



QUESTIONNAIRE D'ÉVALUATION SSI

Guide fournisseur

AFIB

Introduction

L'Association Française des Ingénieurs Biomédicaux (AFIB) est un important relai d'information au sein du secteur biomédical.

Elle s'attèle d'une part à sensibiliser les instances sur l'importance de l'intégration des innovations dans la prise en charge des patients. Elle promeut d'autre part, la formation de l'ingénieur biomédical et la valorisation du métier.

L'association a pour but de favoriser, à tous les niveaux, la réflexion, l'action et la formation sur les thèmes de l'ingénierie clinique et / ou biomédicale. Elle assure notamment une veille technologique permanente au niveau national et international pour anticiper toutes les évolutions des dispositifs médicaux.

L'AFIB s'appuie sur un réseau de plus de 360 membres représentant un collectif important, agile et solidaire pour faire évoluer le paradigme hospitalier.

L'informatique et la sécurité dans les dispositifs médicaux sont des sujets prépondérants pour les ingénieurs biomédicaux. L'intégration et la diffusion des données dans les PACS/SIR, SIH... impliquent une politique de sécurité à appliquer aux dispositifs médicaux et une interaction importante entre Ingénieurs biomédicaux et informatiques.

Le groupe de travail « Exigences de sécurité des Systèmes d'Information pour les équipements biomédicaux des établissements de santé » a produit un questionnaire d'évaluation SSI qui a pour objet de faciliter la prise en compte de la sécurité lors de l'acte d'achat. Il détaille les objectifs de sécurité lors de la relation avec les acteurs du marché.

Le guide fournisseur vous décrit les enjeux et les objectifs de sécurité du questionnaire d'évaluation SSI.

Table des matières

AFIB	1
Introduction	2
1. Thématiques de sécurité.....	4
2. Normes de référence	5
3. Contenu	6
4. Onglet « Page de garde »	7
5. Onglet « Questionnaire »	8

1. Thématiques de sécurité

Les objectifs de sécurité présentés dans le questionnaire de sécurité couvrent les thématiques souhaités par l'AFIB et les établissements de santé. Ils sont basés sur les normes et référentiels de sécurité de référence en cybersécurité. En y répondant, vous pourrez répondre à de nombreux autres appels d'offre dans le secteur Santé en France.

Les thématiques abordés sont :

- La gestion des accès
- La connectivité et la sécurité des réseaux
- L'exploitation et la communication
- La maintenance du dispositif
- La protection des données
- La sécurité physique
- La résilience
- La gouvernance
- La gestion des licences
- La réversibilité
- La conformité

2. Normes de référence

Le questionnaire de sécurité s'est appuyé sur les normes et références de sécurité reconnus en France et à l'international.

- Guide des clauses de sécurité des systèmes d'information types à intégrer dans les marchés publics, Direction des Achats de l'Etat, ANSSI, Juillet 2019
- Guide Pratique, Règles pour les dispositifs connectés d'un Système d'Information de Santé, ASIP Santé, Novembre 2013
- Politique Générale de la Sécurité des Systèmes d'Information du secteur Santé (PGSSI-S),
- Principles and Practices for Medical Device Cybersecurity, International Medical Device Regulators Forum (IMDRF), Mars 2020
- Guide d'hygiène Informatique, Renforcer la sécurité de son système d'information en 42 mesures, Version 2.0, Septembre 2017
- Norme NF EN ISO/IEC 27002 version 2013

Les fournisseurs peuvent également s'appuyer sur les guides et standards ci-dessous pour certains objectifs de sécurité :

- Recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux, ANSSI, Août 2018
- Guide de sélection d'algorithmes cryptographiques, ANSSI, Mars 2021
- Guide pratique technique pour la Destruction des données lors du transfert de matériel informatique, version 2.0, Agence du Numérique en Santé, Août 2022
- Maîtriser les risques d'infogérance, ANSSI, Décembre 2010
- Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, Mai 2021

3. Contenu

Le questionnaire d'évaluation de la cybersécurité est constitué de 2 onglets à renseigner et des 2 onglets de référence.

- Onglet « **Page de garde** » permet d'identifier le fournisseur et le dispositif médical concerné.
- Onglet « **Questionnaire** » regroupe les questions à répondre par le fournisseur.
- Onglet « **Liste_Documents** » qui liste les documents attendus pour répondre aux objectifs de sécurité
- Onglet « **Annexe** » qui représente les différentes configurations types d'un dispositif médical, issues du Guide Pratique des règles pour les dispositifs connectés d'un SI de Santé.

Les seuls champs à renseigner sont en fond bleu clair. Les autres cellules sont protégées contre les modifications.

4. Onglet « Page de garde »

Section 1. Information sur le soumissionnaire

Les marques, modèles et versions doivent être renseignés pour ne pas avoir de doute sur le dispositif médical et le logiciel concerné par les réponses au questionnaire. Si plusieurs modèles et version sont concernés, vous pouvez les rassembler dans le même questionnaire si vous vous engagez à ce que les réponses données sont bien valables pour les différents modèles et versions mentionnés.

Section 2. Présentation du dispositif médical

La présentation fonctionnelle doit permettre de mentionner les principales fonctionnalités du dispositif médical.

La présentation technique doit permettre de préciser l'architecture technique générale du dispositif médical en vous inspirant des schémas de principe de l'onglet « Annexe ». Les différents composants techniques du dispositif médical (ordinateurs, serveurs, appareils, etc.) sont décrits.

Les réponses à la série de questions doivent permettre de rayer les questions de l'onglet « questionnaire » qui ne sont pas pertinentes.

5. Onglet « Questionnaire »

Comme évoqué dans la section 3, seuls les champs en bleu sont à remplir. La colonne « Réponse » propose plusieurs réponses possibles. Si vous souhaitez préciser votre réponse, vous disposez du champs « Explication et commentaires ». La colonne « Référence de vos documents » doit permettre de préciser les documents joints à la réponse pour répondre à la question.

Veuillez bien faire attention à la colonne « Informations et documents demandés » qui détaille ce qui doit être précisée dans la colonne « Explications et commentaires » et les documents demandés.

Nous souhaitons apporter les précisions suivantes.

Question Q7

La politique de mot de passe doit être implémentée sur le dispositif médical. Cela signifie par exemple que s'il y a une longueur minimale du mot de passe, il ne doit pas être possible techniquement d'entrer un mot de passe valide d'une longueur inférieure à ce seuil.

Question Q8

Une authentification forte impose 2 méthodes d'authentification parmi les 3 suivantes, avant de pouvoir donner l'accès :

- « Ce que je sais » : fourniture d'un mot de passe uniquement connu de l'utilisateur autorisé
- « Ce que je possède » : fourniture d'un élément d'authentification physique (carte à puce, clé USB...) ou d'un code par un appareil possédé par l'utilisateur (code via un SMS, code via une application mobile, code via un appareil dédié...).
- « Ce que je suis » : fourniture d'un élément biométrique (empreinte digitale, iris, visage, etc.).

Question Q9

Les recommandations de déploiement du protocole 802.1X pour le contrôle d'accès à des réseaux locaux sont une excellente base pour décrire les modalités de configuration sur le protocole 802.1X.

Lien vers le guide : [guide 802.1x anssi pa 043 v1.pdf](#)

Question Q10

La liste des mécanismes de chiffrement authentifié est fournie par l'ANSSI dans la recommandation 12 du guide de sélection d'algorithmes cryptographiques.

Lien vers le guide : [anssi-guide-selection_crypto-1.0.pdf](#)

Question Q11

La description des flux depuis et vers Internet doit être suffisamment détaillée pour indiquer le service porté par chaque flux : télésupervision, téléassistance, télémaintenance, activation de licence, contrôle permanent des licences, analyse de performance, etc.

Un exemple de matrice de flux attendue est fourni dans l'onglet « Exemple matrice flux » dans le questionnaire.

Question Q22

Common Vulnerability Scoring System (ou CVSS) est un système d'évaluation standardisé de la criticité des vulnérabilités selon des critères objectifs et mesurables. Le score est compris entre 0 et 10, 10 correspondant aux vulnérabilités les plus critiques.

Question Q24

La section 4.2 du guide pratique technique PGSSI-S pour la destruction des données lors du transfert de matériel informatique est une excellente base pour décrire votre procédure de suppression des données.

Lien vers le guide : [PGSSI-S Guide Pratique-Destruction de donnees-V2.0.pdf \(esante.gouv.fr\)](#)

Questions Q27, Q28 et Q29

Les actions de maintenance concernées par ces questions sont celles réalisées sur site de l'établissement. Les actions de maintenance à distance sont abordées dans les questions Q30 et Q31.

Question Q28

Les traces techniques sont les logs dédiés à la surveillance et à la sécurité du dispositif médical. Il y a notamment les logs de tentative de connexion sur le dispositif, les modifications des paramètres systèmes, et les traces de connexion à un compte. Le nom du compte utilisé, la date et l'heure de l'action

doivent être indiqués. Nous excluons ici les logs métier qui tracent les actions réalisées par un utilisateur dans le dispositif médical.

Question Q30

Pour décrire les modalités de connexion en téléassistance et en télémaintenance, les guides suivants de l'ANSSI sont pris en compte dans l'évaluation :

- Les paragraphes 2.2.3 et 2.2.4 du guide d'externalisation des systèmes d'information : [2010-12-03 Guide externalisation.pdf \(ssi.gouv.fr\)](https://ssi.gouv.fr/2010-12-03-Guide-externalisation.pdf)
- Pour la télémaintenance, le chapitre 10 des recommandations relatives à l'administration sécurisée des systèmes d'information : [anssi-guide-admin securisee si v3-0.pdf](https://anssi.gouv.fr/admin-securisee-si-v3-0.pdf)

Questions Q32 et Q33

Les logiciels tiers les plus importants à mentionner sont :

- OS des ordinateurs et serveurs constituant le dispositif médical,
- Logiciel anti-malware sur ces appareils, si le fabricant le fournit,
- Logiciel de bases de données,
- Logiciel permettant la télémaintenance et la téléassistance,

Questions Q36 et Q37

La mise en sécurité est un état du dispositif médical qui lui permet de maintenir les fonctionnalités vitales même en cas d'intrusion sur le dispositif ou de tentative de déni de service sur les interfaces réseau.

Le mode dégradé est un mode de fonctionnement qui permet à l'appareil de fonctionner malgré la perte de connexion réseau, ou en cas de perte d'un ordinateur ou d'un serveur du dispositif médical.

Question Q50

La liste des mécanismes de chiffrement authentifié est fournie par l'ANSSI dans le guide de sélection d'algorithmes cryptographiques.

Lien vers le guide : [anssi-guide-selection crypto-1.0.pdf](https://anssi.gouv.fr/admin-securisee-si-v3-0.pdf)