appui santé & médico-social

AVIS D'EXPERT : COMPRENDRE COMMENT METTRE EN PLACE UN ACCES A DISTANCE POUR LES PROFESSIONNELS DE SANTE

Référence	Avis Expert ANAP_Comprendre comment mettre en place un accès à distance pour les professionnels de santé
Version	VF
Auteur(s)	Daniel Michelle
Date de diffusion	03/03/2015

Définition d'un avis d'expert

Proposition d'actions à mener dans un contexte spécifique, en réponse à un point dur identifié sur la plate-forme MonHopitalNumérique. Ce conseil s'appuie sur l'expérience de l'expert et sur des échanges avec différents partenaires, notamment le groupe d'experts HN de l'ANAP.

Un avis d'expert n'a pas été validé par les instances de l'ANAP.

Les avis d'experts sont disponibles, ainsi que de nombreux outils et publications de l'ANAP, sur le site www.monhopitalnumerique.fr

Résumé du point dur

Dans le cadre d'une activité multi-sites ou de la PDS, les professionnels de santé sont amenés à utiliser le SIH depuis l'extérieur. Il est donc nécessaire de prendre en compte les enjeux en termes de sécurité et d'équipement.

INTRODUCTION : LA DEMANDE DE CONNEXION A DISTANCE, UNE REQUETE LEGITIME DES UTILISATEURS

L'évolution du paysage des établissements de santé favorise l'émergence de nouveaux contextes justifiant une connexion à distance, gardes sur plusieurs sites d'un établissement, astreintes au domicile, partage d'activités, exercice de téléconsultation...

La généralisation de l'informatisation dans les soins engendre une demande croissante des utilisateurs pour un recours à une connexion à distance. Le circuit du médicament est un des principaux processus informatisés, les prescripteurs ont maintenant une demande légitime d'accès à la prescription à distance lors des gardes médicales. Cette demande première d'un accès aux prescriptions médicales à distance par la communauté médicale se complète d'une demande d'un accès

au dossier patient avec possibilité de saisie de données (compte rendu, courrier...).
Les utilisateurs se diversifient aussi le personnel d'encadrement ou technique sollicitent également un accès à distance pour leur logiciel métier (gestion, planning, maintenance...). Cette nouvelle dimension questionne l'évolution vers un nouveau rapport au travail se rapprochant du télétravail.

QUEL POSITIONNEMENT POUR LE DIRECTEUR D'ETABLISSEMENT FACE A CETTE DEMANDE DE CONNEXION A DISTANCE ?

Tout directeur d'établissement de santé est, ou va, donc être confronté à cette demande. En fonction de la maturité de l'établissement dans le développement de l'informatisation, il convient d'analyser l'impact de cette connexion sur les choix actuels ou à venir de l'architecture du système.
En s'appuyant sur la politique de sécurité des systèmes d'information et sur l'architecture de son système, il doit y apporter une réponse mais avant pouvoir :

- **Identifier le besoin actuel mais aussi futur des utilisateurs.**

Le besoin exprimé par l'utilisateur doit être objectivé au regard du besoin réel dans le cadre de la pratique professionnelle.
Il est opportun de projeter les besoins à venir dans le cadre du développement d'activité de l'établissement.
Par exemple, l'évolution des pratiques médicales vers une activité de télémédecine engendre également le questionnement de la prescription à distance. La réponse apportée va, de ce fait, impacter le développement de cette activité.

- **Délimiter le périmètre de l'accès.**

La demande doit être circonstanciée, « Pour qui ? », « Pour faire quoi ? », « Quand ? », il appartiendra de définir ensuite « Avec quoi ? ».
Il s'agit de déterminer les différentes habilitations en fonction du contexte d'utilisation en tenant compte de la réalité de l'architecture du système d'information, du respect de la législation mais aussi des contraintes de sécurité. Même si la demande est légitime, toutes les solutions ne sont pas réalisables.

Le Décret N° 2007-960 du 15 mai 2007[1] relatif à la confidentialité des informations médicales conservées sur support informatique ou transmises par voie électronique montre une volonté forte du respect de la confidentialité et les guides de la CNIL[2] établissent des préconisations en termes de sécurité de données à caractère personnel et respect du droit du patient. Il est nécessaire de formaliser une charte institutionnelle afin de clarifier pour tous les acteurs le bon usage de la connexion distance. Elle définit pour l'établissement les règles d'accès à distance et aux données médicales dans le respect de la réglementation ainsi que la liste des éléments consultables.
Cette charte est validée par le Directeur de l'établissement de santé, le président de CME, le DIM et la CME.
Pour les accès à distance par des libéraux non-salariés de l'Etablissement, le recueil du consentement du patient doit également être organisé et formalisé.

- **Mesurer l'enjeu de la réponse apportée** à cette demande sur l'investissement des acteurs dans les projets institutionnels en cours.

[1] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000466727&dateTexte=&categorieLien=id
[2] Le guide des professionnels de santé de la CNIL (2011).
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL
Le guide des données personnelles de la CNIL (2010)
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf

Il est établi que la réussite du projet d'informatisation est étroitement liée à l'adhésion des praticiens à la mise en œuvre du projet. En répondant à la possibilité de connexion sécurisée depuis l'extérieur de l'établissement, le directeur d'établissement lève un frein existant dans la communauté médicale et bénéficie d'un levier supplémentaire dans la dynamique de changement.
Elle devient un élément à prendre en compte pour intensifier l'engagement médical dans des nouveaux projets.

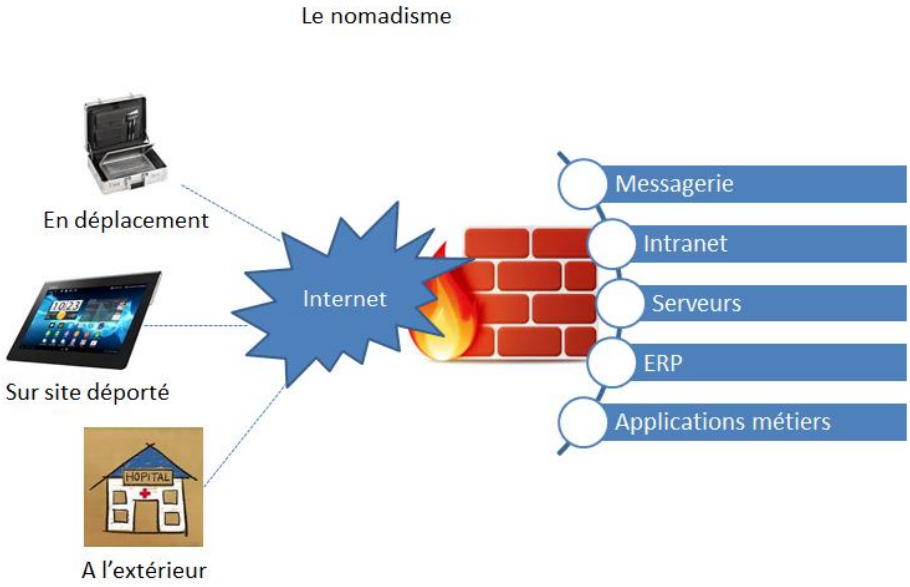
- **Appréhender l'évolution du contexte du travail.**

Si l'on pressent l'évolution du travail vers le télétravail compte tenu des possibilités de connexions à distance, il y a lieu de définir une politique de télétravail pour mettre un cadre à cet exercice.
Le télétravail est prévu et encadré par l'article 133 de la loi n° 2012-347 du 12 mars 2013 relative à l'accès à l'emploi titulaire et à l'amélioration des conditions d'emploi des agents contractuels dans la fonction publique.
Le décret reste à paraître pour préciser les conditions d'organisation du télétravail dans la fonction publique. Le télétravail n'est qu'à ses prémisses dans la fonction publique mais son émergence signe une évolution incontournable à prendre en compte dans les futurs projets d'établissement.

QUEL POSITIONNEMENT POUR LE DSIO/RSSI ?

Pour répondre à une demande de connexion à distance, le DSIO/RSSI doit pouvoir garantir à la fois la sécurité du système mais également la démarche qualité dans cette mise en œuvre.

- **Prendre en compte l'intérêt de donner l'accès à distance aux professionnels** devant la diversité des activités de la communauté médicale.



- **Assurer une sécurité optimale d'accès au SI garantit dans les différentes fonctionnalités de la solution.**
    - **Facilité d'utilisation :**

Un simple navigateur web suffit pour s'interfacer avec les applications requises sur un site central à partir d'Internet.

- **Simplicité à déployer :**

Pas d'intervention sur le terminal utilisé hormis l'éventuelle présence du client applicatif associé au serveur distant.

- **Flexibilité :**

La mise à disposition des ressources s'adapte dynamiquement aux règles d'accès répertoriées (profil de l'utilisateur, date/heure d'accès, mode d'authentification, type et intégrité du terminal…).

- **Contrôle :**

Capture/enregistrement des flux de sessions pour certains accès règlementés (Citrix, Applidis, TSE, VNC,…).

- **Sécurisation forte :**

Construite autour d'une topologie d'accès "à double SAS de sécurité". Cette solution interdit toute tentative de connexion directe aux ressources internes de l'entreprise depuis Internet.

- **Compatibilité SmartPhone/IPhone :**

La solution VPN SSL sécurise les connexions de synchronisation pour Smartphone et IPhone.

- **Garantir les bonnes pratiques pour la mise en œuvre d'une connexion distante.**

1. Formaliser une charte du bon usage des ressources du système d'information expliquant les modalités d'utilisation des accès distants en référence à la PGSSI[3]. Décrire les modalités d'utilisation et d'assistance aux utilisateurs itinérants.
2. Privilégier une solution VPN (SSL) utilisant un client VPN HTML5 (pas d'installation initiale sur le poste local).
3. Virtualiser les applications cibles (Citrix, applidis, TSE...) afin de garantir des temps de réponses corrects, éviter le risque de time out avec les applications dites « Lourdes ».
4. Garantir des liaisons réseaux de qualité (> 3G).
5. Mettre à disposition un client VPN basé sur une technologie HTML 5 évitant tout stockage d'information sur le poste client (personnel ou professionnel. Cette solution garantit l'indépendance de la plateforme.
6. Contrôler l'utilisation des accès à distance par les professionnels de santé.

- **Analyser le contexte afin de valider la faisabilité de ce projet.**

Cette demande fait l'objet d'un certain nombre de questionnement :

- Tout d'abord, ce type de connexion est-il autorisé au niveau de la politique de sécurité du système d'information (PSSI pré requis hôpital numérique) ?
- Si oui, permet-elle la connexion à distance et avec l'usage de quel matériel ?

Il est nécessaire de porter une attention particulière à la sécurité dans ces choix de matériel.

→ Matériel personnel, BYOD (Bring your own device) /« AVEC »)

On retiendra que c'est une solution efficace et sécurisée ne nécessitant pas de paramétrage tech-

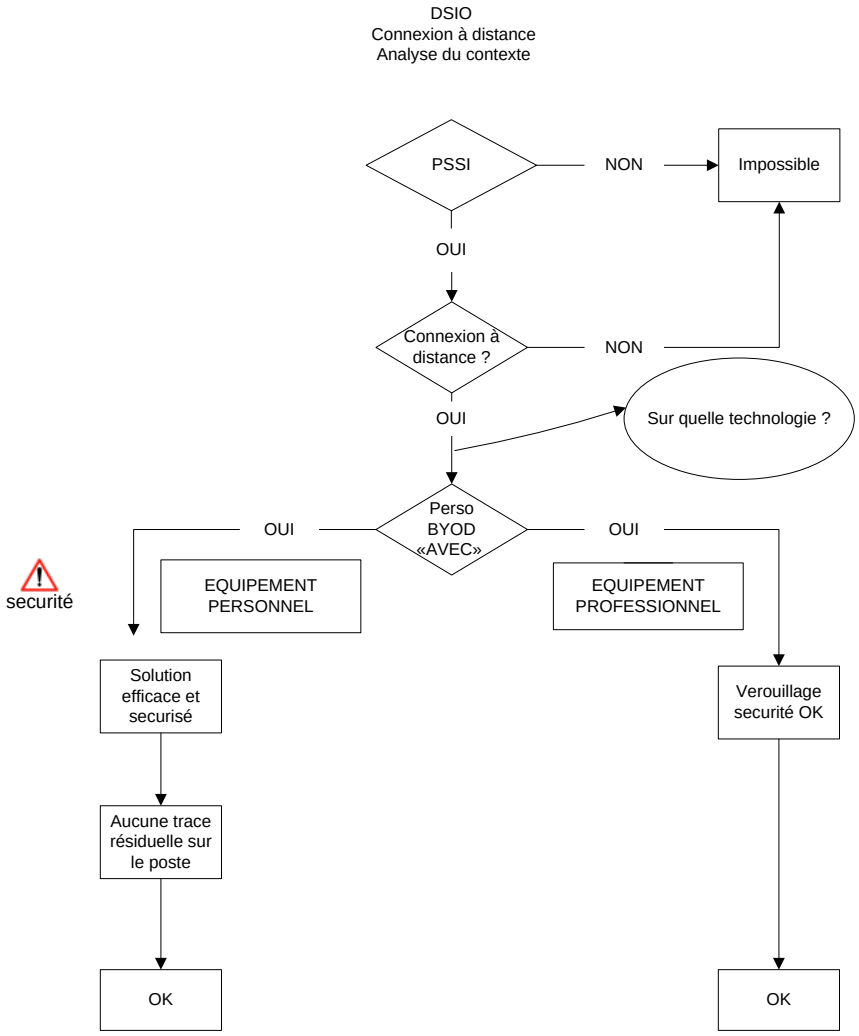
[3] La Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI). (Juillet 2013) http://esante.gouv.fr/sites/default/files/Principes_Fondateurs_PGSSI.pdf

nique de l'utilisateur. Il faut par contre se garantir qu'aucune trace résiduelle ne reste sur le poste personnel utilisé lors de la connexion.

→ Matériel professionnel

Cette solution présente un très bon niveau de sécurité car c'est une solution verrouillée. Ce choix entraine par contre une multiplicité des postes dédiés d'où une incidence financière à prendre en compte.

Le schéma ci-dessous reprend les questionnements préalables à la mise en place d'une connexion à distance :



- **Prendre en compte en compte les délais de temps réponse aux applications dans le cadre de la connexion à distance.**

1. Délais dépendants de la liaison informatique :

Liaisons informatiques	
Personnel	**Professionnel**
	Haut débit (fibre optique)
ADSL (box)	ADSL
3G	3G
4G	4G

2. Délais dépendants de la mise disposition du client :
   - Lourd (localisation sur le poste)
   - Virtualisé

3. Délais dépendants de la conjonction de la liaison et de l'installation

Liaison / Type de client	3G	4G	ADSL (box)	Haut débit (Fibre optique)
Client Lourd	NOK	OK /NOK (suivant débit)	OK	OK
Client Leger	OK	OK	Ok	OK

L'analyse de ces différents éléments techniques permet d'identifier la faisabilité et la qualité de l'accès à distance proposé. Elle objective auprès des utilisateurs la réponse proposée.

- **Définir les modalités de connexion à distance.**

Identification fiable et contrôle des habilitations et droits d'accès

Dans la PGSSI, il est énoncé l'exigence d'une identification fiable des acteurs dans les principes de sécurité (5.3.5 Maitrise des accès) ainsi que le contrôle des habilitations et des droits d'accès.

La sécurisation de l'accès à distance doit être garantie par l'utilisation d'un portail VPN (Virtual Private Network ou Réseau privé virtualisé) utilisant un protocole SSL (Secure Sockets Layer)

- en client Lourd, installation du VPN sur le poste de travail.
- en accès WEB par un navigateur à une connexion à un portail sécurisé. Cette solution permettant la mobilité.
- par l'utilisation d'un authentifieur « Token » USB qui gère les certificats numériques nécessaire à la connexion garantissant ainsi la sécurité de la connexion.

Il faut que le professionnel utilise une connexion cryptée (chiffrement) puisqu'il s'agit de données de santé à caractère personnel.

Les cartes d'authentification fortes (carte de service, CPS, CPE) devraient donc être la cible pour garantir la sécurité et la confidentialité de la connexion. A ce jour, cette cible est accessible en intra établissement mais dès lors que l'on est contraint de mettre à disposition des lecteurs de carte à puce individuelle au personnel itinérant, nous sommes confrontés, de fait, à un écueil technique de compatibilité avec les matériels personnels divers et variés.

L'authentification est possible par carte sur les équipements professionnels mis à disposition par la structure et par utilisateur/mot de passe pour les équipements personnels.

CONCLUSION

Après le déploiement du DPI en intra, la gestion des accès est élargie à l'extérieur des établissements. La demande de connexion à distance par la communauté médicale est légitime mais elle doit être encadrée dans son exercice.
Une étude de faisabilité tenant compte des besoins réels, de l'architecture du système et de la politique de sécurité est un préalable à cette mise en place.
La procédure de connexion à distance, validée au niveau des instances de l'établissement doit être connue de tous les acteurs.
Le type de connexion retenu doit permettre le maximum de garantie tant pour la confidentialité que pour la sécurité du système.