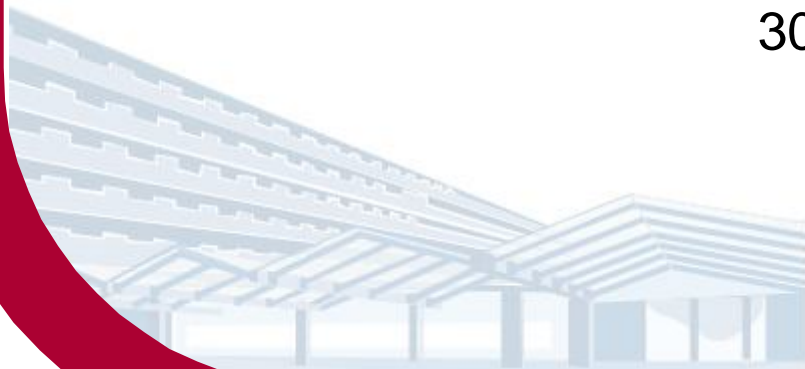


L'informatique pour soigner les patients : sa permanence

Dr. B. Debande
Cliniques universitaires Saint Luc

30/03/2010



CLINIQUES UNIVERSITAIRES SAINT-LUC



D'où venons-nous

- 20 ans d'évolution de l'informatique hospitalière
 - Backoffice
 - ADT, facturation, compta
 - médico-technique lourd (Labo, Radio)
 - Support de processus hospitaliers de plus en plus critiques
 - Agenda de consultation
 - Quartier opératoire
 - Gestion des lits en ligne
 - Prise en charge du patient aux urgences
 - Intégration des flux de données entre nombreuses applications

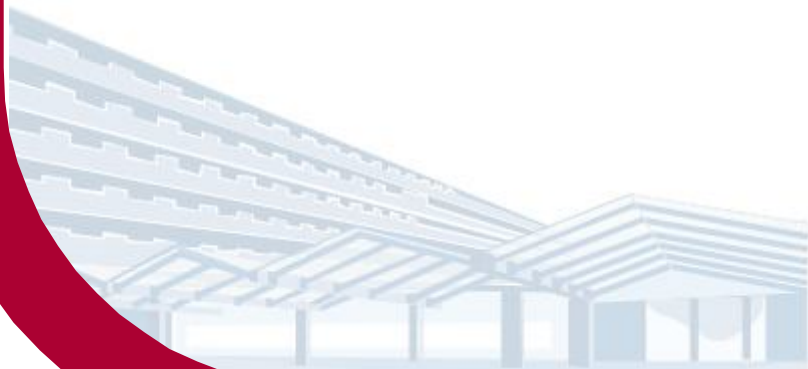
- Support des soins aux patients
 - Prescription et circuit du médicament
 - Protocolage anesthésie
 - Gestion totale des soins intensifs
 - Dossier patient informatisé et passage au paperless
- Convergence IP au niveau du réseau
 - Téléphonie IP
 - Vidéo (télé-conférence, surveillance, ...)
 - Monitoring
 - Dispositifs mobiles

Il faut se poser la questions de la permanence de l'informatique



Permanence de l'information

Permanence du service



Permanence de l'information

- Data ou information ?
 - quid de l'utilisation à long terme
 - loi : 30 ans après dernier contact
 - format des données et logiciel pour les lire
 - « reprise » lors du changement de logiciel
- Fournisseur
 - Belgique = petit pays
 - Acteurs locaux dans un trop petit marché : viabilité

→ Pas d'assurance sur la pérennité

→ Obligation d'assurer un archivage « lisible »

→ Certification des logiciels « soignants »

Permanence du service

Informatique devenue critique aussi pour le « core business » de l'hôpital : les soins au patient

Impact sur tous les métiers autour du patient : médical, paramédical, autres

Si l'informatique s'arrête, l'hôpital s'arrête

Comme l'hôpital ne peut pas s'arrêter, le service informatique doit se débrouiller pour garantir le fonctionnement 24/7



L'informatique devrait donc être
infaillible

Mais nous savons tous qu'elle ne l'est
pas.....



Les « pannes » informatiques

- Panne
 - Machines individuellement fiables, mais complexité croissante nécessite un ensemble d'éléments --> danger du maillon faible
 - Réseau : perte d'un élément = partie de l'arborescence coupée = zone « down »
- Désastre
 - Phénomène naturel, incendie, vandalisme...
 - Réseau: points critiques peuvent tout bloquer

→ Disposer de « backups » n'est plus suffisant (durée de récupération des données)

→ L'objectif ultime = 99,999 % de disponibilité (= 4 heures max de panne par an)

Les « dysfonctionnements » informatiques

- Corruption logique (tout fonctionne et rien ne va plus)
 - Tempêtes sur le réseau
 - Corruptions de bases de données
 - Propagation d'erreurs dans une informatique intégrée
 - Mises à jour ratées (postes, programmes, serveurs)
 - Erreur humaine dans environnement complexe (réseau, machines)
- Virus
 - Mécanisme de « reproduction » toxiques pour un univers clos

- Prévention beaucoup plus difficile
- Moyens des hôpitaux limités (tests, maîtrise du parc...)
- Pour l'utilisateur, ce sont aussi des pannes

99,999% (~= 4h/an)
dysfonctionnements malheureusement
inévitables

Le risque 0 n'existe donc pas...
... mais sans information je ne peux plus
soigner mes patients !



Responsabilité commune

Chacun des acteurs doit apporter sa contribution

Informatique : tout faire pour assurer une disponibilité des applications

Soignants : vivre avec la possibilité d'une panne et s'y préparer pour « survivre »

Assurer une disponibilité

- Mesures classiques
 - Redondance, clustering, virtualisation, 24x7, salle backup
 - Applications critiques ?
 - Viser une fiabilité technique maximale (en fonction de nos moyens : 0,0001% = €€€€€€€)
- Expertise interne qui fait la différence
 - Diagnostic d'un dysfonctionnement dans des systèmes complexes
 - Peu d'espoir d'aide externe dans les système fortement interconnectés et intégrés
 - Esprit « hospitalier » des informaticiens in-house
 - Tout cela avec trop peu de « manpower » au vu de l'évolution des techniques

Assurer une disponibilité

- Interaction capitale avec les « soignants »
 - Problématique différente de la facturation
 - S'ouvrir à un autre monde, sortir de sa cave, mesurer les enjeux de son client interne
 - Préparer la communication, avoir des relais en cas de problème

La disponibilité est une question de moyens et d'hommes pour les mettre en œuvre

Ne faudrait-il pas songer à regrouper les (rares) ressources humaines informatiques des hopitaux ?

Fonctionner sans informatique

business continuity plan (BCP):
soigner sans outil informatique

Quels sont les processus réellement critiques ?

Capital = faire des choix

Probabilité faible des pannes = se focaliser sur l'essentiel

Survivre à une panne : une heure – ½ journée – 1 jour

Que mettre en œuvre pour resynchroniser le système

Rester raisonnable : en situation de crise, les moyens humains sont critiques et affectés à la continuité du service

- **Qui doit se préoccuper du BCP**
 - Question posée au management (souvent question du CA qui entrevoit surtout la « perte d'exploitation »)
 - Réfléchie et mise en œuvre par les acteurs de terrain
 - Leadership « soignant », informatique en support
 - La conclusion ne peut pas être : stop à l'informatisation
- **Comment se lancer dans un BCP**
 - Profiter des pannes, même mineures, pour sensibiliser
 - Economies liées à l'informatisation (...) → investissement humain en coordination BCP (lié à sécurité ?)
 - Méthodologies existent, se documenter, former un référent
 - Ne pas accepter « l'informatique n'a qu'à s'arranger pour que cela fonctionne tout le temps »

En réalité

- Disponibilité informatique
 - coûte cher → balance avec autres besoins
 - travail peu visible → peu valorisé/valorisant
 - évolution technologies aide
 - globalement prise de conscience et actions dans ce sens

en fait-on assez ? trop ? → prendre conseil



En réalité

- Plan de continuité
 - Qui s'en préoccupe vraiment ?
 - travail peu visible → peu valorisé/valorisant
 - Trop souvent « en plus du reste », pas dans les priorités
 - Trop de travail, pas assez de personnel
 - Un vrai projet à mettre en place

leadership « soignant » indispensable

Et ma responsabilité de soignant ?

Question difficile... Pas encore de jurisprudence

Par analogie à l'électricité : prouver que l'on a mis tout en œuvre pour minimiser le risque suite à la panne

Mise en place de moyens techniques adéquats (informatique)

Procédures en cas de panne définies et connues (soignant)

Attitude prudente pendant la panne

Se limiter aux interventions strictement nécessaires

Ne pas oublier qu'il nous reste quelques neurones

Quel que soit le niveau d'information fourni par des machines, c'est le prestataire de soins qui finalement reste responsable vis-à-vis du patient

Faut-il leur dire tout cela ?

Risque de ruiner les efforts passés à gérer le changement vers l'informatisation....

Mais la disponibilité des systèmes est une des angoisses générées par ce changement

Question de style de management, de leadership

En parler permet d'objectiver le problème, montrer que l'on s'en préoccupe, qu'il s'agit d'une responsabilité partagée entre la technique et les soignants

Agir en conséquence joindre l'action à la parole...

Conclusions

- L'informatique est omniprésente en ce compris dans les activités de soins : pas de retour en arrière possible
- La disponibilité totale de l'outil informatique n'existera probablement jamais : + fiable mais + complexe et pilotée par des hommes
- Data <> information : important de garantir un accès à l'information à long terme
- Ensemble, informaticiens et soignants, chacun à son niveau et avec ses moyens, doit contribuer à assurer la continuité du business
- En étant transparent sur les risques et les enjeux, mettre en œuvre un vrai projet BCP d'abord pour assurer une continuité des soins au patient