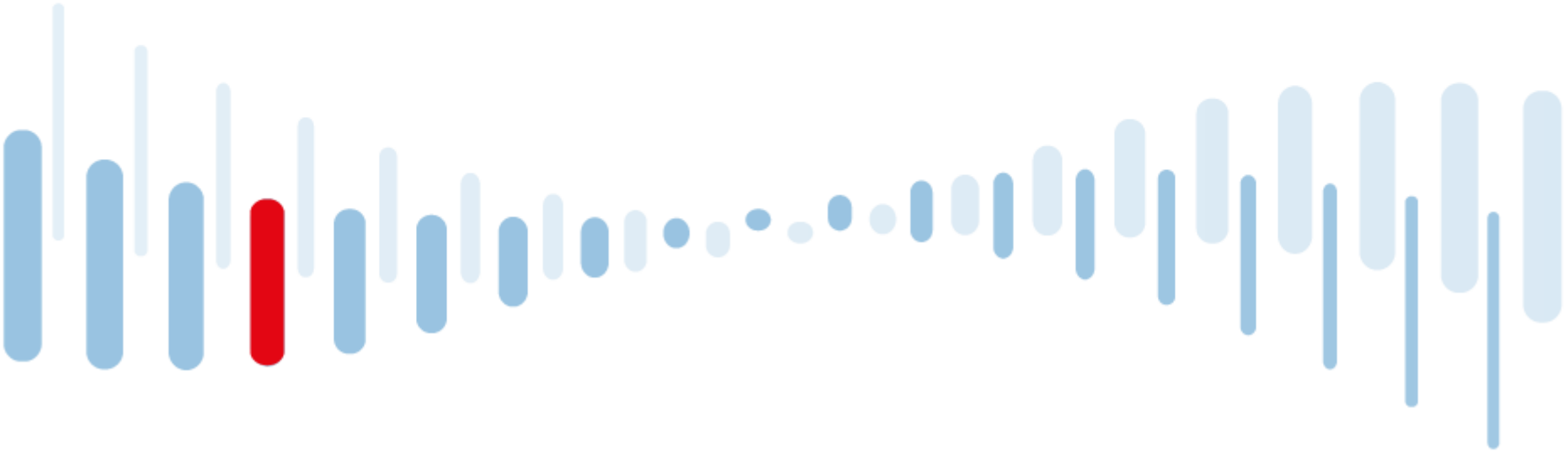
politique générale de sécurité du système d'information de santé :

PGSSI-S

Christophe JODRY, chargé de mission sécurité
ASIP Santé

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Pourquoi la PGSSI-S?



Des enjeux cyber sécurité dans le domaine de la santé

Choisir les dispositifs d'authentification adaptés.

Imputabilité

Gérer la traçabilité des accès au système d'information.

Confidentialité

Assurer les sauvegardes et la reprise sur incident.

Intégrité

Accompagner les nouveaux usages.

Disponibilité

Innovation

Gestion des risques

Sensibiliser les utilisateurs aux nouvelles menaces.

En réponse, la PGSSI-S

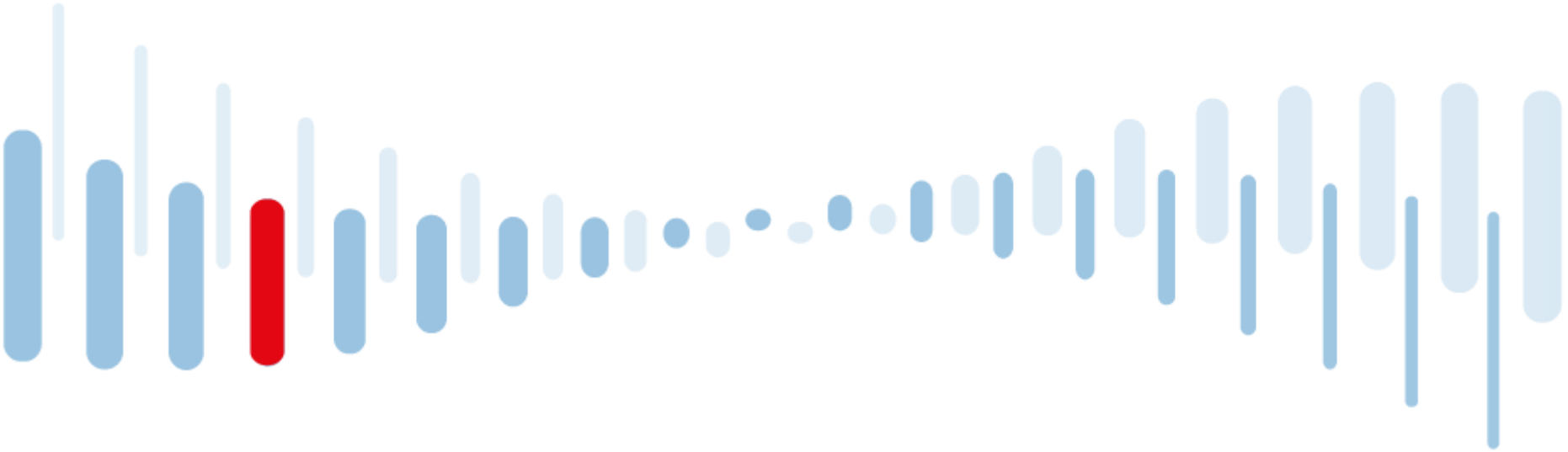
Définir les exigences et recommandations incontournables en matière de sécurité,

liées à la protection de la donnée de santé à caractère personnel,

dans le respect des droits du patient,

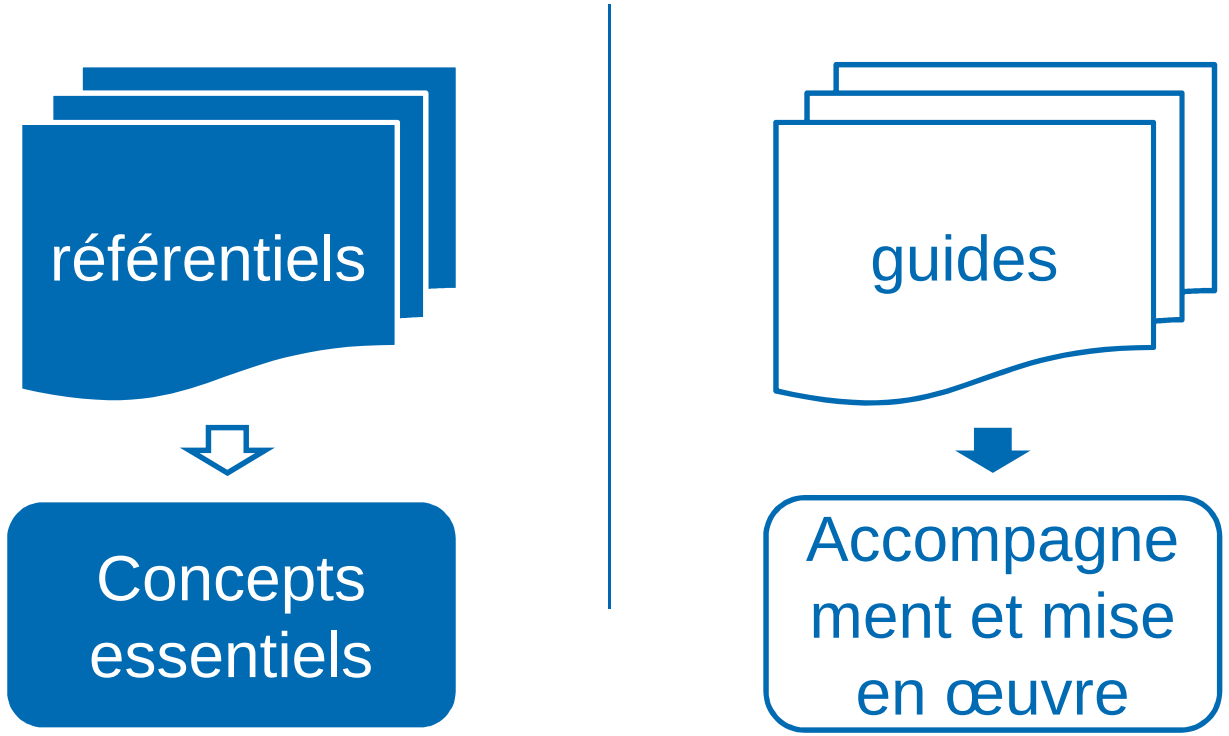
avec des contraintes opérationnelles et économiques acceptables pour l'ensemble des acteurs des secteurs sanitaire, médico-social et social.

Qu’est-ce que la PGSSI-S?



Constitution du corpus documentaire

La PGSSI-S est **un corpus documentaire et non une norme ou un référentiel unique.**



Opposabilité de la PGSSI-S

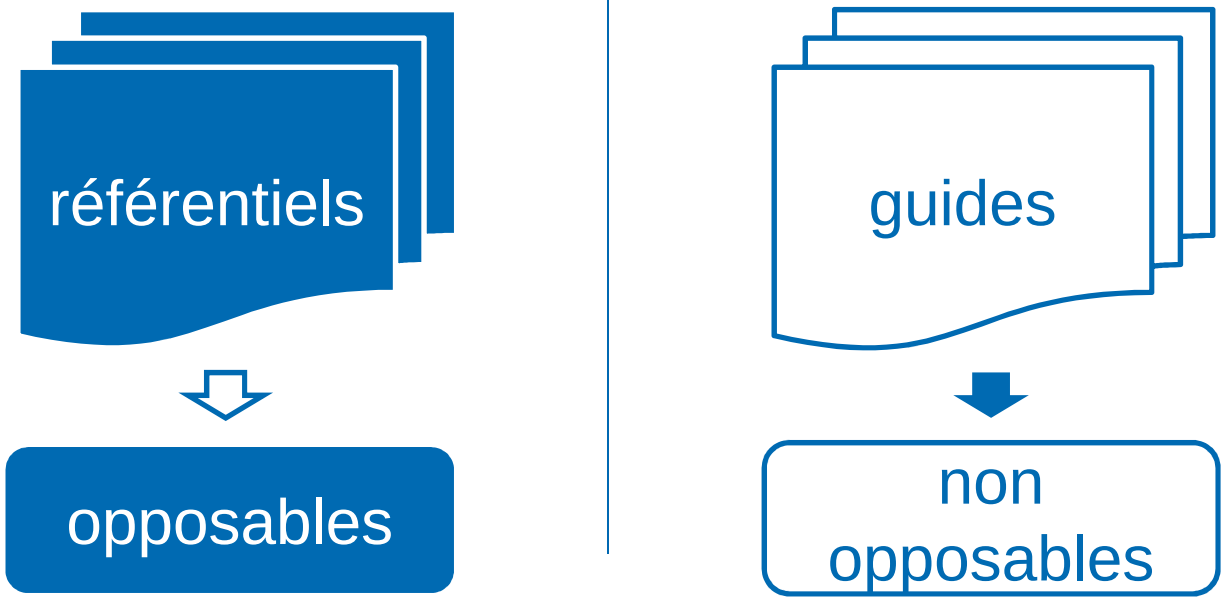
La PGSSI-S est rendue opposable par l'article L1110-4-1 créé par la loi n° 2016-41 du 26 janvier 2016 - art. 96 (V).

Un texte est dit opposable à la date de sa publication au Journal Officiel.

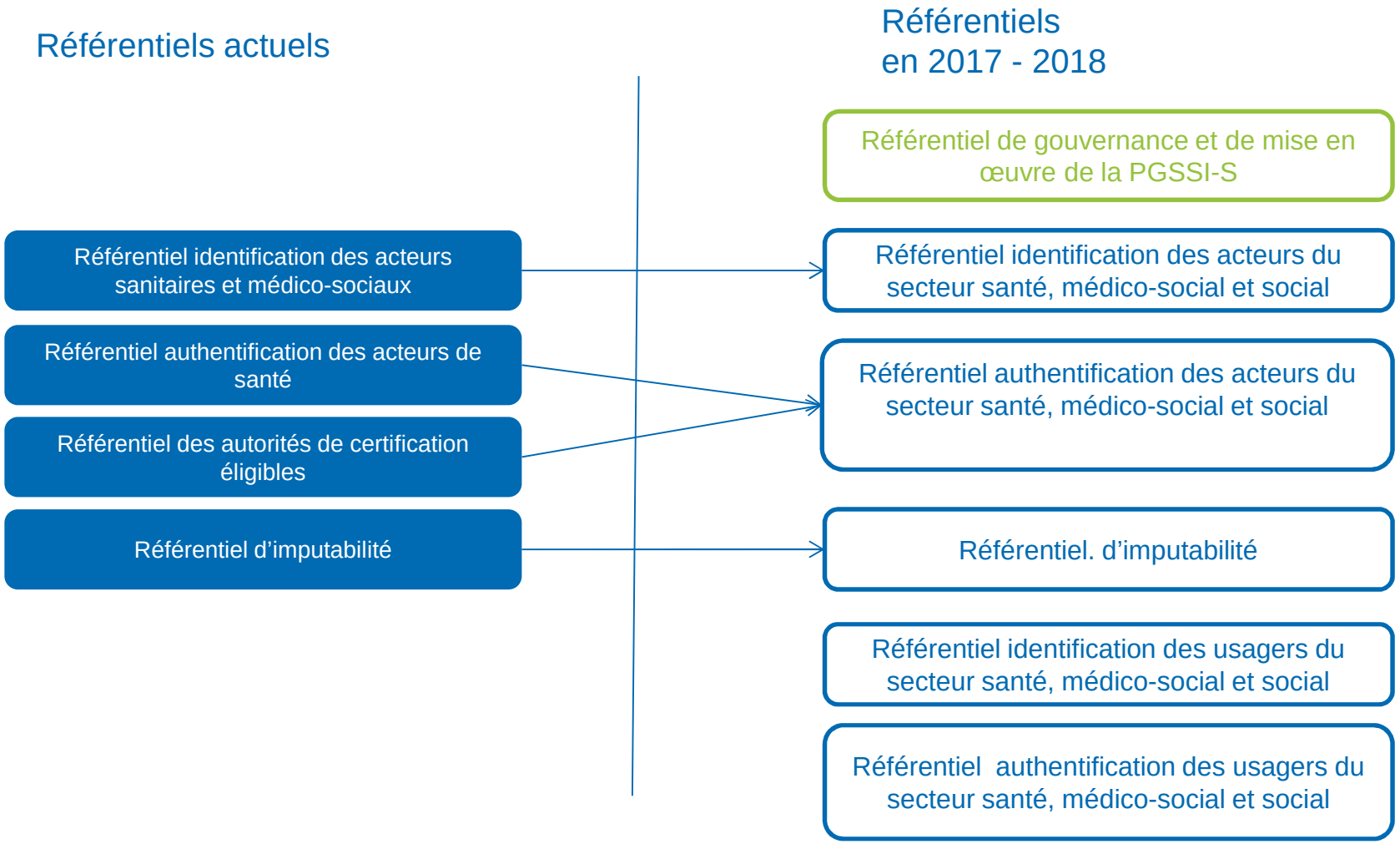
L'opposabilité a pour effet juridique de rendre le texte contraignant ou encore de lui donner force obligatoire.

Concrètement, l'administration, comme les administrés, pourront s'en prévaloir, y compris dans le cadre d'un recours contentieux, pour défendre leurs intérêts respectifs.

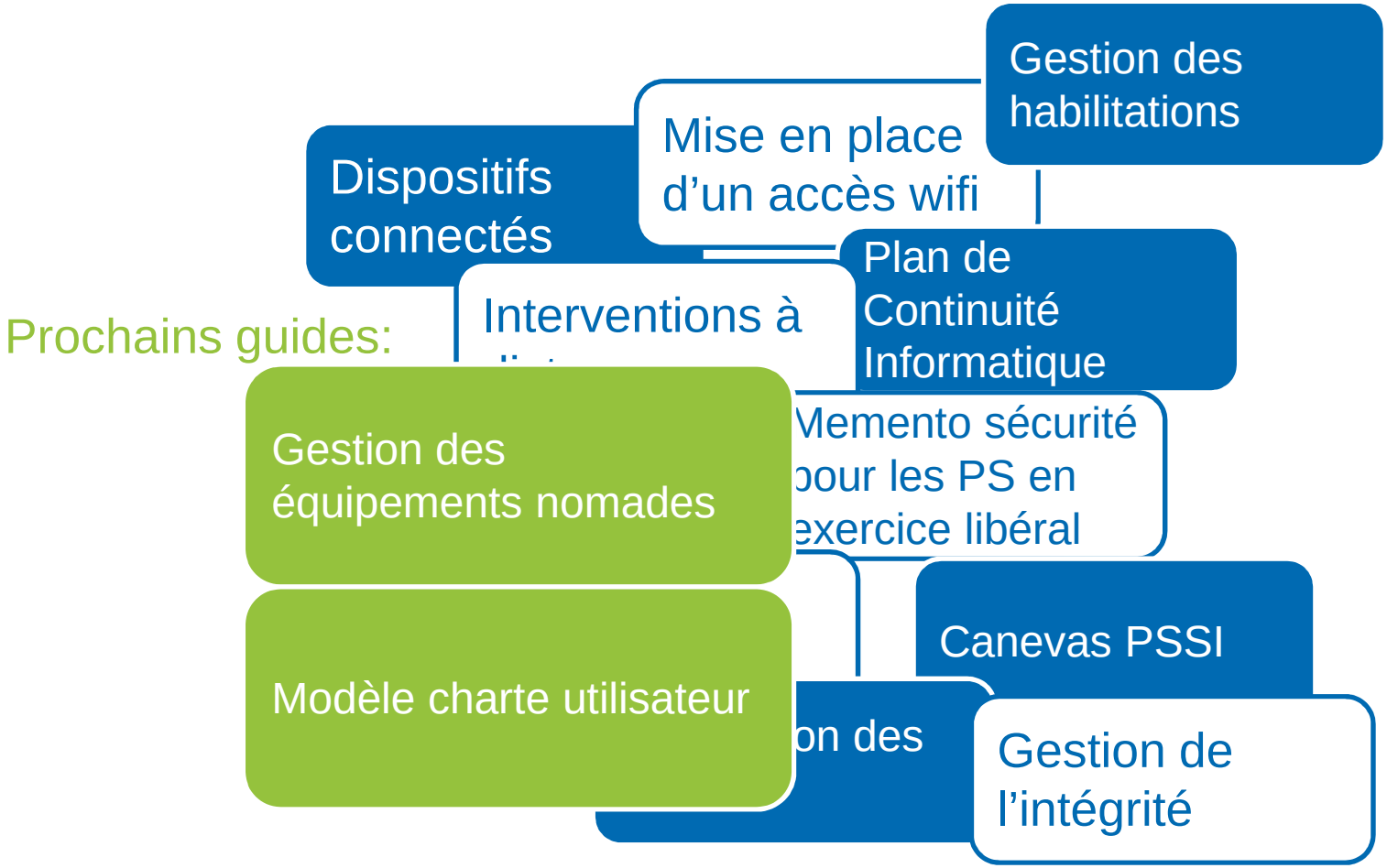
Opposabilité et typologie des documents



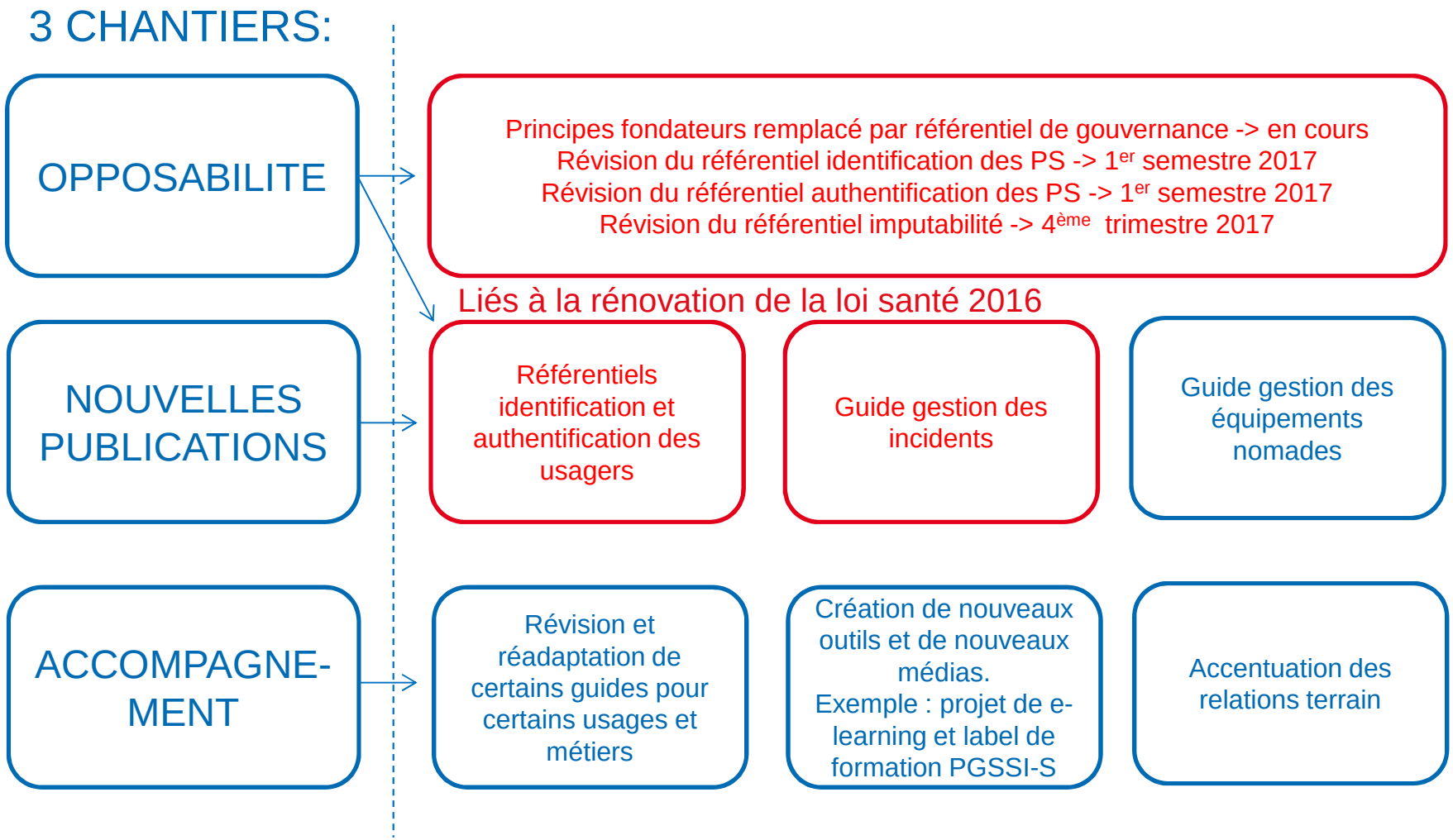
Les référentiels



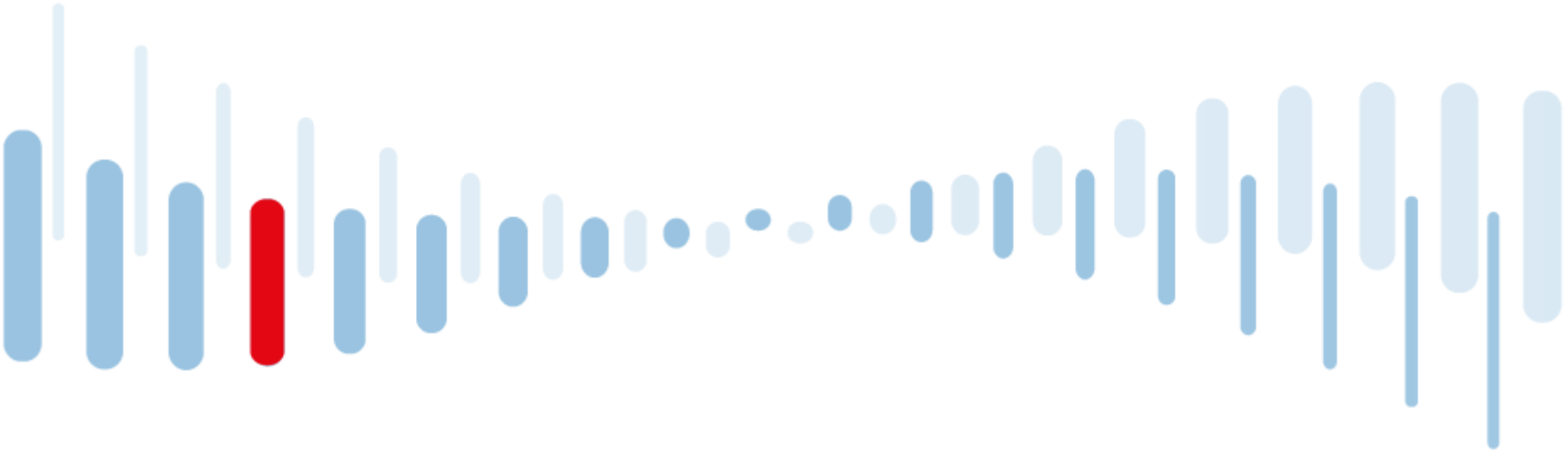
Les guides


Gestion des habilitations
Mise en place d'un accès wifi
Dispositifs connectés
Plan de Continuité Informatique
Interventions à
Prochains guides:
Gestion des équipements nomades
Memento sécurité pour les PS en exercice libéral
Canevas PSSI
Modèle charte utilisateur
on des
Gestion de l'intégrité

La feuille de route 2017



Conclusion



La PGSSI-S, un code de la route pour la sécurité des systèmes d'information santé

Un cadre réglementaire valable pour tous les acteurs, du piéton au poids lourd.

Un cadre réglementaire qui s'adapte aux innovations.

Le code de la route doit s'adapter à la voiture autonome.

Tout véhicule acheté doit permettre la conformité à la PGSSI-S.

L'ASIP Santé n'est pas le gendarme mais la prévention routière.

Lien vers la PGSSI-S

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

Concertation publique en cours jusqu'au 31 mars :

- Référentiel de gouvernance et de mise en œuvre;
- Guide de la gestion des équipements nomades;
- Charte utilisateur à destination des petites et moyennes structures;
- Quizz de sensibilisation utilisateur.

Quizz charte utilisateur

asipsanté L'AGENCE FRANÇAISE DE LA SANTÉ NUMÉRIQUE

Vous recevez un mail avec une pièce jointe d'une adresse inconnue vous annonçant que vous avez gagné un voyage aux Bahamas.

1. Vous cliquez sur la pièce jointe et préparez vos bagages.

2. Vous n'ouvrez pas la pièce jointe et prévenez votre service informatique ou votre hiérarchie.

3. Vous ne lisez jamais vos mails.

Vos fichiers indispensables à votre travail sont sauvegardés :

1. sur votre ordinateur de travail uniquement.

2. sur le serveur informatique que votre employeur met à disposition.

3. sur une clé USB.

4. sur un espace sur internet avec votre compte personnel.

5. sur... vous ne savez pas en fait.

Votre collègue vous demande votre mot de passe pour gérer vos activités lors de vos congés.

1. Vous lui donnez sur un post-it et lui promettez d'envoyer une carte postale.

2. Vous lui envoyez par mail pour ne pas qu'il le perde.

3. Vous n'avez pas de mot de passe, c'est plus pratique.

4. Vous refusez gentiment.

Le curseur de votre souris se met à bouger seul à l'écran.

1. Cool, votre ordinateur travaille pour vous.

2. Vous redémarrez votre ordinateur et reprenez votre travail.

3. Vous alertez votre service informatique ou votre hiérarchie.

Vous travaillez sur un dossier sensible et confidentiel sur votre ordinateur. Vous êtes appelés en urgence par un collègue dans une autre pièce.

1. Vous éteignez votre ordinateur, fermez le bureau à triple tour, enclenchez l'alarme , levez le pont-levis et allez aider votre collègue.

2. Vous verrouillez votre session en une seconde et allez aider votre collègue.

3. Vous allez aider votre collègue en signalant à toute personne croisée que votre ordinateur est libre d'accès.

En arrivant au travail, vous trouvez une clé USB par terre, devant l'entrée.

1. Vous la laissez là, afin que celui qui l'a perdue puisse la retrouver.

2. Vous la ramassez et l'apportez au service informatique en expliquant où vous l'avez trouvée.

3. Vous la ramassez et courez la brancher sur votre poste pour regarder ce qu'il y a dessus.

4. Vous la ramassez et courez la brancher sur le poste de votre collègue pour regarder ce qu'il y a dessus. Mieux vaut éviter de mettre un virus sur votre propre poste !