Introduire la sécurité numérique dans les procédures d'acquisition

Questionnaire standardisé de l'AFIB portant sur les questions d'informatique et de la sécurité numérique

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin

Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/ - DOI : https://doi.org/10.34746/ids213

Avant-propos

A lire

L'AFIB a proposé **4 recommandations** en lien avec la prévention des cyberattaques dans le document: *Définir le niveau de risque associé aux équipements biomédicaux* [1]

Cet outil se concentre sur la première recommandation : **Introduire la sécurité numérique dans les procédures d'acquisition**

Introduire la sécurité numérique dans les procédures d'acquisition

Définir la collaboration dans les établissements de santé

Assurer la sécurité autour des équipements biomédicaux

Définir la criticité des équipements biomédicaux

Quand utiliser ce questionnaire ?

L'inclure dans les annexes techniques obligatoires des procédures d'achat

Lors de l'enregistrement d'une mise à disposition d'équipements avec une solution logicielle

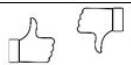
Lors des essais matériels pour évaluer la maturité du système informatique du dispositif

Après la sélection du fournisseur pour préparer l'installation et la mise en service

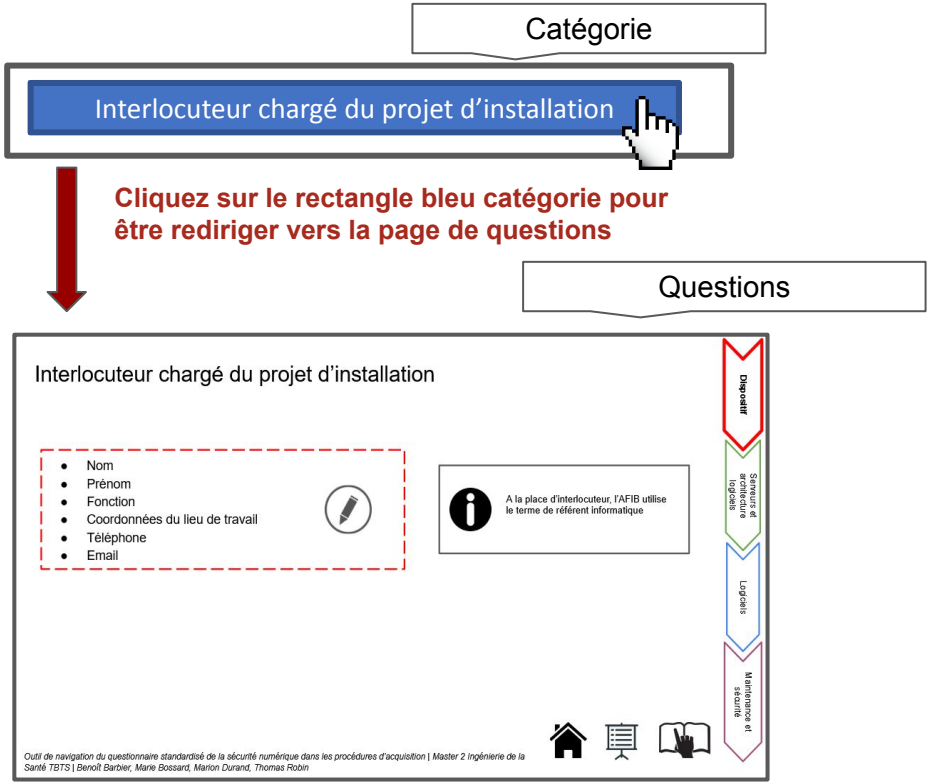
La prise en compte des réponses au questionnaire informatique doit **influencer l'évaluation et la sélection de l'équipement**, mais elle n'est pas un critère de blocage. Il est recommandé d'**inclure le service informatique dans le processus** d'analyse pour évaluer la faisabilité. Cela leur permet également de planifier en amont les ressources techniques et financières nécessaires à l'installation.

Mode d'emploi

1) Explication des icônes

SYMBOLES	EXPLICATIONS
	Revenir au début du document (cliquable)
	Revenir au logigramme concerné par la section (cliquable)
	Permet de revenir au mode d'emploi (cliquable)
	Permettent de naviguer à la diapositive précédente ou suivante respectivement (cliquable)
	Type de réponse : **oui / non**
	Type de réponse : **texte**
	Type de réponse : **document**
	Type de réponse : **chiffre**
	Informations complémentaires

2) Exemple



Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/ - DOI : https://doi.org/10.34746/ids213

Questionnaire en 4 parties

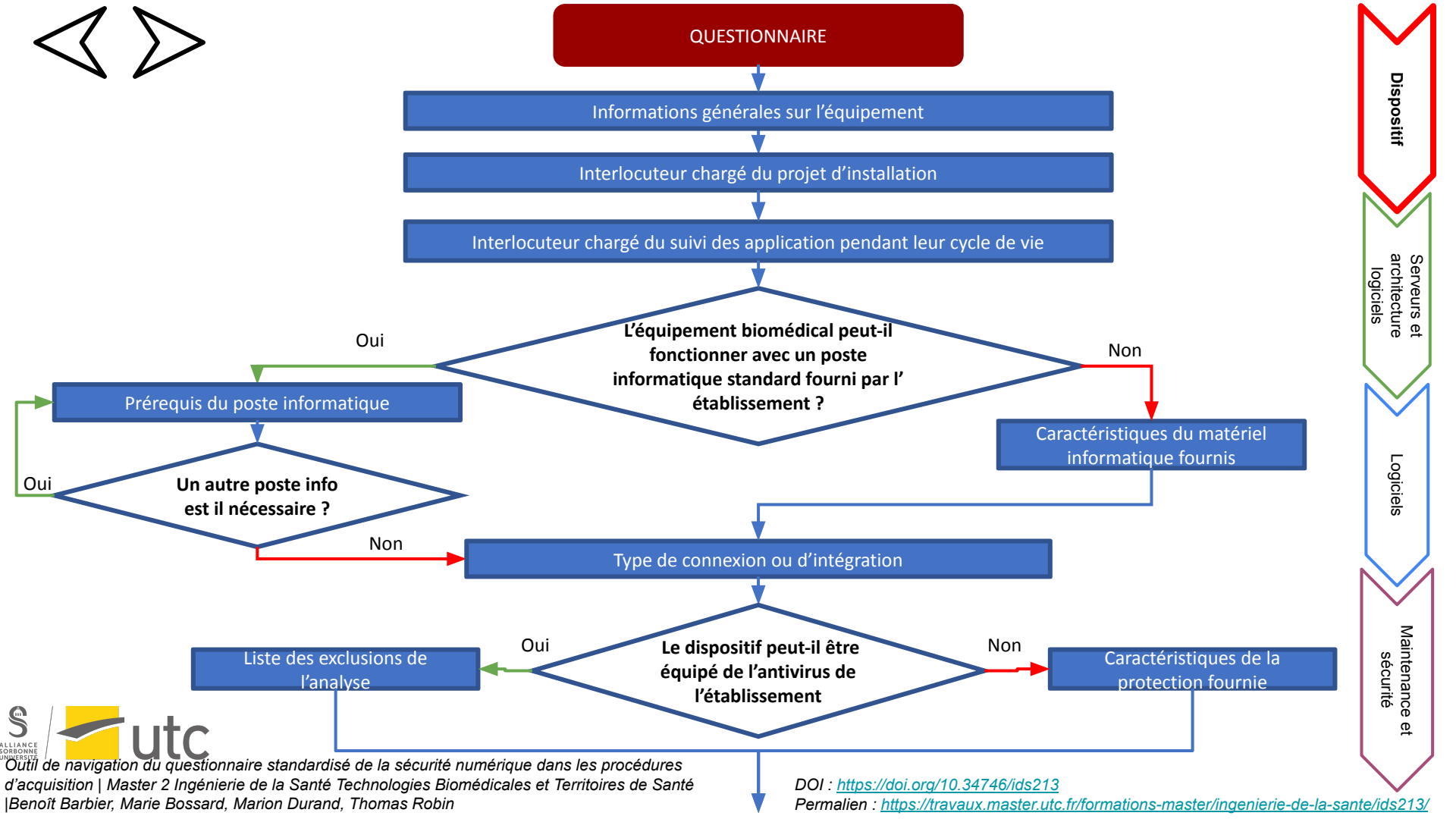
Description générale du dispositif

Description du ou des serveurs et description générique du ou des logiciels

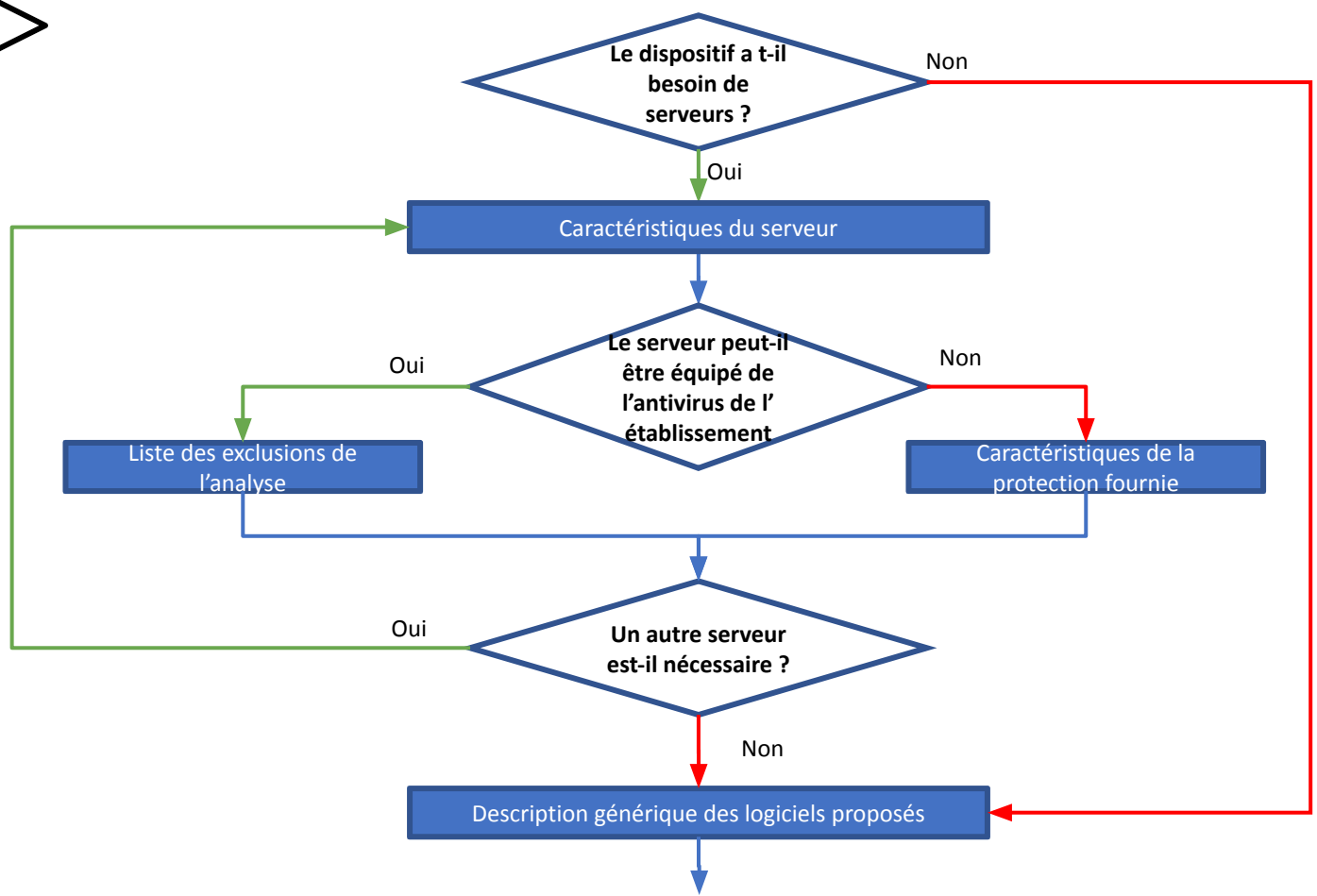
Description du ou des logiciels et leur intégration dans la structure de l'établissement

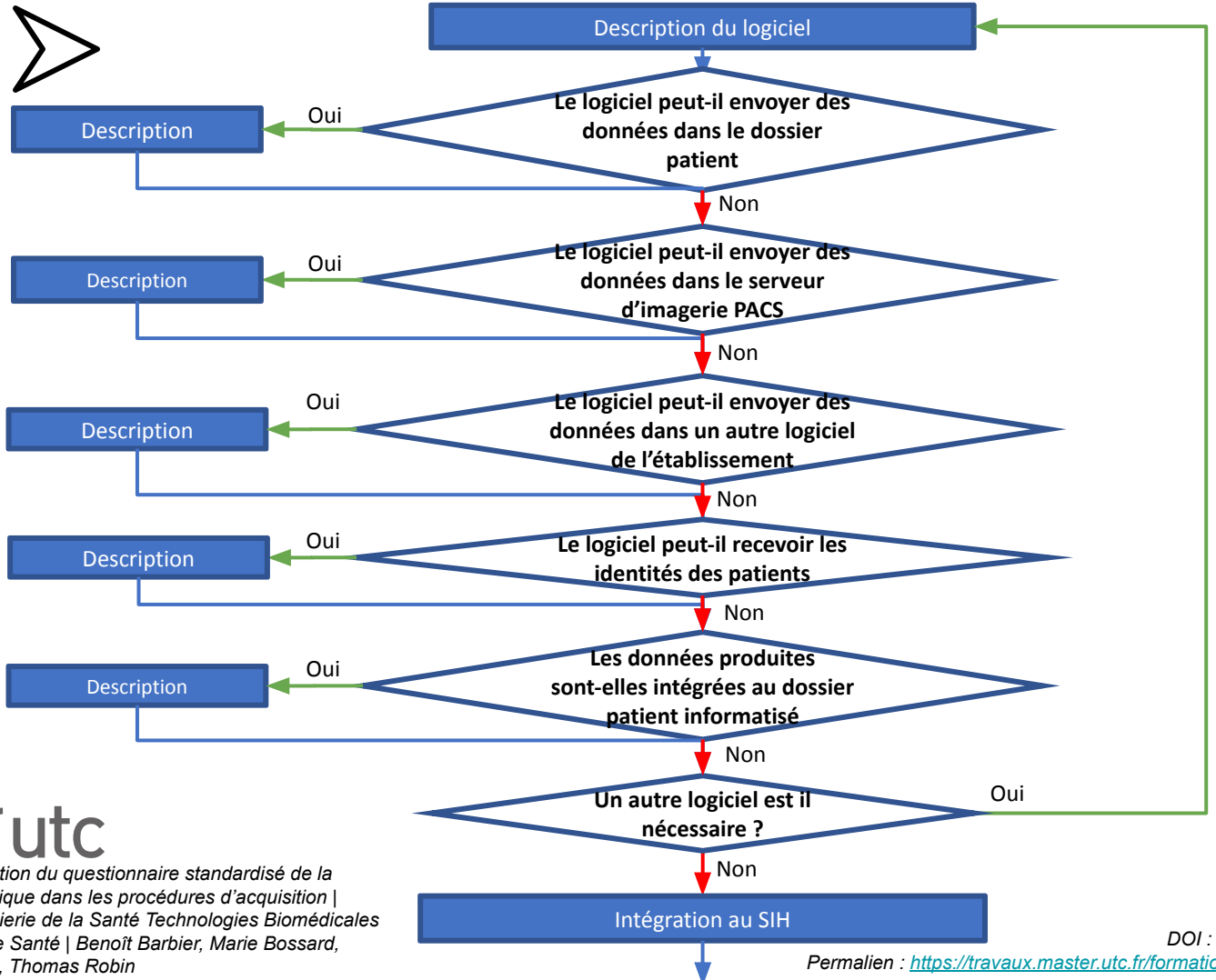
Maintenance du ou des logiciels et sécurité des données

Vous pouvez cliquer pour accéder au logigramme spécifique à chaque partie.



DOI : https://doi.org/10.34746/ids213
Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/


Le dispositif a t-il besoin de serveurs ?
Non
Oui
Caractéristiques du serveur
Le serveur peut-il être équipé de l'antivirus de l' établissement
Oui
Non
Liste des exclusions de l'analyse
Caractéristiques de la protection fournie
Un autre serveur est-il nécessaire ?
Oui
Non
Description générique des logiciels proposés



Dispositifs

Serveurs et architecture logiciels

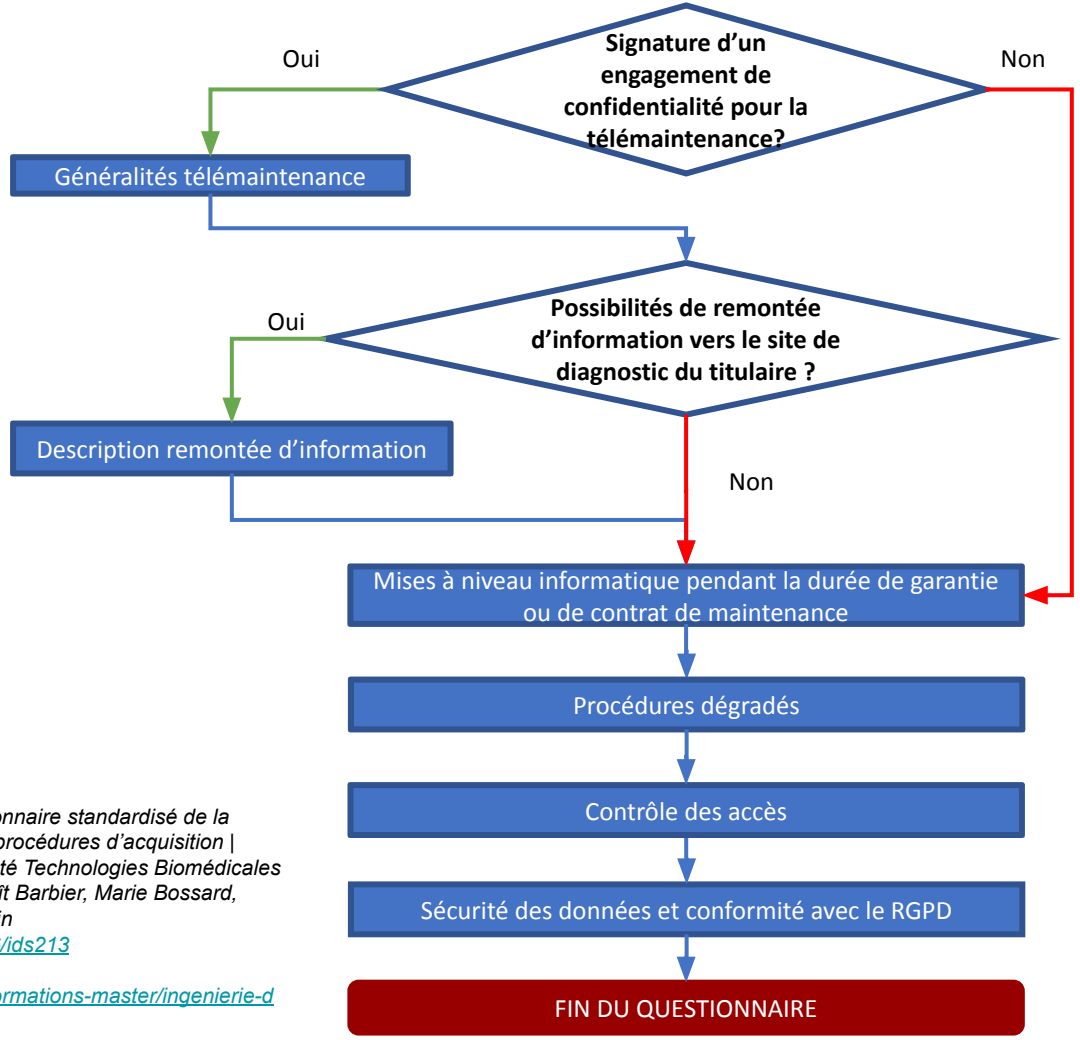
Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin

DOI : https://doi.org/10.34746/ids213

Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/



Dispositifs

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213
Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Informations générales sur l'équipement

- Désignation
- Marque
- Type
- Fabricant
- Lieu de fabrication
- Fournisseur
- Date de première mise sur le marché

La cybersécurité est une exigence qui fait partie des exigences générales des règlements 2017/745/UE et 2017/746/UE

- Classe du dispositif (I, IIa, IIb, III, DIV) au titre du marquage CE 93/42 ou CE 98/79
  → Joindre le certificat de conformité CE précisant la classe
- Classe du dispositif (I, IIa, IIb, III, DIV) au titre du marquage CE 2017/745 ou 2017/746
  → Joindre le certificat de conformité CE précisant la classe
- S'agit-il d'un logiciel partageant le marquage CE des dispositifs médicaux ?

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Interlocuteur chargé du projet d'installation

- Nom
- Prénom
- Fonction
- Coordonnées du lieu de travail
- Téléphone
- Email

A la place d'interlocuteur, l'AFIB utilise le terme de référent informatique

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Interlocuteur chargé du suivi des applications pendant leur cycle de vie

- Nom
- Prénom
- Fonction
- Coordonnées du lieu de travail
- Téléphone
- Email

A la place d'interlocuteur, l'AFIB utilise le terme de référent informatique/plateforme et utilise le terme de durée de vie plutôt que cycle de vie

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Prérequis du poste informatique

- Ecran
  - Taille (123)
  - Résolution (123)
  - Connectivité (123)
  - Autre caractéristique (123)
- Processeur (✎)
- Mémoire RAM (✎)
- Espace disque dur (123)
- Système d'exploitation
  - OS (✎)
  - Version (123)
- Spécificités (dongle, ports périphériques…) (✎)
- Besoins périphériques (DVD, ROM, imprimante…) (✎)
- Carte graphique (✎)
- Réseau
  - Interface (✎)
  - Débit (123)

Cette partie doit se faire en **étroite collaboration avec le service informatique** pour vérifier la compatibilité du matériel à acquérir avec l'existant et pour vérifier l'adéquation de la proposition avec les exigences de sécurité numérique

La **version du système d'exploitation (OS) est importante en cybersécurité** :

- Les anciennes versions comportent davantage de vulnérabilités connues
- La prise en charge diminue pour les anciennes versions
- Les nouvelles versions offrent de meilleures fonctionnalités de sécurité

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

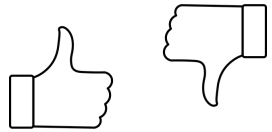
Matériel informatique livré avec la solution

- Dénomination du matériel
- Documentation détaillée si nécessaire
- Système d'exploitation
  - OS
  - Version

- Le titulaire s'engage à effectuer les mises à jour de sécurité du système d'exploitation

Type de connection ou d’intégration

- Besoin de connexion au réseau filaire
- Besoin de connexion au réseau wifi
- Besoin d’intégration au domaine réseau de l'établissement



En fonction du type de connection du matériel, les mesures de cybersécurité relatives à ce matériel ne seront pas les même. **Chaque type de connexion doit impliquer une réflexion spécifique en cas de passage à un mode dégradé**.

En règle générale, les cybercriminels adoptent une approche opportuniste, cherchant à tirer parti de failles potentielles, notamment l'utilisation de logins et mots de passe volés accessibles en ligne, des mesures de sécurité informatique insuffisantes, des logiciels et sites non mis à jour, ou des systèmes d'exploitation obsolètes, ainsi que la possible naïveté du personnel.

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Caractéristiques de la protection fournie

- Protection contre les codes malveillants
  - Le système est équipé de son propre dispositif de protection contre les codes malveillants ?
  - Nom
  - Modalité de mise à jour

- Le dispositif peut-il fonctionner dans une architecture comportant un pare-feu personnel lié au poste de travail ?
- Le logiciel peut fonctionner dans une architecture comportant un pare feu d'établissement pour les accès à Internet ?
- Des mesures de performances en présence du dispositif de protection contre les codes malveillants seront réalisés pendant la phase de qualification de l'installation ?

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Liste des exclusions de l'analyse

- Nom de l'Antivirus de l'établissement
- Liste des exclusions de l'analyse

Le déploiement d'un antivirus est essentiel sur tous les équipements, en particulier ceux connectés à Internet, pour se protéger contre les menaces en constante évolution. Il est impératif de maintenir à jour le logiciel antivirus et sa base de données de signatures.

Les antivirus commerciaux offrent **des mises à jour automatiques.** Vous pouvez également envisager des fonctionnalités complémentaires telles qu'un pare-feu, un filtrage Web, un VPN, et des outils anti-hameçonnage.

Une **gestion centralisée des antivirus** facilite le suivi et le contrôle de leur déploiement sur l'ensemble des équipements. Cela contribue à renforcer la sécurité des systèmes d'information.

Caractéristiques du serveur

- L'équipement biomédical peut fonctionner avec un serveur standard fourni par l'établissement
- Nombre de serveurs nécessaires (123)

- Fonctionnement sur un serveur virtuel
- Processeur (123)
- Mémoire RAM (123)
- Besoin : volumétrie pour les logiciels (123)
- Besoin : volumétrie pour les données (123)
- Système d'exploitation compatibles (OS et version)
- Base de données
- Spécificité (dongle, autre)

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Liste des exclusions de l’analyse

- Nom de l’Antivirus de l’établissement
- Liste des exclusions de l’analyse

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d’acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Caractéristiques de la protection fournie

- Protection contre les codes malveillants
  - Le système est équipé de son propre dispositif de protection contre les codes malveillants ?
  - Nom
  - Modalité de mise à jour

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Description générique des logiciels proposés

- Le fournisseur concède à l'établissement l'ensemble des licences d'utilisation nécessaires au fonctionnement de l'équipement
- Le titulaire s'engage à n'installer que les seuls logiciels nécessaires au bon fonctionnement du dispositif objet du marché
- Fournir la liste exhaustive des logiciels installés
  - Nom
  - Niveau de version
- Fonctionnalités principales du logiciel
- Le ou les logiciels sont installés sur des configurations standard de l'établissement
- Description des interactions entre les logiciels
- Système d'exploitation avec lesquels le ou les logiciels sont compatibles (préciser les versions)
- Liste exhaustive des services systèmes strictement nécessaires au fonctionnement attendu du ou des logiciels

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Description du logiciel

- Gestion des licences logicielles - Description (licences utilisateurs, licences à vie, abonnement, licences flottante, licences sites…)
- Fourniture d'un package d'installation (MSI)
  - Si non, décrire la procédure de réinstallation en cas de panne du matériel informatique
- Gestion d'un dossier patient ?
- Saisie de données administratives ?
- Saisie de données médicales ?
- Production d'un compte rendu ?
- Communication avec l'extérieur du centre hospitalier ?
- Saisie des données d'activité (PSMI, actes, etc) ?
- Caractéristiques techniques de l'application client (client lourd, web enrichi, etc.)
- Mode de gestion des données (base de données, fichiers plats, …)
- Liste des données produites
  - Nature
  - Format, extension
  - Volume (préciser l'unité) 123
  - Archivage médico-légal des données

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Description : envois de données dans le dossier patient

- Possibilité d'envoyer des données dans le dossier patient
- La connexion au dossier patient est-elle incluse dans l'offre ?
- Nature des données transmises

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Description : envois d'éléments dans le serveur d'imagerie PACS

- Possibilité d'envoyer des éléments dans le serveur d'imagerie PACS
- La connexion au PACS est-elle incluse dans l'offre ?
- Nature des données transmises

L'envoi d'éléments dans un système de stockage et de communication d'images médicales, communément appelé PACS (Picture Archiving and Communication System), est **essentiel pour la gestion des données d'imagerie médicale** dans un environnement hospitalier. Cependant, la cybersécurité joue un rôle crucial dans la protection de ces données sensibles.

Les images médicales contiennent des **informations hautement sensibles,** y compris des données personnelles de patients. Il est essentiel de protéger ces informations contre les accès non autorisés, les fuites de données et les attaques.

Les PACS sont **vulnérables aux menaces en ligne**, notamment les attaques par ransomware, les intrusions malveillantes, les vols de données et les fuites. Les conséquences de ces attaques peuvent être graves, allant de la divulgation de données personnelles à la perturbation des services de soins de santé.

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Description : envois d'éléments dans un autre logiciel

- Possibilité d'envoyer des éléments dans un autre logiciel de l'établissement ?
- Quel logiciel ?
- L'interface avec cet autre logiciel est elle incluse dans l'offre ?
- Nature des données transmises

Le cloisonnement des réseaux peut être comparé à une digue qui a pour rôle d'empêcher un pirate informatique de propager une infection à travers l'ensemble d'un système d'information. Cette stratégie doit également s'appliquer aux comptes d'administration et aux postes dédiés à ces tâches spécifiques.

En isolant certaines parties du réseau ou en restreignant l'accès à des comptes sensibles, on réduit la surface d'attaque potentielle pour les cybercriminels. Cela contribue à renforcer la sécurité globale du système d'information en limitant la propagation de menaces et en protégeant les informations et les ressources critiques. **Le cloisonnement des réseaux et la gestion rigoureuse des comptes d'administration sont des pratiques essentielles dans la protection des systèmes informatiques contre les intrusions et les attaques**.

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Description : réception des identités de patients

- Possibilité de recevoir des identités de patient
- L'interface complète est-elle incluse dans l'offre ?
- Nature des données transmises

La réception des identités de patients à l'hôpital est une étape critique dans la prestation des soins de santé. Cependant, elle comporte des défis importants en matière de cybersécurité. Les hôpitaux recueillent et gèrent des informations sensibles sur les patients, y compris des données médicales et personnelles.

La protection de ces informations est essentielle pour éviter les violations de la vie privée, les fuites de données et les utilisations malveillantes. Les mesures de cybersécurité, telles que l'authentification à deux facteurs, la cryptage des données, la gestion des accès et la sensibilisation du personnel, sont essentielles pour assurer la sécurité des données des patients.

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Description : intégration au dossier patient informatisé

- Intégration des données produites au dossier patient informatisé
- La connexion est-elle incluse dans l'offre ?
- Nature des données transmises

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Intégration au SIH

SIH = Système d'information hospitalier
Les SIH sont conçus pour faciliter la collecte, le stockage, la gestion, le partage et la sécurisation des données médicales et administratives

- Fournir une matrice des flux réseau afin de préciser la nature des échanges, les ports et protocoles nécessaire
- les communications sont-elles cryptées ?
- Fournir un schéma d'architecture détaillé de l'équipement où sont présentés les modules fonctionnels et techniques, ainsi que les interfaces
- Gestion d'un identifiant patient (NIP) ?
- Gestion d'un identifiant séjour (NDA) ?
- Interface entrante des identités/mouvements HL7 ? Format et version ?
- Interface entrante des rendez-vous HL7 SIU ?
- Interface entrante Worklist ?
- Interface sortante des documents HL7 ORU (courrier, compte rendu, tracé, ECG, EEG, rapport pdf OPH …) ?
- Interface sortante des documents du SIH (courrier, compte rendu, tracé, ECG, EEG, rapport pdf OPH, …) ?
- Interface sortante Dicom (conformance statement) ?
- Interface avec un SIL ou middleware de laboratoire
  - préciser le nom du SIL

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Généralité sur la télémaintenance

- La mise en place de la télémaintenance est soumise à l'acceptation et au retour signé d'un engagement de confidentialité
- Le titulaire accepte que la connexion de télémaintenance se fasse uniquement via la passerelle Internet sécurisée mise à disposition par l'établissement acquéreur ?
- La prise en main à distance est-elle proposée par le fournisseur ?
- La prise de main à distance est-elle incluse dans l'offre ?
- Jours et horaires d'accès
- Contraintes de mise en service
- La prise en main à distance fait-elle l'objet d'un compte rendu détaillé ?
- Modalités de transmission de ce compte-rendu ?

DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Remontée d'information par télémaintenance

- Possibilité de remontée d'informations vers le site de diagnostic du titulaire ? 
  - Si oui, quels sont les éléments administrés à distance
    - Remontée d'alertes ? 
    - Diagnostic ? 
    - Curatif ? 
    - Surveillance (alertes prédictives) ? 
    - Évolutions logicielles via la télémaintenance ? 
- Le titulaire garantit l'absence de remontée de données personnelles ou identifiantes ? 
- Le titulaire garantit que la remontée d'information est sécurisée et qu'elle ne concerne que les informations strictement indispensables à la maintenance ? 

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Mise à niveau informatique

- Préciser le type de contrat de maintenance incluant les mises à jours ci-dessous
- Liste des mises à jours comprises dans la durée de garantie et de contrats ci-dessus :
  - Mise à niveau des logiciels (soft) ?
  - Mise à niveau du matériel (hard) ?
  - Mise à niveau des interfaces avec le SIH ?
  - Mise à jour des protections anti-virus ?
  - Autres mises à jours

L'intégration de clauses de sécurité dans les contrats d'achat est essentielle pour renforcer la cybersécurité. Cela implique de spécifier des délais pour les mises à jour de sécurité, des audits de sécurité possibles, et des engagements en matière de protection des données de la part des fournisseurs et des établissements. Ces clauses encouragent les fournisseurs à maintenir un niveau élevé de sécurité, renforçant ainsi la résilience des systèmes d'information, en particulier dans des domaines sensibles comme la santé.

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Procédures dégradées

- Fonctionnement normal possible en cas de panne du réseau hospitalier
- Fonctionnement dégradé possible en cas de panne du réseau hospitalier
  - Si oui, fournir la procédure dégradée
- Solution ou procédures dégradées possibles en cas de défaillance du système suite à une attaque informatique
  - Si oui, finir la procédure dégradée

En 2021, 52% des structures de santé ont été contraintes de fonctionner en mode dégradé pour la prise en charge des patients, ce qui représente une augmentation de 7% par rapport à 2020. Ce mode dégradé varie en fonction de la nature de l'incident et des procédures spécifiques mises en place dans chaque structure. Il peut inclure l'application d'un plan de continuité, l'utilisation de méthodes manuelles (papier) pour la gestion des patients, l'utilisation de postes de travail dédiés, ou la mise en place de solutions de contournement pour faire face à des dysfonctionnements dans les logiciels de prescription, entre autres.

Source : Ministère des solidarités et de la Santé. Observatoire des Signalements d'incidents de sécurité des systèmes d'information pour le secteur santé. Rapport public 2021

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Contrôle d'accès

- Des journaux d'évènements collectent les traces des opérations système et applicatives
- Décrire les éléments de traçabilité intégrés aux logiciels pour le suivi des actions utilisateurs/administrateurs
- Décrire les modalités mises en place pour assurer la traçabilité des modifications de valeurs sensibles ou de la suppression de valeurs sensibles
- Possibilité de comptes différents et d'une gestion des droits utilisateurs, administrateur et maintenance
- Les mots de passe des comptes nécessaires à l'administration de la solution sont modifiables par l'acquéreur ?
- Le fournisseur garantit qu'aucun compte d'accès générique n'est "codé en dur" dans le code ou dans les scripts du logiciel
- L'équipement utilise le service de l'annuaire d'identité et d'authentification de l'établissement pour authentifier les utilisateurs
- Le système intègre un mécanisme de verrouillage automatique du poste en cas de non-utilisation pendant un temps donné paramétrable (ime out)
- Le mécanisme de verrouillage ne désactive pas les fonctions de monitoring et d'affichage des équipements dédiés
- L'identification des praticiens dans l'ensemble des données dans le logiciel est effectuée en utilisant le numéro du Répertoire Partagé des Professionnels de Santé RPPS

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Sécurité des données et conformité avec le RGPD

- Fournir l'analyse des risques liées aux systèmes d'information du dispositif médical
- Signer les clauses spécifiques RGPD en annexe
- Le titulaire accepte la réalisation d'audits
- L'export de données patients peut être réalisé uniquement au sein de l'établissement
- l'export des données patients fait l'objet d'une anonymisation non réversible des identités des patients
    - Si oui, fournir la procédure de gestion des données à caractère personnel ou la procédure d'anonymisation
- Tout déplacement de données personnelles par extraction, copie ou procédure d'export vers des disques locaux ou médias amovibles est autorisé uniquement aux personnels de l'établissement disposant des droits d'administrateurs
- Le système interdit nativement les copies d'écran
- Si l'équipement médical est porteur de données jugées sensibles par l'établissement, un stockage en ligne sécurisé des données peut être mis en place
- Ce stockage utilisera les dispositifs installés dans l'établissement (baies de stockage par exemple)

Suite des questions

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Sécurité des données et conformité avec le RGPD

- Décrire les modalités de restauration suite à la perte de données
- Les techniciens du fournisseur qui réalisent des opérations de maintenance ou de télémaintenance ne sont pas autorisés à accéder à l'identité des patients
- Si la solution proposée entre dans le périmètre de sous-traitant du Règlement Général européen sur la Protection des Données, le titulaire devra respecter ce règlement à date d'application et accepter des audits de de vérification de conformité
- Des données de santé sont-elles hébergées chez le titulaire ou l'un de ses sous-traitant ?
    - Si oui, l'hébergeur est agréé "hébergeur de données de santé" par l'ASIP (ou toute commission compétente désignée par la réglementation)
- Le centre de maintenance ou d'hébergement est en dehors du territoire national ?
    - Si oui, fournir la preuve que des dispositions adaptées ont été préalablement réalisées et validées par les autorités compétentes

Dispositif

Serveurs et architecture logiciels

Logiciels

Maintenance et sécurité

Questions précédentes

Outil de navigation du questionnaire standardisé de la sécurité numérique dans les procédures d'acquisition | Master 2 Ingénierie de la Santé Technologies Biomédicales et Territoires de Santé | Benoît Barbier, Marie Bossard, Marion Durand, Thomas Robin
DOI : https://doi.org/10.34746/ids213 Permalien : https://travaux.master.utc.fr/formations-master/ingenierie-de-la-sante/ids213/

Référence

[1] V. BOISSART, D. LAURENT, L. MONNIN, M.-J. ORY, F. RAJI, et S. ROUSSEL, « GROUPE DE TRAVAIL AFIB 2019–2020 : Sécurité Numérique des équipements biomédicaux », IRBM News, février 2021, vol. 42, n°1, p. 100298, doi: https://doi.org/10.1016/j.irbmnw.2021.100298