La Politique générale de sécurité des systèmes d'information de santé (PGSSI-S)

Présentation

Club EBIOS
8 septembre 2016

Erik Boucher de Crèvecœur
Service de l'expertise technologique

Introduction

La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S)

- n'est pas une PSSI…
- C'est un ensemble de documents élaboré depuis 2012 par l'Etat (DSSIS / ASIP Santé) pour organiser la sécurité des SI de Santé :
  - Principes fondateurs
  - Guides organisationnels
  - Référentiels techniques
  - Guides pratiques
- Ils sont destinés aux structures de santé et aux industriels qui les équipent et les accompagnent.
- Ils sont soumis à concertation avec l'ensemble des acteurs partie prenante du domaine santé / médico-social.

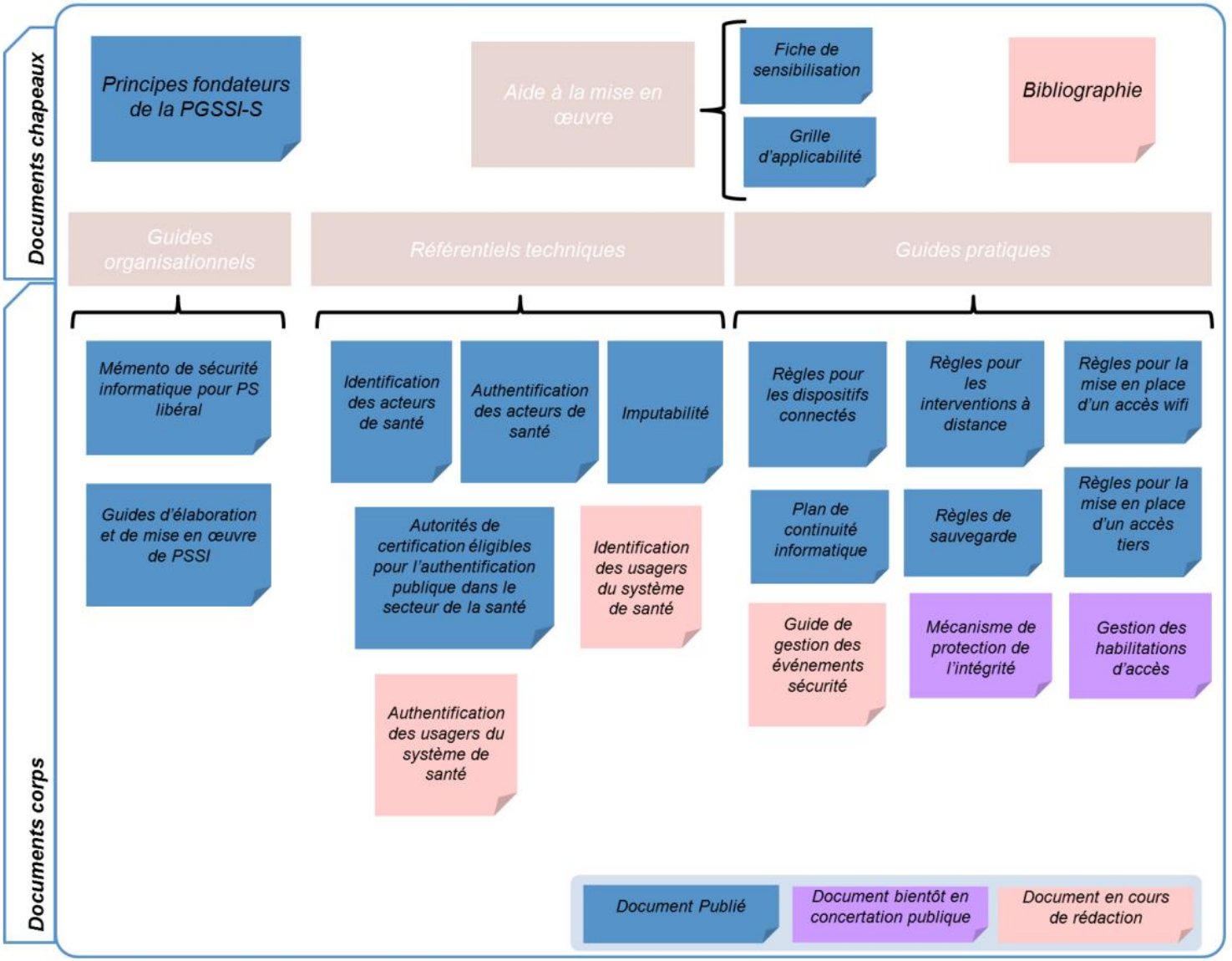
Principes fondateurs de la PGSSI-S

- **Conformité au cadre juridique**
  - Loi I&L, Code de la Santé publique, RGS, PSSI-E, PSSI-MCAS
- **Qualité de la prise en charge sanitaire du patient**
  - « La sécurité des données de santé apporte de la confiance et de la fiabilité » (impacts sur la sécurité des soins)
- **Respect des droits du patient**
  - « Garantir notamment la confidentialité, la traçabilité et la pérennité des données de santé à caractère personnel tout au long du cycle de vie des données (de leur création ou saisie à leur archivage et destruction »
  - Information et recueil du consentement du patient au traitement de ses données
- **Adoption des bonnes pratiques éprouvées dans d'autres secteurs**
  - « les normes ISO 2700x, la méthode EBIOS de l'ANSSI, le RGS »
- **Sécurité juridique des acteurs de santé**
  - « Identifier clairement les responsabilités juridiques de chaque acteur dans leur usage au quotidien de ces données, notamment celles à caractère personnel »

Corpus documentaire

17 documents

575 pages



Types de documents

- Documents globaux
  - Principes fondateurs
  - Fiche de sensibilisation
  - Grille d'applicabilité des référentiels

- Guides organisationnels
  - Mémento de sécurité informatique pour les professionnels de santé en exercice libéral
  - Guide d'élaboration et de mise en œuvre d'une PSSI, avec en annexe :
    - un canevas de PSSI,
    - un modèle de plan d'action SSI,
    - une grille de couverture des règles de la PSSIE,
    - un modèle de charte utilisateurs,
    - un modèle de charte administrateurs.

Types de documents

- Règles et Guides pratiques (recommandations, état de l'art)
  - Dispositifs connectés
  - Interventions à distance sur les Systèmes d'Information de Santé
  - Mise en place d'un accès wifi
  - Mise en place d'un accès web pour des tiers
  - Sauvegarde des Systèmes d'Information de Santé
  - Plan de Continuité Informatique
  - Destruction de données lors du transfert de matériels informatiques

Et, en cours d'élaboration :

- *Gestion des habilitations d'accès*
- *Protection de l'intégrité pour le stockage des données*
- *Gestion des équipements mobiles*
- *Gestion des événements et incidents SSI*

Types de documents

- Référentiels techniques (qui deviendront opposables)
  - Authentification des acteurs de santé
  - Identification des acteurs sanitaires et médico-sociaux
  - Imputabilité
  - Autorités de certification éligibles pour l'authentification publique dans le secteur de la santé

Et, en cours d'élaboration :

  - *Identification des usagers et patients*
  - *Authentification des usagers et patients*

Opposabilité de la PGSSI-S

Code de la santé publique - Art. L. 1110-4-1

« Afin de garantir la qualité et la confidentialité des données de santé à caractère personnel et leur protection, les professionnels de santé, les établissements et services de santé, les hébergeurs de données de santé à caractère personnel et tout autre organisme participant à la prévention, aux soins ou au suivi médico-social et social utilisent, pour leur traitement, leur conservation sur support informatique et leur transmission par voie électronique, des systèmes d'information conformes aux référentiels d'interopérabilité et de sécurité élaborés par le groupement d'intérêt public mentionné à l'article L. 1111-24. Ces référentiels sont approuvés par arrêté du ministre chargé de la santé, pris après avis de la Commission nationale de l'informatique et des libertés. »

Référentiels déjà identifiés comme pouvant être rendus opposables :

- un premier arrêté portera les référentiels d'identification et d'authentification des acteurs de santé, et le référentiel d'imputabilité ; il détaillera :
  - la grille d'applicabilité
  - les dates de mise en œuvre pour chacun des référentiels (*3 ans pour les paliers minimum initiaux*)
  - les dérogations possibles sur justification, assumées par les responsables de traitement
- dans un second temps, un arrêté portera les référentiels d'identification et d'authentification des usagers et patients

Les paliers et l'applicabilité

- **Les référentiels et guides de la PGSSI-S présentent les exigences par paliers :**
  - le **palier minimal** fixe des exigences de sécurité indiscutables,
  - le palier le plus élevé est un **palier cible**, un objectif de sécurité.

- **Pour un SI donné, le palier minimum à mettre en œuvre est déterminé par :**
  - **la Grille d'applicabilité des référentiels de la PGSSI-S**, qui fixe un palier minimum pour différents contextes d'usage métier,
  - **une analyse de risques** pour éventuellement réévaluer le palier minimum à la hausse en fonction des spécificités du SI (obligations règlementaires, risques particuliers…).

NB: la Grille d'applicabilité actuelle (1.0) va devoir être revue pour être utilisable dans le cadre de l'opposabilité des référentiels.

Merci de votre attention

Et à l'écoute de vos questions ☺

Site de l'ASIP sur la PGSSI-S

http://esante.gouv.fr/services/politique-generale-de-securite-des-systemes-d-information-de-sante-pgssi-s/en-savoir-plus-0

Référentiels de la PGSSI-S

http://esante.gouv.fr/pgssi-s/espace-publication