OUR WEB PORTAL, A SECURE WAY TO SHARE YOUR NETWORK

- Secure access to medical records and prescriptions made at the patient's bedside
- Internet access for patients and visitors
- Sharing a multi-service wired and wireless
- IP infrastructure (voice, video and data)
- Legal obligations (patient confidentiality, EU directive)



MOBILITY OF HEALTHCARE STAFF AND PATIENT SERVICES

The healthcare institution must meet needs while taking a number of constraints into account:

- **Access to medical applications** (patient file, prescription records) and mobility of healthcare staff
- **Internet access for visitors** - patients, suppliers, doctors, etc...
- **Mobility of administrative staff** (meal management)
- **Sharing of wired and wireless multi-service communication infrastructure** supporting healthcare applications, voice, video, GPS
- **Security for users and the data** carried over the network (confidentiality, traceability and access control)
- **Integration with legacy solutions and architecture** – wired networks, directories, VLAN...
- **Legal obligations:** institutions are obliged in France and across Europe to retain connection data from 6 to 24 months in Europe (EU directive 2006/24/EC).

UCOPIA, MEETING THE NEEDS OF HEALTHCARE INSTITUTIONS

Improving health services and efficiency leads to the roll-out of technical resources (Wi-Fi, bedside multimedia terminals, etc.) giving healthcare staff access to medical records and applications for prescribing treatments at the patient's bedside.

• Patient services: ease and simplicity

Thanks to the UCOPIA user account creation tool and patient authentication by Web portal, **accommodating patients on the network is straightforward and no burden.**
It is easy to:
- Provide a password
- Define access rights (internet, email, printer)
- Define connection conditions (e.g. a one-hour credit in a restroom).
- Provide a ticket containing all the information needed to connect
- Let visitors register themselves over the internet and immediately send them a password by text message to their mobile phone.
- Automatically cancel the patient's rights on departure.

All this can be accomplished by an individual with no network skills (receptionist, administrative staff).

• UCOPIA meets legal security and traceability requirements
(EU directive 2006/24/EC)

With its mechanisms for authentication, control, data filtering and logging in an SQL database, **UCOPIA ensures the security of the network and users, and the traceability of connections.** UCOPIA stores a historical log of connections (who did what and when), an essential feature in response to the requirements of anti-terrorism legislation, formally adopted in France in March 2006, and to be in force across the European Union by 2009 at the latest.

• The healthcare institution decides on the business model

With UCOPIA, the healthcare institution can make access free or paid for depending on where the connection is made (reception, wards, waiting rooms, staff offices, etc.).
The institution may decide to make access free in the wards, and charge for it in waiting rooms.

• Security levels appropriate to user population categories

UCOPIA incorporates a full, robust set of security mechanisms (strong authentication based on passwords, certificates, CPS cards (healthcare professional authentication) and allows security profiles appropriate to various groups (healthcare and administrative staff, patients) to be defined.
The authentication method can be customised for each group, as can the access rights to network resources and applications. UCOPIA dynamically manages VLANs: A doctor's data can simply be redirected to his or her unit's VLAN while patient traffic is partitioned on a patient VLAN.unité de soin tandis que le trafic des patients sera isolé sur un VLAN Patients.

• Straightforward and centralised administration

UCOPIA offers a set of centralised administration tools that can be used to manage security policies and roaming profiles as well as the Wi-Fi infrastructure. Administrators can allow doctors to log in to their hospital's various sites and access the same services, irrespective of their location.

• Stronger security on the wired network

UCOPIA can also handle wired connections, for self-service workstations, for instance, with authentication, access control, roaming, etc.
The wired and wireless network environment thus becomes more secure and comfortable for users.

120 MORE THAN **INSTITUTIONS**
EQUIPPED IN 2010

OUR BEST REFERENCES IN 2010:

ORPEA, Capio, SSA Cetima, Résidences Noble Age, MIPIH, CH Robert Ballanger (AP-HP), CH Mulhouse, Hôpital Erasme Bruxelles ...

TESTIMONIAL FROM LIBOURNE HOSPITAL (33)

The Hospital of Libourne has chosen the UCOPIA solution to secure access to its network. «The deployment of mobile access for health care professionals working at the hospital is a success and a secure Wi-Fi access service for all patients will be deployed very soon within our hospitals. For Libourne Hospital, the outcome is now extremely positive.»

Frédéric Dubrana,
IT Manager for Libourne Hospital.

CREDITS PHOTO: FOTOLIA - GRAPHIC DESIGN: CLAIRE TAGLIAFERRI - TEL.: +33(0)6 80 14 10 00

UCOPIA Communications - 201, Avenue Pierre Brossolette 92120 - MONTROUGE - FRANCE
Tél. : + 33 (0) 1 40 92 73 90 - Fax : + 33 (0) 1 40 92 73 99 Email : contactus@ucopia.com - www.ucopia.com