

Inside the IT Department

What happens in the IT department?

The hospital IT department plans, builds, and runs clinical and administrative information systems. It secures networks and data, ensures interoperability, supports users, and steers projects with biomedical engineering and clinical leadership. In France, practices align with the ANS doctrines [1, 2], ANSSI cybersecurity guidance [3] and GDPR [4].

Main service lines

User services. 24/7 helpdesk, on-site support, endpoint lifecycle, identity and access management (IAM) with role-based access.

Clinical applications. Electronic health record, computerized physician order entry (CPOE) / electronic medication administration records (eMAR), LIS, RIS / PACS archiving, oncology information systems (OIS) for radiotherapy, perioperative and ICU systems, appointment and bed management, telemedicine [2].

Administrative/finance. HR and payroll, ERP for procurement and stocks, revenue cycle, reporting and BI.

Integration. Service interfaces, API gateways, master patient index using *Identité Nationale de Santé* (INS), document exchange via *Mon Espace Santé* [2].

Infrastructure and tooling

Network. Segmented LAN/Wi-Fi, NAC, VPN, segregation of medical devices networks, QoS.

Compute & storage. On-prem clusters, backups, selected cloud providers with HDS or SecNum-Cloud compliance [5].

Security stack. Centralized logging / SIEM, EDR, anti-malware, MDM, PAM for admins, secrets vault, email security, vulnerability scanning and patch management, data loss prevention per risk.

Observability. Monitoring of infrastructure, applications, and integrations; synthetic probes for critical workflows; capacity and SLA dashboards.

Data protection, cybersecurity, and compliance

GDPR. Legal bases, consent where needed, DPO oversight, DPIA for high-risk processing, rights management, records of processing [4].

Security baseline. Risk analysis, policy and minimum configurations, incident response, backups tested offline, phishing drills, business continuity and disaster recovery plans [3].

Health data hosting. For outsourced or cloud services, HDS certification is required; contracts include sovereignty, audit, logging, and exit plans.

Team and interfaces

The IT department runs on predefined roles, on-call rotas, briefings, change control, and incident response playbooks. ANSSI hygiene guides, HDS and GDPR requirements, and ANS interoperability rules reduce operational risk and strengthen cross-department communication; they are mandatory anchors in French hospital quality and security programs.

References

- [1] Agence du Numérique en Santé (ANS). *Fondements de la doctrine du numérique en santé*. <https://esante.gouv.fr/doctrine/fondements>.
- [2] Agence du Numérique en Santé (ANS). *Espace de publication CI-SIS*. <https://esante.gouv.fr/offres-services/ci-sis/espace-publication>.
- [3] Agence nationale de la sécurité des systèmes d'information (ANSSI). *Guide d'hygiène informatique*. https://cyber.gouv.fr/sites/default/files/2017/01/guide_hygiene_informatique_anssi.pdf.
- [4] *General Data Protection Regulation*. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [5] *Articles L1111-1 à L1111-9 du Code de la santé publique*. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006185255/2025-07-01.