Système de l’information au LBM et accréditation ISO 15189 version 2012

Partie 2

Didier CHAMARD*

Biologistes LBM ISIBIO (01)

** Le formateur déclare ne pas avoir de conflits d’intérêt avec d’autres sociétés*

PLAN DE LA JOURNEE

A.Généralités sur le S.I - Définitions - Référentiels et documents de travail - S.I vs 15189

B.Réseaux - Sécurité

C.Architectures réseaux d'un LBM - Hébergements données de santé

D.Aspects pratiques SI vs 15189

Généralités sur les réseaux informatiques

Sécurité informatique

LBM ISIBIO (01)

Glossaire

ADSL : **Asymmetric** Digital Subscriber Line : technique de communication numérique sur ligne téléphonique, mise en œuvre par les fournisseurs d'accès à internet. Comme son nom l'indique, la technologie ADSL fournit un débit asymétrique. Le flux de données est plus important dans un sens de transmission que dans l'autre. Contrairement à la technologie SDSL.

ASIP Santé : Agence des Systèmes d'Information Partagée de Santé

CDA : Clinical Document Architecture (CDA) est le standard de document médical électronique structuré produit par HL7.

DMZ : une zone démilitarisée (ou DMZ, de l'anglais demilitarized zone) est un sous-réseau séparé du réseau local et isolé de celui-ci et d'Internet par un pare-feu. Ce sous-réseau contient les machines étant susceptibles d'être accédées depuis Internet.

HL7 : Health Level Seven (HL7) est une organisation internationale produisant des standards d'interopérabilité pour le domaine de la santé.

LOINC : Logical Observation Names and Codes est une nomenclature internationale, permettant la codification des résultats d'examens, notamment ceux de biologie médicale, pour les échanges de ces résultats sous forme dématérialisée, entre systèmes d'information. La licence d'utilisation de LOINC est gratuite. LOINC traduite en français est mise en accès public par l'ASIP Santé.

MPLS : MultiProtocol Label Switching (MPLS) est un mécanisme de transport de données basé sur la commutation d'étiquettes ou « labels".

MW : système middleware de gestion du plateau technique ou d'un sous-ensemble de celui-ci, et/ou d'un ensemble d'analyseurs délocalisés dans les unités de soins.

SDSL : Symmetric Digital Subscriber Line. la ligne SDSL a, contrairement à la ligne ADSL, des débits symétriques : son débit en réception (download) est égal au débit en émission (upload).

SISP : Système d'Information de Santé Partagé entre le laboratoire et d'autres organisations ou professionnels de santé. Un serveur de résultats de biologie entre dans cette catégorie. Le DMP est un SISP de portée nationale.

TCP/IP : Protocole des couches liaison, réseau et transport sur lequel s'appuient le réseau internet et la quasi-totalité des réseaux locaux.

VPN : le réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Il correspond en fait à une interconnexion de réseaux locaux via une technique de « tunnel ».

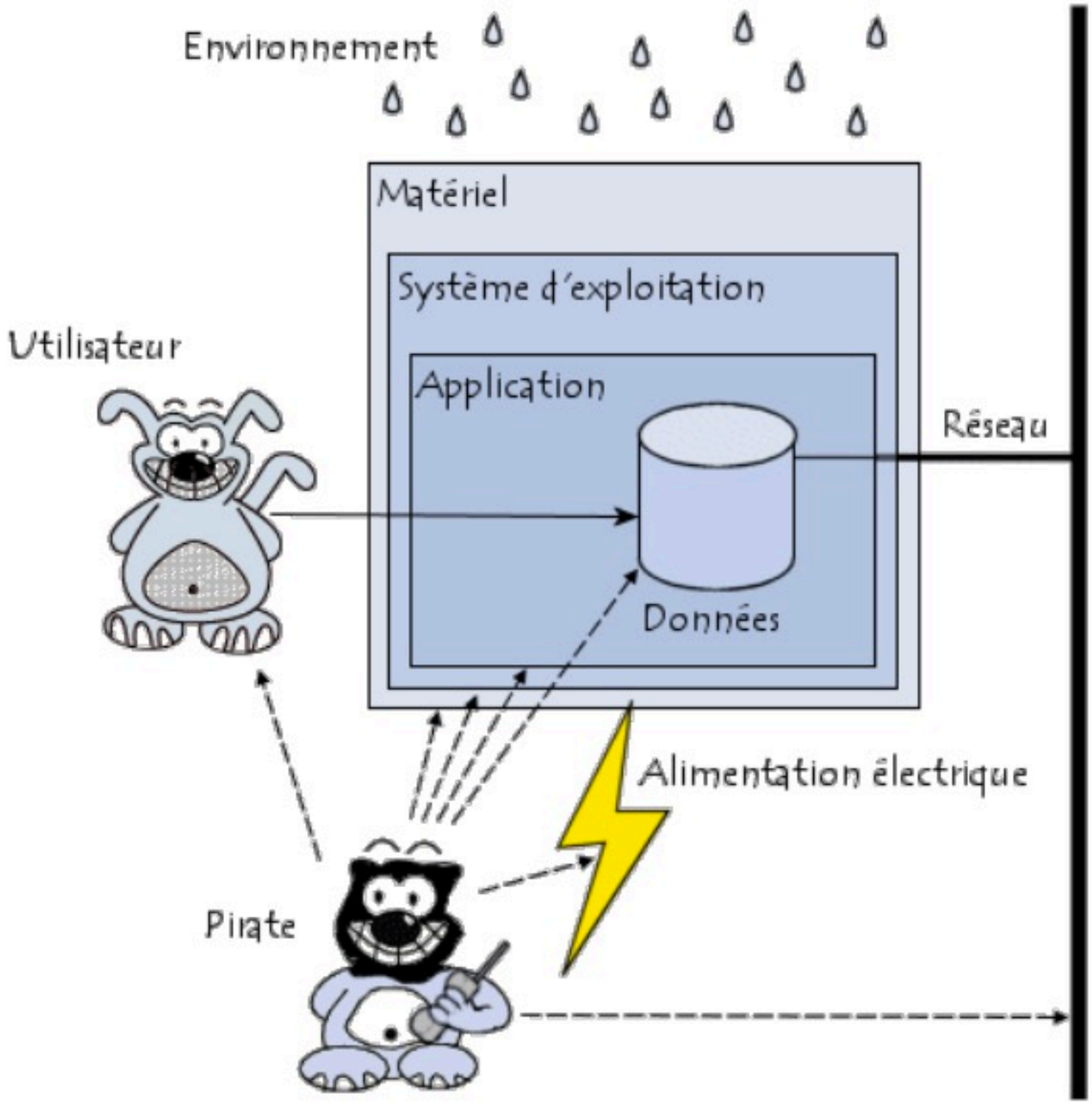
Plan du chapitre

a. Attaques et moyens de défense réseau

b. Cryptographie et signature électronique

c. Réseau & hébergements données de santé - DMP

a. Attaques réseau



Source : JF PILLOU commentçamarche.net 2015

Méthodes utilisées pour les attaques

- Négligence utilisateurs : sessions ouvertes, accès permanent des hot-line SII dans les SIL, pas de changements des autorisations d'accès après départ d'un collaborateur
- Se faire passer pour un informaticien
- Mots de passe vulnérables «123456» …
- Ecoute réseau
- IP spoofing : prendre la même adresse IP qu'un poste donné d'une entreprise
- Injection de petits programmes (virus, cheval de Troie)
- Exploitation failles O.S
- Scan du système de protection de l'entreprise
- Repérage & intrusion réseaux Wi-Fi

Labio.fr piraté : demande de rançon et publication de résultats médicaux

Allo docteur, j'ai mal à ma sécurité 123

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « *des centaines* » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.

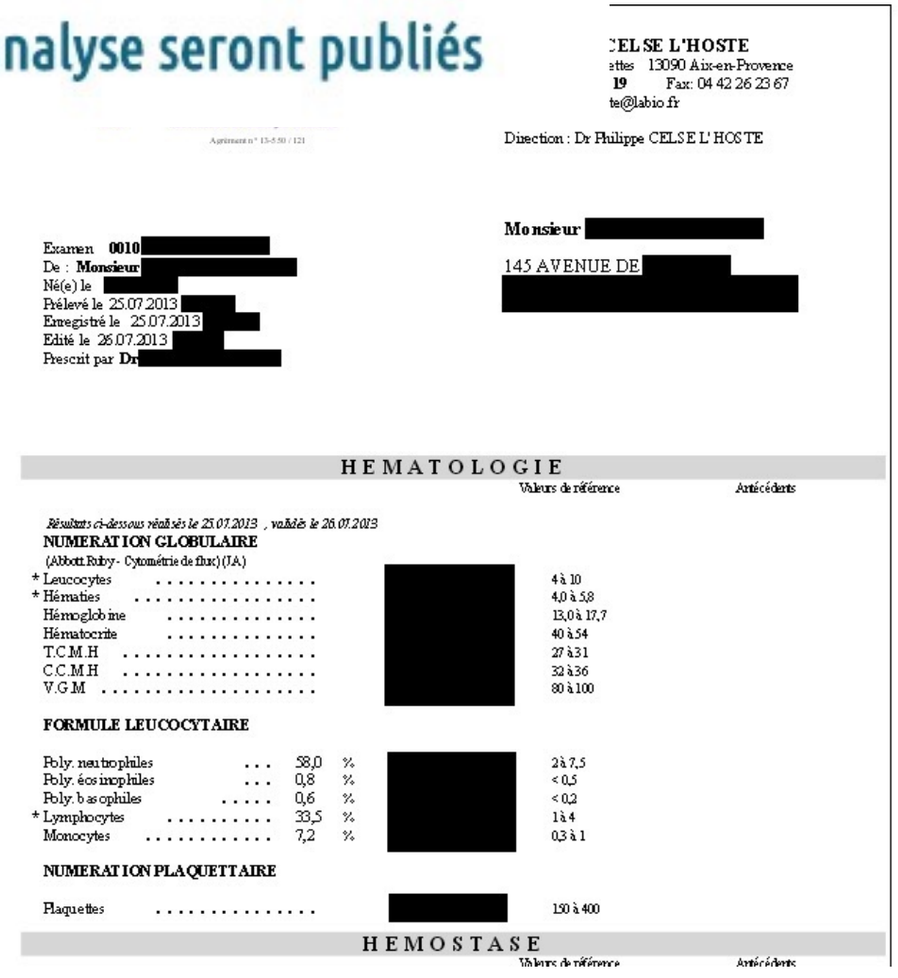
Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de SynoLocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle se refusait à céder aux demandes de son maitre chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données avaient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés

Le laboratoire LABIO communique après son piratage informatique

Posted On 22 avr 2015 By : Damien Bancal Comment: 0 Tag: communication, laboratoire, Rex Mundi

Il y a quelques semaines, les laboratoires LABIO ont été attaqués par le maître chanteur Rex Mundi. Ce groupe de pirates, via une technique d'interception de la base de données, a mis la main sur les identifiants de connexions. En échange de son silence, Rex Mundi a réclamé 20000. Les laboratoires n'ont pas payé. Les données ont été diffusées. Suite à cette attaque, LABIO, via son avocat, a communiqué sur ce sujet.



CELSE L'HOSTE
ettes 13090 Aix-en-Provence
19 Fax: 04 42 26 23 67
te@labio.fr

Direction : Dr Philippe CELSE L'HOSTE

Examen 0010[redacted]
De : Monsieur[redacted]
Né(e) le [redacted]
Prélevé le 25.07.2013[redacted]
Enregistré le 25.07.2013[redacted]
Edité le 26.07.2013[redacted]
Prescrit par Dr[redacted]

Monsieur [redacted]
145 AVENUE DE[redacted]

HEMATOLOGIE

	Valeurs de référence	Antécédents
Résultats ci-dessous réalisés le 25.07.2013 , validés le 26.07.2013		
NUMERATION GLOBULAIRE		
(Abbott Ruby - Cytométrie de flux) (JA.)		
* Leucocytes	4 à 10	
* Hématies	4,0 à 5,8	
Hémoglobine	13,0 à 17,7	
Hématocrite	40 à 54	
T.C.M.H	27 à 31	
C.C.M.H	32 à 36	
V.G.M	80 à 100	
FORMULE LEUCOCYTAIRE		
Poly. neutrophiles ... 58,0 %	2 à 7,5	
Poly. éosinophiles ... 0,8 %	< 0,5	
Poly. basophiles ..... 0,6 %	< 0,2	
* Lymphocytes ..... 33,5 %	1 à 4	
Monocytes ..... 7,2 %	0,3 à 1	
NUMERATION PLAQUETTAIRE		
Plaquettes	150 à 400	

HEMOSTASE

	Valeurs de référence	Antécédents

Prévention des attaques réseaux

(3 niveaux)

Indispensable

- disposer d'une bonne sauvegarde de toutes ses données
- faire un audit des portes inutilement ouvertes (modems installés à demeure, logiciels de transmissions permanentes…)
- lorsqu'ils existent, vérifier que les comptes d'administration ont des mots de passe sécurisés
- supprimer les comptes utilisateurs non utilisés (notamment à la suite de chaque départ)
- désactiver les services non utilisés sur les machines (serveur Internet par exemple)
- supprimer les partages de fichiers non nécessaires

Souhaitable

- mettre à jour systèmes et logiciels (serveurs et serveurs Web principalement) «Windows & Office update», maj navigateurs, logiciels de messagerie ...
- installer un FireWall & structurer les réseaux en zones étanches par activité et sensibilité(VLAN). Instituer un système de mots de passe.
- Bien isoler les serveurs Internet
- Interdire les **clés USB perso <=> charte du personnel**
- Limiter postes avec accès sur le web

Recommandable

- Auditer la sécurité globale du système (analyses des points faibles, tentative volontaires d'intrusion)
- Créer une zone tampon (DMZ)

Technologies de défenses

- Antivirus
- Pare-feu (Firewall)
- Antispyware
- Anti phishing
- *Sauvegarde (sera vue plus loin)*
- *VPN*
- *Cryptage des données*

VPN

VPN = Virtual Private Network :

- Chemin virtuel sécurisé entre une source et une destination
- Réseaux privés à moindre coût

Principe:

- Chaque extrémité est identifiée
- Transit des données après chiffrement

Applications au LBM :

- Accès via internet à l'intranet du LBM
- Accès sécurisés à l'intérieur d'un LBM (via intranet)

b. CRYPTOGRAPHIE

(transmission sécurisée des données)

Définitions:

- **Cryptographie**
  - science qui utilise les mathématiques (algorithme) pour chiffrer et déchiffrer des données
  - Pour stocker des informations sensibles ou les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu
- **Cryptanalyse**
  - La cryptanalyse est la science de l'analyse et du cassage des communications sécurisées
  - cryptanalystes = attaquants
- **Cryptologie**
  - cryptographie et cryptanalyse

(sources: Gérard Soula, LERTIM, Faculté de Médecine Marseille)

Schéma de la cryptographie

2 phases:

- Chiffrement = cryptage: dissimulation garantie d'un texte clair
- Déchiffrement = décryptage : retour au texte initial clair

Il existe plusieurs manières de crypter un document.

Le chiffrement asymétrique

- Appelé à clé publique parce que basé sur l'existence de deux ensembles
  - Les valeurs qui sont rendues publiques : clé publique
  - Les valeurs qui sont conservées privées par leur propriétaire : clé privée ou clé secréte

- Chaque partenaire d'un réseau possède un couple unique clé publique/clé privée

- Les clés publiques doivent être communiquées à l'ensemble des partenaires

Qu'est ce que la sécurisation des échanges électroniques ?

- **Authentification de l'émetteur et du destinataire:**
  - Quand l'auteur du message est le Dr Y, on doit être sur que le message vient bien du Docteur Y.
  - **Signature électronique**, **certificat**
- **Non répudiation :**
  - Si j'ai reçu le message du Dr Y, je ne doit pas pouvoir dire que je ne l'ai pas reçu
- **Intégrité :**
  - Le message ne doit pas pouvoir être modifié notamment par quelqu'un qui pourrait l'intercepter
- **Confidentialité :**
  - Le message ne doit être lisible que par son destinataire.

Source : vidéo « informatique médicale & FSE CHU Nancy

http://unf3s.cerimes.fr/media/paces/Lorraine/sesamvitale/index.html

Signature électronique *

(application cryptographie)

* *NPC avec signature scannée*

Clé privée

La clé secrète = clé de chiffrement = clé privée = clé unique

Il n'existe pas de passe-partout <=> impossible de chiffrer sans cette clé => Personne ne peut imiter la signature électronique

Clé publique

Pour lire le document crypté, le laboratoire remet une copie de sa clé de déchiffrement = clé publique

Une clé privée permet de calculer une clé publique, mais l'inverse est impossible.

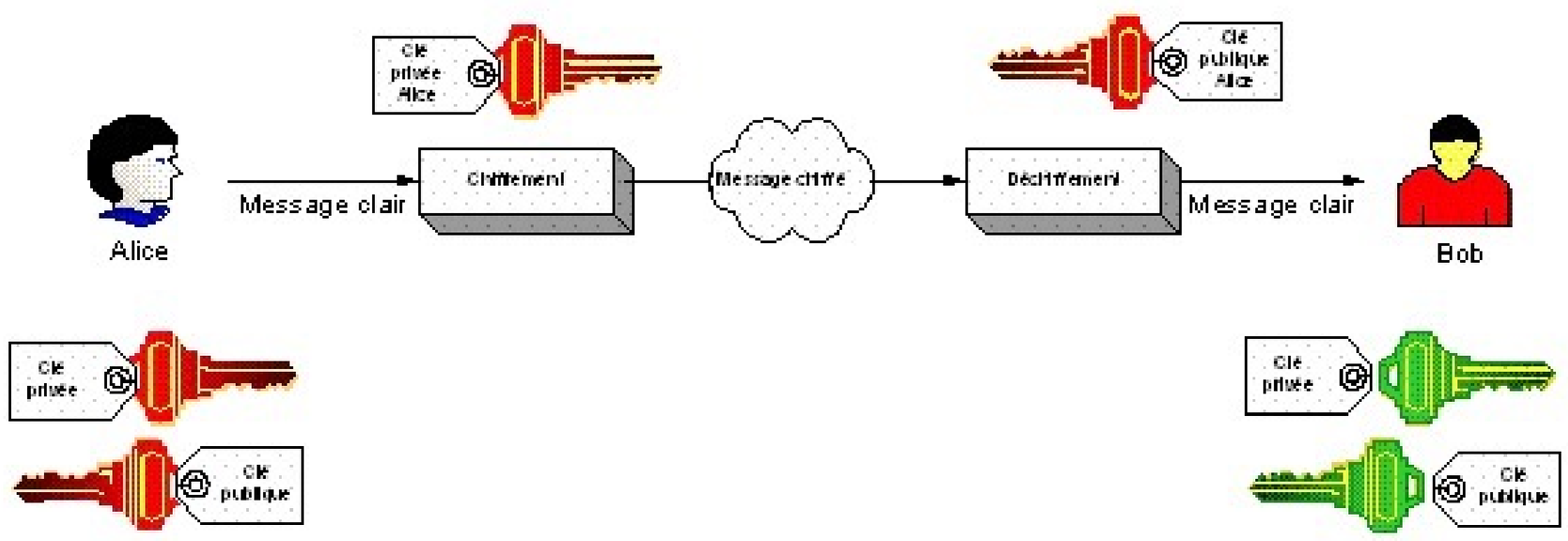


Figure 36 : Chiffrement asymétrique

http://www.sfil.asso.fr/les-dernieres-informations/95-pgssi-s

PLAN DE LA JOURNEE

A.Généralités sur le S.I - Définitions - Référentiels et documents de travail - S.I vs 15189

B.Réseaux - Sécurité

C.Architectures réseaux d'un LBM - Hébergements données de santé

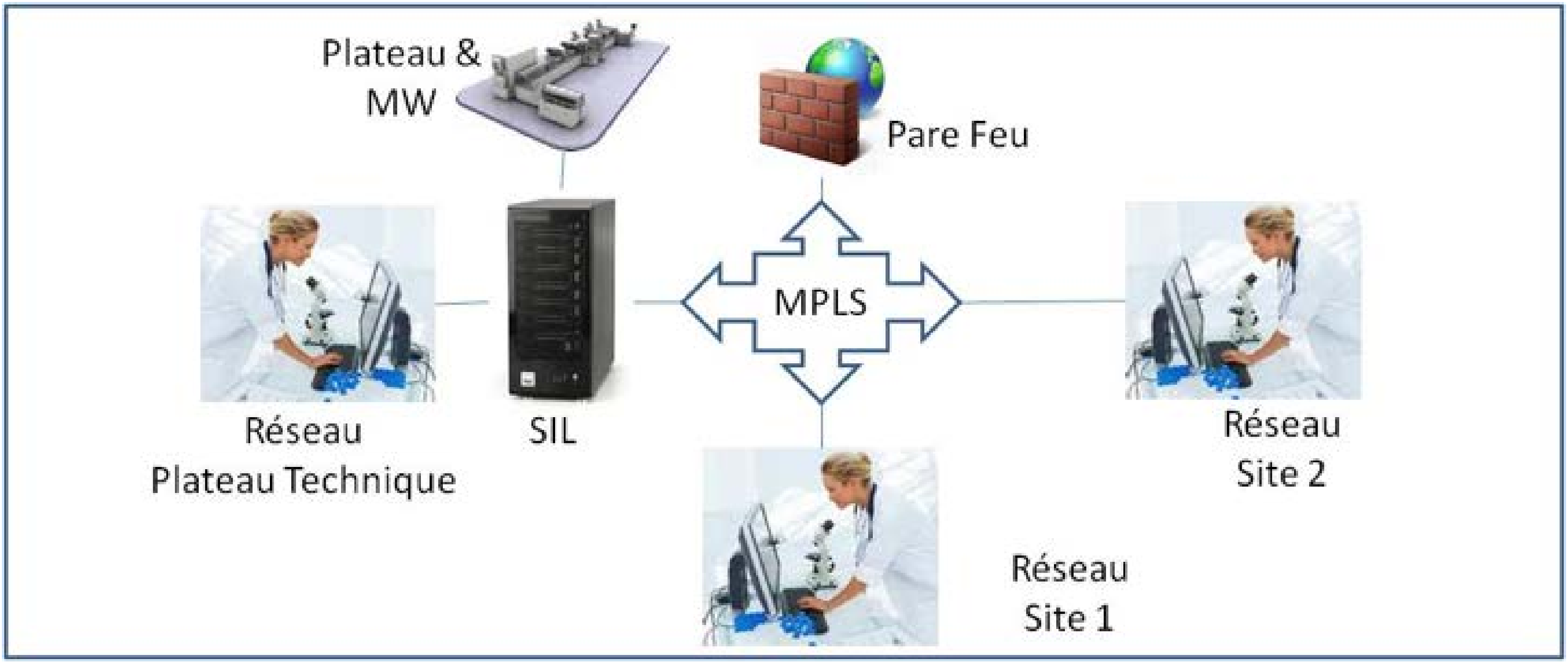
D.Aspects pratiques SI vs 15189

C. Problématiques architecture réseaux dans un LBM

Hébergement données de santé

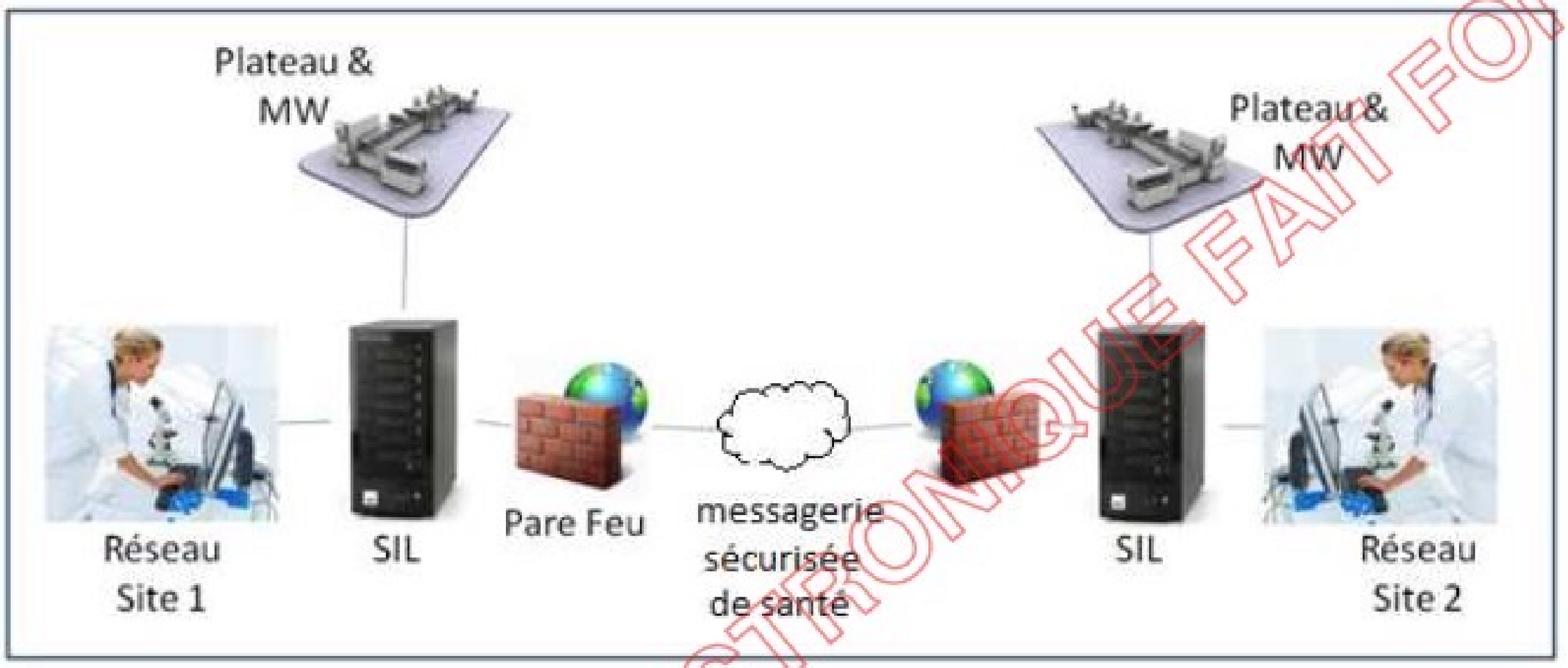
Exemples de réseaux au LBM

Mono SIL, mono/multi MW



Multi SIL, multi MW :

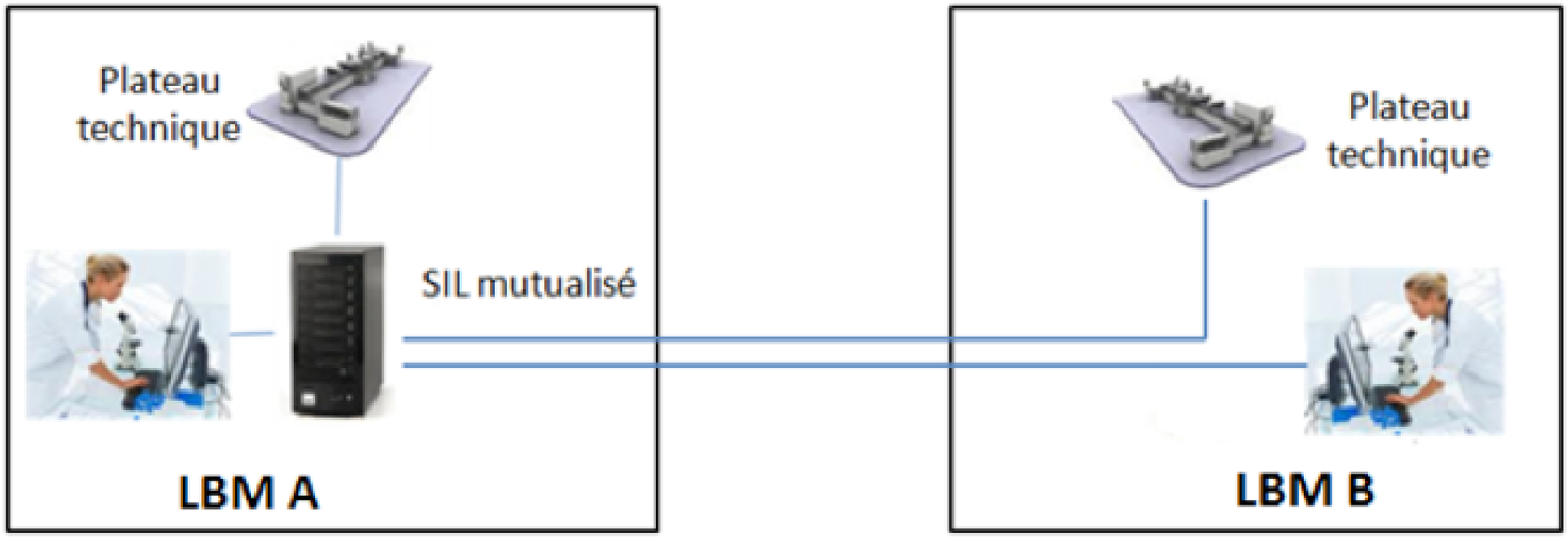
Dans cette configuration, deux sites travaillent ensemble sur un périmètre identifié mais restent sur des systèmes séparés. Les échanges de données ²sont réalisés entre les deux SIL par messagerie sécurisée de santé.



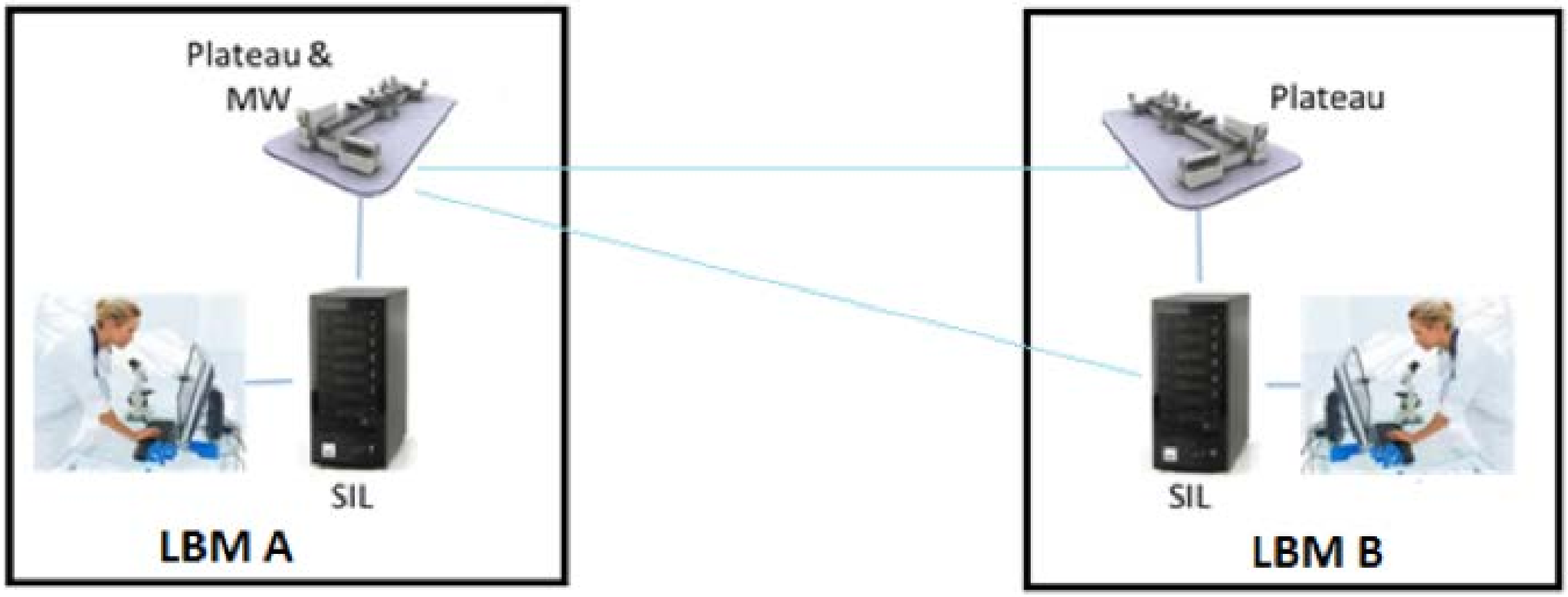
Dans cette configuration :

- Un premier niveau de validation biologique est réalisé par le LBM exécutant ;
- Le paramétrage des analyses dans les SIL est potentiellement différent ;
- Le paramétrage des feuilles de prescription est potentiellement différent ;
- Les MW sont potentiellement différents.

SIL mutualisé entre 2 LBM :



MW mutualisé entre 2 LBM :



Conséquences ? …

F.Macary 11/2014 : « … *Si deux LBM partagent un même serveur exploité par le SIL commun ou par les SIL des deux labos, alors ce serveur est nécessairement chez un hébergeur agréé données de santé.* *Cet agrément n'est pas délivré par l'ASIP mais par la ministre en charge de la santé, après examen du dossier par un comité d'agrément. L'ASIP ne fait qu'instruire le dossier.*

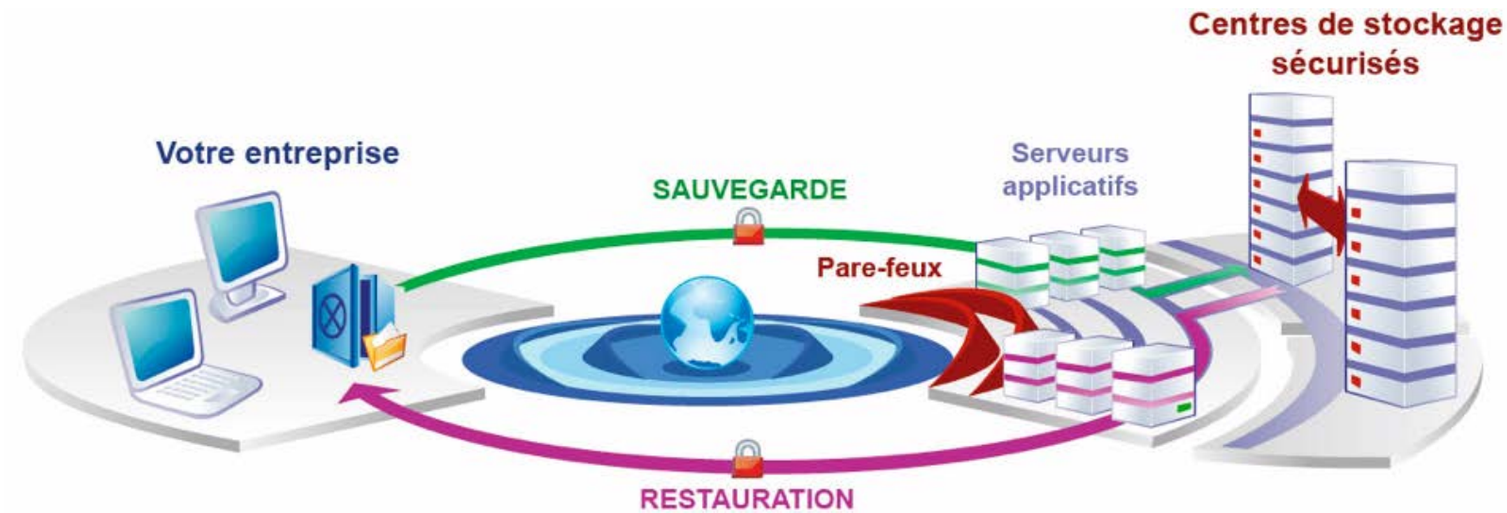
L'agrément garantit que les règles d'accès aux données de santé des patients telles que stipulées dans l'article L1111-8 du CSP sont bien respectées. En particulier il garantit qu'un personnel d'un LBM n'a accès qu'aux patients pour lesquels ce LBM a réalisé ou doit réaliser des examens.

*Un exemple de SIL multi-LBM est un SIL commercialisé par son éditeur en mode SaaS***. Chaque LBM ne voit que ses propres patients… »*

*** Le logiciel en tant que service ou Software as a Service (SaaS) est un modèle d'exploitation commerciale des logiciels dans lequel ceux-ci sont installés sur des serveurs distants plutôt que sur la machine de l'utilisateur. Les clients ne paient pas de licence d'utilisation pour une version, mais utilisent généralement gratuitement le service en ligne ou payent un abonnement récurrent.

Serveurs de résultats

Sauvegarde externalisée



Conditions d'hébergement : l'agrément préalable des hébergeurs de données de santé à caractère personnel

L'article L.1111-8 du CSP précise les conditions dans lesquelles les données de santé peuvent être confiées à un hébergeur.

- La personne concernée par les données de santé doit avoir consenti expressément à l'hébergement de ses données.
- L'hébergeur doit être agréé pour son activité.
- L'hébergeur est soumis aux règles de confidentialité prévues à l'article L.1110-4 du Code de la santé publique et à des référentiels d'interopérabilité et de sécurité.
- Lorsque les professionnels de santé ou les établissements de santé hébergent leurs propres données de santé, ils ne sont pas soumis à l'agrément et ne sont pas tenus de recueillir le consentement exprès de l'intéressé pour conserver ces données[3].

En revanche, dès lors qu'une entité héberge des données de santé de patients dont elle n'assure pas la prise en charge, elle est considérée comme hébergeur et doit obtenir un agrément.

Q11 - A partir de quelle durée de conservation des données de santé à caractère personnel un prestataire de service est-il considéré comme hébergeur ?

L'article 4 de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, établit que les dispositions de cette loi « ne sont pas applicables aux copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises ».

Si on transpose cette exclusion au contexte de l'agrément des hébergeurs de données de santé à caractère personnel, les prestataires qui proposent des services de type réseau de télécommunication, pour lesquels la durée du stockage des informations est limitée à la traversée des équipements actifs des réseaux sans mise en œuvre de traitement de niveau applicatif, ne sont pas considérés comme entrant dans le champ de la procédure.

4.13. Maîtrise des enregistrements

Ce chapitre de la norme porte sur la façon dont le laboratoire de biologie médicale organise l'enregistrement des données issues du SMQ et de la réalisation des examens.

Les documents relatifs à la réalisation des examens de biologie médicale conservés par le LBM et la durée de leur conservation sont déterminés par arrêté. Toutefois, une durée spécifique s'applique pour des domaines particuliers :

- pour la génétique et cytogénétique : articles R. 1131-20 et R. 1131-13 (durée 30 ans) ;
- pour le dossier du donneur de gamètes : article R. 1244-5 (durée 40 ans) ;
- pour l'assistance médicale à la procréation (AMP) : point I.1.2. de l'arrêté du 3 août 2010 modifiant l'arrêté du 11 avril 2008 relatif aux règles de bonnes pratiques cliniques et biologiques d'assistance médicale à la procréation (durée 20 ans) ;
- pour le diagnostic prénatal (DPN) : article R. 2131-2 (durée 5 ans).

En outre, la détention, le traitement, la conservation de données de santé à caractère personnel sur des supports informatiques sont organisées par les articles L.1110-4 et l'article L.1111-8 du CSP. En particulier, conformément au décret n°2006-6 du 4 janvier 2006, les hébergeurs de données de santé à caractère personnel doivent être agréés par le ministère chargé de la santé. La liste figure sur le site de l'ASIP Santé[12]. L'application de cette dernière disposition ne sera vérifiée qu'à compter du 1er novembre 2016.

Hébergeurs agréés

SÉCURITÉ | 19 JANV. 2015

Liste des hébergeurs agréés de données de santé à caractère personnel (mise à jour - 19 janvier 2015)

Dans le cadre de la procédure d'agrément des hébergeurs de données de santé à caractère personnel précisée par le décret du 4 janvier 2006, 77 décisions d'agrément ont à ce jour été rendues, par le ministre en charge de la santé.

=> quid de nos propres prestataires … ?

DMPanacée ?


Accueil
Patient
Professionnel de santé
Structure de Soins
DMP
ESPACE PROFESSIONNEL DE SANTÉ
DOSSIER MÉDICAL PERSONNEL
Rechercher...
En savoir plus sur le DMP
En pratique
Passer au DMP
Accès au DMP
Accueil > Professionnel de santé > En savoir plus sur le DMP > Le DMP en quelques mots
Le DMP en quelques mots
Le DMP au service des professionnels de santé
Les conditions d'accès au DMP
Votre patient et vous : des droits partagés sur le DMP
Le DMP garantit le respect du secret professionnel et la sécurité des données
PARTAGEZ
Le DMP en quelques mots
Le DMP a été institué par la loi pour faciliter le partage d'informations entre professionnels de santé, éviter les actes redondants et agir contre les interactions médicamenteuses.
DMP
ACTUALITÉS
Mai 2014
Réunion ville-hôpital au CHU de Bordeaux
Février 2014
2014 : Plus que jamais l'année du DMP
Toutes les actualites
LE DMP EN FRANCE
Les chiffres du DMP près de chez vous
Ouvrir la carte
FAQ
Toutes les questions que vous vous posez sur le DMP
En savoir plus

Logiciels compatibles ? :

- 3 SIL : Hexalis – GLIMS - Kalisil
- 25 SIH

DMP DOSSIER MÉDICAL PERSONNEL

Search...

Liste des logiciels DMP Compatibles

Affichage de 25 résultats par page

Rechercher: SGL

Editeur/candidat	Logiciels		Homologation		
	Nom	Catégorie (*)	Profils	Authentification	Date
Agfa Healthcare	Hexalis v4.2	SGL	Alimentation	Indirecte	27/09/13
MIPS	GLIMS v9 (GLIMS v8, GLIMS v9)	SGL	Alimentation	Indirecte	26/10/12
NETIKA	KALISIL v2	SGL	Alimentation	Indirecte	20/02/15

Affichage de 1 à 3 sur un total de 3 enreg (filtré à partir de 185 enregistrement(s))

Principaux messages

1. *L'enfer c'est (peut être) les autres*, la sécurité informatique NON !

2. La naïveté est le pire des vices dans la sécurité informatique

3. Sauvegardez, sauvegardez, il en restera toujours quelque chose

4. Il faut apprendre à ne pas partager lorsque 2 LBM travaillent ensembles…

5. L'ASIP est incontournable