NOTE D'AUDITION

Cybersécurité dans les établissements de santé

Cour des Comptes - vendredi 3 mai 2024

France Assos Santé
La voix des usagers

Mai 2024

Perception de France-assos-santé sur la sécurité informatique des hôpitaux (publics, privés à but lucratif, privés à but non lucratif).

Notre association constate d'une part que la perception par les usagers du système de santé de la cybersécurité reste très éloignée des réalités. D'un point de vue général, il convient de rappeler que les patients voient ce sujet, au même titre que l'ensemble des sujets ayant trait au numérique, comme un champ assez opaque. Il est difficile aujourd'hui pour la population générale de voir plus loin que les clichés véhiculés par l'imaginaire collectif et les œuvres de fiction. Celles-ci mettent en avant à outrance les attaques géopolitiques et des guerres ultra-technologiques, quand la réalité est beaucoup plus triviale.

Au-delà de ce premier point de référence, qui est donc assez trompeur, **les usagers identifient mal les conséquences liées à une cyberattaque**. C'est particulièrement vrai concernant les fuites de données en tant que telles mais aussi concernant l'impact direct sur les établissements.

- Dans le premier cas, **les risques associés par les usagers autour des fuites de données, qui sont des risques individuels**, sont en premier lieu une utilisation malveillante par des acteurs privés qui dans le domaine de la santé cristallisent régulièrement des craintes. Il s'agit des banques et des assurances (peur d'exclusion de garantie, refus de prêts immobilier, augmentation de cotisation, etc.) et des employeurs (peur de licenciement abusif, discrimination à l'embauche, etc.). Evidemment le cadre juridique en France et même en Europe est protecteur pour les usagers concernant ces éventuels risques, et rien ne vient fonder à ce jour d'inquiétudes sur les potentiels accès et utilisations d'informations issues de fuites de données par ces acteurs. Les listes d'information sur le « dark-web » ne sont pas achetées et ratissées par les banques et assureurs pour passer au crible leur clientèle.

- Dans le second cas, **les conséquences sur l'établissement sont souvent inconnues pour les usagers**. A l'exception des incidents importants qui nécessitent la fermeture du service des urgences comme on a pu le voir dans certains cas. Ces fermetures sont souvent médiatisées, autant par sensationnalisme par les médias que par nécessité de rediriger les flux de patients vers d'autres services sanitaires appropriés.

Du point de vue des associations de patients et d'usagers de la santé, et notamment des représentants des usagers qui sont présents dans les gouvernances des établissements la perception de la cybersécurité est différente. Si ces personnes et organisations sont aussi pour la plupart concernées par les idées fausses détaillées plus haut concernant les risques individuels, elles portent une perspective complémentaire. **Dans le prolongement de l'engagement des représentants d'usagers pour l'amélioration continue de la qualité et de la sécurité des soins dans les établissements, ils considèrent que le risque zéro n'existe pas** et qu'il ne fait pas clouer au pilori les établissements victimes d'incidents.

Si les communautés associatives **ne souhaitent pas verser dans le « name and shame » (nommer et couvrir de honte) avec les établissements de santé, elles demandent tout de même des gages.**
Avant tout que tous les meilleurs efforts soient faits pour éviter l'arrivée d'un incident, ce qui nécessite des **moyens financiers et humains à la hauteur, et qu'une politique de crise efficace soit mise en œuvre**. Celle-ci doit autant concerner la réaction pendant un incident quand celui-ci survient, que dans l'adoption d'**un plan d'amélioration continu de la réponse cyber dans l'établissement.**

Si les enjeux d'infrastructures numériques ne sont pas accessibles en compréhension à la grande majorité des usagers et associations, c'est aussi le cas des soignants et des équipes administratives. Il nous est alors difficile de nous prononcer concernant les standards à adopter ou les moyens adéquats nécessaires.

Cependant, nous identifions bien les enjeux liés aux professionnels de santé :

- **Dans l'adaptation de l'organisation des soins pendant une crise cyber** qui paralyse des services de l'établissement, et éviter les effets indésirables graves qui en découlent : erreur d'administration médicamenteuse en l'absence d'accès au dossier patient, etc.
- **Dans la diminution des failles humaines qui sont à l'origine de la plus grande part des incident**s, nécessitant sensibilisation et formation des équipes pour diminuer les risques : utilisation de services numériques non approuvés, pièces-jointes et liens vérolés, etc.

Il faut cependant noter que **la recrudescence de fuites de données massives** dans le secteur des entreprises privées (fichiers clients) et des acteurs ou agences et services publiques (Pôle Emploi / France Travail et Caisse des Allocations Familiales en tête, organismes de tiers-payant, etc.) **présente un risque en termes d'opinion publique.**
La masse de données concernées chez des acteurs de confiance, sans rapport avec les établissements de santé, pourrait être à même de modifier le rapport des usagers avec les incidents cyber en établissements. **La relative indulgence des usagers envers les établissements qui les soignent pourrait être rapidement écornée si les services publics continuent d'être des passoires numériques.**

Concernant la typologie des établissements, nous n'avons pas à ce stade documenté de différence d'investissements et de moyens consacrés à la réponse cyber. Cependant nous rejoignons le constat fait par un certain nombre d'acteur concernant **la compétition entre les secteurs et établissements pour le recrutement de compétences dédiées à la cybersécurité.**

En ce sens, **les établissements publics subissent une double concurrence** alors que ces profils sont limités en nombre et très recherchés :

- Avec les établissements privés qui bénéficient de grilles et offres salariales plus intéressantes.
- Avec les autres secteurs d'activité, hors santé (entreprise des technologies, etc.), qui offrent des opportunités de carrière et salariales elles aussi plus compétitives.
-

Il serait à ce titre intéressant de **comparer les niveaux d'investissements et de budgets alloués par les différents établissements** (recommandations entre 5 et 10% du budget des systèmes d'information) en différenciant les infrastructures et les ressources humaines et en étudiant l'impact de la mutualisation de moyens qui ne doit pas être un prétexte au sous-investissement.

De manière générale, notre association note **une montée en puissance des acteurs publics et de leur accompagnement auprès des établissement**s, notamment au travers des GRADeS, de l'ANSSI et du programme CARE porté par le ministère de la santé / Agence du numérique en santé. Elle est associée à une prise de conscience importante, **constatée dans les programmes d'action des établissements et par nos représentants des usagers** et à une structuration croissante des réseaux informels de compétence pour mutualiser les expertises (Club RSSI, etc.). En quelques années, la cybersécurité est passée au sein des établissements d'un risque négligeable facile à cacher à un risque pris à bras le corps par tous les acteurs, au bénéfice de l'amélioration de la gestion de ces risques, nécessaire face à l'explosion de l'exposition numérique de nos hôpitaux.

Le récent appel à financement du programme ministériel CARE a en quelques semaine rempli ses objectifs avec plus de 1200 établissements (et la totalité des Groupements hospitaliers de territoire) qui ont candidaté à sa première vague soit 84% des établissements éligibles. Si on peut se féliciter de l'intérêt porté par les établissements pour cette initiative, mais 98,8% du budget pour cette première mouture déjà virtuellement engagé si toutes les candidatures sont validées. Si le dimensionnement du financement est donc plutôt conforme au volume du secteur, la marge de manœuvre est courte. Nous pouvons donc nous interroger sur **la pérennité de ces financements qui ne doivent pas être des coups d'épée dans l'eau**. Le déblocage de fonds dédiés pour répondre à l'urgence de la dette technologique, humaine et organisationnelle dans la cyber est essentielle mais ne résoudra pas sur le long terme tous les enjeux budgétaires. L'engouement des établissements traduit cette urgence, même si 1 établissement éligible sur 6 n'a pas porté sa candidature, et déjà les enveloppes sont dépensées potentiellement en totalité.

Actions de France Asso Santé en matière de sensibilisation des usagers à la protection / sécurisation de leurs données de santé.

France Assos Santé a fait de la cybersécurité **un axe de travail majeur, en l'intégrant notamment dans ses 3 priorités pour sa feuille de route numérique en santé 2024**. Conformément à nos actions auprès des communautés associatives, nous avons intégré la cybersécurité dans nos différentes activités :

- **De formation :** item abordé au sein de l'atelier « comprendre les enjeux de la e-santé », au catalogue de formation depuis 2023. Cet atelier de 2h en ligne touche 200 représentants des usagers sur la période 2023-2024, avec 13 sessions organisées auprès de 10 délégations régionales France Assos Santé.

- **De sensibilisation :** avec la mise à disposition de ressources pédagogiques sous format de poste et fiches vulgarisées à destination du réseau associatif et du grand public sur la cybersécurité en établissement de santé et sur les mesures de protection des données partagées, à l'occasion de la journée européenne de la protection des données de santé en 2023 et 2024. Organisation d'ateliers de sensibilisation avec des partenaires externes sous format de « serious-game » avec des représentants des usagers en établissement, reprenant les enjeux organisationnels, budgétaires, humains, temporels et techniques de la réponse cyber.

- **D'alerte :** Via la publication d'articles sur notre site internet, par exemple lors de la circulation d'arnaques / tentatives de hameçonnage se faisant passer pour France Assos Santé, ou lors de la fuite de données majeures, par exemple celle qui a impacté les organismes gestionnaires de tiers-payant (Viamedis, Almerys) en février 2024.

Le message de sensibilisation principal que nous portons auprès des usagers est de **rappeler quels sont les risques réels qu'ils encourent en conséquence à une cyberattaque dans un établissement où ils sont ou ont été pris en charge**. L'objectif étant de contribuer à leur faire **adopter les bons réflexes pour se prémunir des risques individuels et pouvoir réagir en cas de problème**. Nous avons concentré notre discours sur le hameçonnage qui représente un mode opératoire très répandu pour cibler les individus, et dont les tentatives peuvent être alimentées par l'apport de données personnelles issues de fuite de données en établissement de santé (contact à jour, téléphone, adresse, numéro de sécurité sociale, etc.).

Les usurpations d'identité sont aussi un risque réel pour les usagers bien que l'impact de la vente de jeux de données identifiantes massifs sur le « dark-web » ne soit pas bien étudié. En particulier au cœur des craintes des usagers la circulation de leur numéro de sécurité sociale qui s'est multipliée avec les fuites récentes concernant services publics, gestionnaire de tiers-payant et établissements de santé. En ce sens, l'action des associations est difficile car les risques sont complexes à évaluer, pour les usagers ces menaces sont difficiles à identifier et l'accompagnement est technique. **Le développement d'une offre de plus en plus pédagogique et didactique pour l'exercice des droits via Cybermalveillance.gouv.fr est facilitante pour les usagers.**

Nous tenons donc à rappeler que les risques suite à une fuite de données sont, à ce jour, de cet ordre plutôt que sur une utilisation malveillante des données à caractère médical. Ces utilisations ne sont cependant pas à exclure. Elles comprennent non pas un risque direct via les assureurs et banques comme souvent imaginé par les usagers, mais un **risque de tentative d'atteinte réputationnelle ou de chantage.** Dans ce cas, les attaques peuvent passer par l'employeur, la famille ou l'individu lui-même. Cependant des données complémentaires sont nécessaires pour pouvoir réaliser ces arnaques et elles ne peuvent pas être automatiquement massifiées au contraire du hameçonnage. Le développement de l'intelligence artificielle générative représente cependant un risque important à court et moyen terme pour faciliter la densification de ces modes opératoire.

Si on peut noter que les informations médicales sont mieux protégées dans les établissements que les informations de contact, utilisées dans la très grande majorité des utilisation malveillantes à ce jour, les usagers méritent et réclament que l'ensemble de leurs données bénéficient d'une protection maximale. **La protection de la vie privée et du secret médical ne peut pas être bradée. Les risques qui pèsent sur les individus ne vont cesser de croitre avec la multiplication des incidents et fuites de données, touchant les établissements de santé et de nombreux acteurs y compris services publics.**

Les risques à moyen et plus long termes concernant les données de santé déjà disponibles sur le « dark-web » sont incertains et ne doivent pas être négligés. Cette crainte existe aussi bien pour les acteurs malveillants traditionnels que pour des acteurs économiques privés qui pourraient en faire un usage délétère. Concernant ce risque d'utilisation par des entreprises, l'étude fine des risques et une surveillance publique concernant ces usages seraient pertinentes pour mitiger les risques encourus par les usagers et consolider la confiance de ceux-ci.

Protéger les données des usagers aujourd'hui c'est les protéger demain de risques que nous n'avons pas anticipé. Le principe de précaution doit donc aussi presser une politique nationale ambitieuse et dotée de moyens adéquats et dédiés aux enjeux du monde de la santé alors que les établissements de santé sont soumis à une tension financière et organisationnelle croissante.

Modalités de participation et de formation des représentants des usagers aux enjeux de cybersécurité dans les établissements de santé. Participation ou information de France-assos-santé aux retours d'expérience d'attaques/d'exercices cyber sur des hôpitaux.

Participation des représentants des usagers :
France Assos Santé a fait de **la participation des représentants des usagers un axe majeur de plaidoyer dans le champ de la cybersécurité**. Fort de l'expérience des quelques milliers de représentants au sein des établissements de santé dont une des motivations principales est de **contribuer à l'amélioration continue de la qualité et sécurité des soins**, il nous semble essentiel d'appliquer la même démarche concernant les enjeux de la cybersécurité.
L'expérience et le vécu des usagers sont portés par les représentants des usagers au sens collectif du terme. Ils sont formés (formation socle obligatoire de 3 jours) à dépasser leur expérience personnelle ou les considérations de leur association pour porter une dimension collective dans leurs travaux. Cela donne une légitimité au « droit à la parole » qui leur est accordé par la loi de 2002 sur la démocratie sanitaire et leur donne l'assise nécessaire pour œuvrer pour l'intérêt commun des usagers.

Nous avons identifié plusieurs points d'action dans l'organisation de la réponse cyber pour lesquels la participation des représentants des usagers est pertinente :

- **La sensibilisation des gouvernances :**

Les représentants des usagers ont à cœur de voir mis en œuvre des politiques et programme ambitieux de cybersécurité. Si le risque zéro n'existe pas, ils sont là pour rappeler que tous les meilleurs efforts doivent être déployés et peuvent donc alerter les gouvernances quand ils jugent que l'établissement ne mets pas suffisamment de moyens en ce sens. Les représentants des usagers peuvent dans ce cas notamment se faire le relai des enjeux portés par les RSSI ou DSI. Le rôle des établissements dans la sensibilisation des usagers doit aussi se renforcer comme pour d'autres messages (antibio-résistance, épidémies, etc.) et accompagner les modalités d'information comme l'envoi de modèle lettre-plainte qui laisse souvent les usagers assez démunis. Les représentants des usagers sont donc aussi là pour rappeler ces besoins.

- **La sensibilisation des équipes médicales et administratives :**

En rappelant les risques individuels qui pèsent sur les usagers les représentants des usagers peuvent renforcer la responsabilisation des équipes. En s'appuyant notamment sur l'impact sur les usagers en cas de fuite de donnée et sur les risques pour les patients hospitalisés quand les services de soins sont touchés lors d'un incident cyber. **C'est un élément déterminant car les failles humaines des équipes médicales et administratives sont une des vulnérabilités les plus répandues et pourtant facilement évitable.**

Les représentants des usagers peuvent contribuer à ce que les actions de sensibilisation et de formation sur la gestion des risques numériques soient efficaces et prises au sérieux par les équipes. La participation de représentants des usagers aux cotés de membres des équipes et de la gouvernance à des séances de sensibilisation type « serious-game » reprenant les enjeux organisationnels, budgétaires, humains, temporels et techniques de la réponse cyber nous parait une action pertinente. Avec l'objectif d**'améliorer les représentations de chacun concernant les rôles des différents acteurs et les divers impacts les touchants**. In fine, cela permettrait d'aborder des éléments nouveaux pour enrichir l'adaptation des plans de gestion de crise au croisement des différentes perspectives.

- **La participation aux exercices de crise :**

De plus en plus d'établissements organisent des exercices de crise sous l'impulsion gouvernementale (indicateur 15-3 de la feuille de route ministérielle du numérique en santé). Les représentants des usagers peuvent contribuer à ces exercices de crise dont un des objectifs et de pouvoir croiser les perspectives et réalités des différents acteurs d'un établissement avec les actions et procédures prévues au décours d'un incident cyber. A ce titre, les représentants des usagers peuvent apporter leur expertise concernant l'organisation des services et des parcours des patients pour compléter le panorama dressé. Leur connaissance transversale de l'établissement peut être un atout lors de la réalisation de ces exercices et dans les suites données. **Cette recommandation s'appuie sur l'expérience réussie de représentants des usagers dans divers établissements.**

Différents niveaux de participation peuvent être envisagés dans le cadre des exercices de crise :

- **En tant qu'observateur :** pour être dans un premier temps correctement identifié par les acteurs au sein de l'établissements impliqués dans la réponse cyber qui sont peu en contact avec eux habituellement. C'est une opportunité pertinente pour que les représentants des usagers s'approprient de lanière plus concrète les enjeux d'organisation de la réponse cyber et surtout mieux comprendre ce qui est mis en œuvre dans l'établissement.
- **En tant que contributeur :** si les représentants des usagers n'ont bien entendu pas de responsabilité dans la gestion d'un incident cyber, leurs apports lors des échanges pendant un exercice de crise peuvent être pertinents. En particulier pour compléter la vision de l'impact sur les soins d'un incident et la gestion des patients de l'établissement et pour la transposition des enseignements de l'exercice de crise en recommandations pour améliorer la politique de gestions des risques numériques.

- **La participation à la rédaction des documents de gestion de crise cyber:**

Les représentants des usagers peuvent contribuer à travers leurs perspectives à améliorer les chapitres ou parties des documents suivants
-Plan blanc
-Plans de reprise et de continuité d'activité
-Analyse d'impact sur la protection des données

Les représentants des usagers n'apportent pas d'expertise juridique, technique ou éthique, mais contribuent à rappeler l'importance de prendre en compte la réalité des usagers et d'éclairer lors de la rédaction de ces documents les angles morts éventuels en particulier concernant l'information des usagers pendant et après un incident cyber.

- **Retours d'expérience organisé à destination de la CDU :**

En complément de l'utile contribution du développement de la méthode « patient-traceur » suite à un incident détaillée plus haut nous recommandons que les représentants des usagers et la Commission des Usagers au sein des établissements bénéficient d'une présentation dédiée des retours d'expérience réalisés. Ceux-ci devraient **intégrer des dimensions spécifiques concernant la gestion des effets indésirables graves potentiels liés à l'incident cyber et à l'information adressée aux usagers** en lien avec les avancées des enquêtes pour déterminer le périmètre des données éventuellement compromises (volées, supprimées, modifiées).

- **Discussions et travaux avec la CDU :**

la CDU pourrait être saisie de s'exprimer et de **rendre un avis concernant la politique de gestion des risques** mise en place, sur les efforts déployés pour l'amélioration de cette politique et sur les ajustements nécessaires lors de la révision des différents plans de gestion de crise. Cela nécessite qu'elle soit en possession des informations sur le sujet, avec une transparence et complétude satisfaisantes.

- **Retours d'expérience des représentants des usagers :**

France Assos Santé **collecte des retours d'expérience auprès des représentants des usagers dans les établissements touchés par des incidents moyens à majeurs** afin de documenter leur intégration dans la réponse cyber. L'accent est mis sur l'information des usagers et sur la communication transparente de l'impact de l'attaque cyber.

- **Formation des représentants des usagers :**

Les enjeux de cybersécurité ont été sélectionnés pour l'ouverture d'u**n nouveau module au catalogue de formation de France Assos Santé pour l'année 2025**. Il sera destiné aux représentants des usagers exerçant un mandat en établissement de santé (sanitaire en priorité mais aussi ouvert au médico-social).

Ce module aura pour vocation de compléter l'offre actuelle et les modules existants suivants : "Améliorer la qualité en établissement de santé" et "Renforcer la sécurité du patient" et prolongera les aspects généraux abordés dans le guide France Assos Santé « Guide du représentant des usagers en établissement de santé » concernant l'amélioration de la gestion des risques et des effets indésirables graves en établissement.

Les objectifs pédagogiques seront centrés sur **la montée en connaissance des représentants sur les risques cyber dans un établissement et les modalités de mise en œuvre de la réponse cyber lors d'un incident et des actions d'amélioration continue de la réponse cyber.** Il sera attendu des apprenants de pouvoir à l'issue de la formation adopter une posture adéquate dans leur établissement pour pouvoir participer de manière constructive au sein de l'établissement aux actions sur la cybersécurité.

Des séances de sensibilisation sont aussi organisées par le siège sur demande des équipes régionales France Assos Santé pour apporter des éléments de formation et réflexion auprès des commissions dédiées à la e-santé en région ou des représentants en charge des relations et partenariats avec la gouvernance régionale du numérique en santé notamment les GRADeS.

Information des patients sur la sécurité informatique des hôpitaux en termes de continuité et de qualité des soins.

En dehors des incidents ayant entrainé la fermeture de services d'urgence, l'impact d'incidents sur la continuité des soins a été peu observé. Pourtant, l'impact de ces incidents a le potentiel de :

- **Générer des événements indésirables graves** dus à l'indisponibilité du dossier médical, l'indisponibilité de certain matériel nécessaire, qui peuvent entrainer des erreurs d'administration médicamenteuses ou exiger des transferts de patients critiques, sources de complications.

- **Entrainer un déséquilibre concernant l'accès aux soins dans le bassin de vie**, notamment quand les urgences sont impactées ou certains services spécialisés en tension. Cet axe est cependant trop peu étudié, et il serait pertinent que des analyses en conséquence soient diligentées et puissent alimenter les travaux d'instances de démocratie en santé territoriales comme les Conseils Territoriaux de Santé ou les Conférence Régionales Santé Autonomie, en sus des instances de l'établissement. **La question du renoncement au soin et de ses conséquences doit ainsi se poser à ces différentes instances,** suite aux comportements d'accès à la santé observés au cours de certains incidents importants.

Les attaques majeures, avec fermeture de services, encouragent les usagers à décaler leur prise de rendez-vous (manque de confiance dans l'établissement, retard diagnostic en attendant un autre rendez-vous ailleurs ou en évitant les urgences, etc.).

Dans les deux cas l'information des usagers reste très lacunaire, autant pendant un incident qu'après concernant l'impact sur les services qui peut perdurer pendant plusieurs mois voire plus d'une année. **Cette information n'est d'ailleurs pas évoquée lors des exercices de crise**, comme nous le rapportent les représentants des usagers qui y participent. L'information sur le déport des usagers sur d'autres modalités d'accès aux soins doit être plus transparente et pas seulement abordée par les médias locaux qui apportent en général peu de solutions concrètes. **Pourtant la lisibilité du système de santé pour l'accès aux soins, en particulier les soins non-programmés, est une difficulté constante, aggravée dans ces cas.**

Association de France-assos-santé, soit au niveau national soit au niveau local, à la politique de sécurité informatique des hôpitaux et de protection des données de santé.

France Assos Santé s'associe en particulier à l'échelle régionale aux politiques de sécurité informatique des hôpitaux et de protection des données de santé. Nos 18 délégations régionales entretiennent des liens étroits avec la gouvernance régionale du numérique en santé. Elles assurent aussi le suivi direct de l'activité des représentants des usagers dans les établissements pour leur proposer un accompagnement adapté avec le support du siège. **A ce titre l'association est donc en lien avec les GRADeS**, et les échanges sur les enjeux de la cybersécurité sont de plus en plus fréquent. Notre association a par ailleurs été invitée à intervenir lors des 3 dernières éditions du **Cybercamp Santé,** dont 2 fois en qualité de grand témoin. Nous avons pu être associé à des travaux et réflexion au sein de la **Task Force Cyber du porgramme CARE dans le champ de la sensibilisatio**n des gouvernances.

L'association a donc œuvré pour construire sa légitimité pour être un interlocuteur d'intérêt, et ainsi préparer la mise en action de notre feuille de route pour favoriser la participation des représentants des usagers dans les établissements.

Les représentants des usagers contribuent aussi de manière ponctuelle, sur la base des ressources proposées par l'association aux politiques de gestion des données de santé en particulier liées à l'utilisation d'outils comme Mon Espace Santé ou le Dossier Patient Informatisé de l'établissement. France Assos Santé échange régulièrement avec la Délégation ministérielle du Numérique en Santé, la Caisse Nationale d'Assurance Maladie et la Commission Nationale Informatique et Liberté sur ces enjeux. **Avec la massification des interventions des représentants des usagers et le portage d'un plaidoyer national, nous souhaitons continuer de consolider nos travaux avec ces acteurs et d'autres partenaires sur les enjeux spécifiques de la cybersécurité.**

Perception de France Assos Santé sur la démarche de « patient-traceur » de la HAS appliquée aux enjeux de circulation et de protection des données de santé des patients.

La méthode de « patient-traceur » est utilisée dans le cadre de la certification des établissements comme méthode d'évaluation des critères définis par la HAS, mais peut aussi être utilisée en dehors dans une démarche d'auto-évaluation et amélioration continue de la qualité. **Cette démarche est essentielle car elle est la seule qui permet de prendre en compte le vécu des malades à travers leur récit, à croiser avec les expériences des équipes (soignantes et administratives)**. La méthode nécessite de recruter des patients dont le passage dans l'établissement est compatible avec cette évaluation en termes de temporalité. Le passage ne peut pas être trop éloigné dans le temps, et ce délai idéal n'est pas nécessairement le même entre tous les services, par exemple entre un service d'urgence et un service qui accueille des patients chroniques en cancérologie. Pour examiner la pertinence de la méthode de « patient-traceur » il faut déterminer les indicateurs à évaluer grâce à cette méthode :

Dans le champ de la gestion des risques numériques, les critères de la HAS (en particulier **le Critère 3.6-02 « Les risques de sécurité numérique sont maîtrisés »**) se concentrent sur la mise en place d'une gouvernance et de programmes d'actions et de formation, qui sont invisibles pour le patient au décours de sa prise en soins. **Ils ne nous semblent donc pas se prêter à l'utilisation de la méthode du « patient-traceur** », pour différentes raisons :

- **Difficulté à intégrer des patients ayant eu une expérience récente** liée à un incident cyber au sein de l'établissement, l'établissement n'ayant lui-même pas forcément été concerné directement.
- **Peu de critères de certification** reposant sur la prise en charge du patient, et **dont il pourrait alors se faire témoin.**

On peut noter que d'autres critères pourraient éventuellement se prêter davantage à l'exercice, par exemple :
Le critère 1.1-18 « Le patient reçoit une information claire et adaptée à son degré de discernement sur les modalités de sa prise en charge » et l'item « Le patient sait qu'il ne doit pas échanger avec l'équipe médicale via une messagerie non sécurisée. ». Pour lequel la méthode du « patient-traceur » est déjà identifiée pour l'évaluation dans le guide de la HAS. A ce titre les usages numériques des usagers peuvent représenter des vulnérabilités supplémentaires, et les éviter contribue directement à la réduction des risques cyber.
Mais cela concerne des éléments qui ne reflètent qu'une part minime de la politique de gestion des risques cyber.

En revanche nous notons que **la méthode du « patient-traceur » peut tout à fait se prêter à l'évaluation de l'expérience patient et de la qualité de la gestion cyber en dehors de la démarche de certification de l'établissement. Comme le font déjà certains établissements, dans une démarche d'auto-évaluation et amélioration continue de la qualité.** Dans ce cas, il nous semble très pertinent que les établissements mettent en œuvre cette méthode d'évaluation à la suite d'un incident cyber pour compléter le retour d'expérience de gestion de crise.
En effet, en dehors du point de vue médical et administratif largement représenté dans les retours d'expérience et de la période de crise allant de la découverte de la vulnérabilité ou incident et sa résolution technique à court terme, il reste des angles morts importants. Notamment concernant les usagers et leur vécu :

- **De l'impact dans leurs soins pendant une hospitalisation**, en ciblant les services concernés par une modification d'activité.

- **De l'annonce de l'incident, lors d'un passage dans l'établissement**, par notification courrier ou courriel suite à un passage. En interrogeant la temporalité de cette notification et son contenu : fermeture de service ou annulation de prise en soins, confirmation de fuite de données, information sur les droits, modèle de lettre-plainte, etc.

Le recours à un « patient-traceur » représente **une méthode très pertinente pour compléter la documentation des retours d'expérience et placer l'amélioration de l'information des usagers aux différentes étapes de l'incident comme un sujet de travail et d'amélioration de qualité**. Si les enjeux d'amélioration sont nombreux pour les établissements, les enjeux d'infrastructures, de sensibilisation et de formation des équipes ne doivent pas occulter la dimension d'information des usagers. Notamment en se rappelant que les incidents majeurs impactent durablement les établissements qui ne recouvrent pas la totalité des leurs services numériques rapidement, les délais pouvant même aller jusqu'à un an et demi.

A propos de France Assos Santé

L'**Union nationale des associations agréées d'usagers du système de santé (UNAASS)** dite France Assos Santé a été créée en mars 2017 dans la continuité d'une mobilisation de plus de 20 ans pour construire une représentation des usagers interassociative. Organisation de référence pour défendre les intérêts des patients et des usagers du système de santé, sa mission est inscrite dans le Code de la santé publique (loi du 26 janvier 2016). Forte d'un maillage territorial de 18 délégations régionales (URAASS), **elle regroupe près de 100 associations nationales et plusieurs centaines d'associations régionales** qui agissent pour la défense des droits des malades, l'accès aux soins pour tous et la qualité du système de santé. Elle forme **les 15 000 représentants des usagers qui siègent dans les instances hospitalières, de santé publique ou d'assurance maladie**. Elle prend une part active dans le débat public et porte des propositions concrètes auprès des acteurs institutionnels et politiques pour améliorer le système de santé.

France Assos Santé

La voix des usagers

Défendre vos droits Vous représenter Agir sur les lois

Document réalisé par le service communication de France Assos Santé. Avril 2024.