CIRRNET®

patientensicherheit schweiz
sécurité des patients suisse
sicurezza dei pazienti svizzera

Quick-Alert®

N° 53

IT & ID

Confusions entre patient-e-s liées aux outils numériques

Signalements* notifiés au CIRRNET de Sécurité des patients Suisse :

Cas 1

« Je devais administrer des antalgiques en même temps à deux personnes fraîchement opérées. Pour une des patientes, j'étais sur le mauvais dossier, et elle a reçu du Tramadol au lieu de morphine. »

Cas 2

« Le problème, c'est que dans le système – surtout quand plusieurs dossiers patients sont ouverts en même temps –, c'est très facile d'être sur le mauvais dossier. Cela m'est aussi déjà arrivé, et jusqu'ici je l'ai toujours remarqué à temps. Aujourd'hui, je l'ai vu trop tard. Cela n'a pas eu de conséquences... »

Cas 3

« Nous avions simultanément dans la division deux patientes qui avaient le même schéma thérapeutique. Pour commencer le traitement, il fallait attendre la valeur de la créatinine. Peu avant midi, lorsque le résultat de la première patiente est arrivé, je n'ai pas pris garde au fait que dans le programme de prescription de la chimiothérapie, c'est le dossier de l'autre patiente ayant le même schéma qui était ouvert et j'ai inscrit le résultat de laboratoire à cet endroit. J'ai prescrit par erreur à la patiente une dose de chimio trop faible. C'est au moment où l'équipe infirmière a redemandé si elle pouvait administrer le traitement que j'ai réalisé que j'avais signé la prescription pour la fausse patiente. »

Cas 4

« Pendant la visite, j'ai voulu annoncer le patient A en radiologie. Son dossier était ouvert. À ce moment, j'ai reçu l'appel d'une ancienne patiente B, qui voulait discuter d'un problème avec moi. J'ai donc dû ouvrir son dossier. Après cette conversation, j'ai encore été interrompu deux fois par d'autres choses dont j'ai dû m'occuper. J'ai ensuite repris l'ordinateur et j'ai annoncé le patient A en radiologie... … un peu plus tard, la TRM a appelé pour me dire qu'elle attendait toujours la patiente B. J'ai alors compris que j'avais inscrit l'examen radiologique au mauvais endroit et c'est la patiente B que j'avais annoncée en radiologie. ».

Cas 5

« Contrôlé la glycémie chez le patient A et ouvert son schéma d'injection. Contrôlé l'insuline pour le patient B, et pour cela, j'ai ouvert son dossier, mais ne l'ai pas refermé. Ensuite avec une collègue, contrôlé et administré l'insuline pour le patient A. Fermé son schéma d'injection et constaté à ce moment que c'est le schéma du patient B qui avait été appliqué au patient A. »

Cas 6

« Dans une chambre à deux lits, une patiente s'est plaint de douleurs. J'avais le chariot avec l'ordinateur avec moi. Je lui ai administré les antalgiques qu'elle avait en réserve. Au bout de quelques minutes, j'ai voulu le documenter dans le dossier et j'ai remarqué à ce moment que je lui avais administré les médicaments inscrits en réserve pour sa voisine de chambre. Après un petit moment, les douleurs de la patiente avaient diminué. »

Cas 7

« Un médicament a été prescrit au mauvais patient. En vérifiant la prescription d'un autre patient, quelque chose m'a paru bizarre. J'ai demandé au médecin-assistant pour qui ce médicament était prévu. Il a alors stoppé le médicament dans le système, mais avec mon login. »

Cas 8

« L'anamnèse médicamenteuse avait été inscrite dans le système pour le mauvais patient. »

Cas 9

« Inscrit la prescription d'un antibiotique i.v. et de Solumedrol i.v. chez le mauvais patient dans le système. »

* Textes partiellement modifiés sur le plan rédactionnel pour une meilleure compréhension

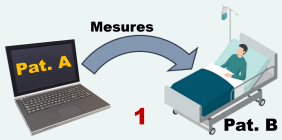
Commentaires des expert-e-s

L'établissement de dossiers informatisés dans presque tous les secteurs de la santé visait entre autres à renforcer la sécurité des patients. Malgré des améliorations incontestables, on remarque aujourd'hui encore à quel point l'emploi de ces outils peut être source de risques et de problèmes [1–4]. Comme cela a été clairement démontré, ces derniers sont notamment liés à des déficits techniques, structurels et/ou organisationnels susceptibles de rendre l'utilisation des systèmes difficile et de favoriser les erreurs humaines. L'éventail des facteurs d'influence en la matière est très large, mais les exemples cités ou observés le plus fréquemment sont les suivants :

- Manque de convivialité des systèmes
- Formations et directives lacunaires
- Dispersion des informations entre différents systèmes
- Appareils inappropriés (p. ex. écrans trop petits)
- Couverture WLAN insuffisante dans les bâtiments
- Performance et stabilité insuffisantes des réseaux
- …

Parmi les nombreux risques qui peuvent en découler figure l'utilisation erronée du mauvais dossier (confusion entre patient-e-s liée aux outils numériques). Cela peut se traduire par l'inscription de données (p. ex. prescriptions médicamenteuses) et/ou l'utilisation d'informations ne concernant pas la bonne personne, en raison de l'ouverture involontaire du mauvais dossier [5–7]. Les déclarations CIRS et les exemples de cas relatés par des collaborateurs/collaboratrices mettent en évidence quatre types principaux de confusions (fig. 1-4) :

1. Des interventions relatives aux soins, au traitement ou au diagnostic, ou encore l'administration de médicaments proviennent du mauvais dossier patient.



2. Des anamnèses, des observations, des valeurs mesurées (signes vitaux, etc.), des interventions réalisées, etc. sont documentées dans le mauvais dossier patient.

3. Des mesures, médicaments, examens, etc. sont prescrits dans le mauvais dossier patient.

4. Des données provenant d'autres systèmes informatiques (p. ex. résultats de laboratoire au format PDF) sont enregistrées dans le mauvais dossier patient.

On constate que ces erreurs se produisent aussi bien à proximité directe des patient-e-s (« bedside ») qu'à d'autres endroits (bureau de la division ou des médecins, etc.). De même, la problématique concerne tous les secteurs de prise en charge qui travaillent avec des dossiers informatisés. Selon le type d'erreurs commises dans l'enregistrement de données ou la consultation de l'information, les conséquences pour les patient-e-s peuvent être très lourdes. Il est également probable qu'un grand nombre de ces erreurs ne sont pas remarquées et on ne peut dès lors qu'émettre des hypothèses quant à leur portée effective [8].

Les déclarations CIRS ne permettent pas toujours de déterminer avec certitude les causes des erreurs. L'une d'entre elles tient sans aucun doute au fait que l'interface utilisateur des différents systèmes contient une grande quantité d'informations condensées. Les champs où figure l'identité du patient (nom, prénom, date de naissance, numéro ID) n'occupent souvent qu'une petite partie de l'écran, inférieure à dix pour cent. En outre, ces données ne se distinguent pas, graphiquement, des autres données. S'y ajoute manifestement le fait qu'une fois à leur poste de travail informatique, les collaborateurs/collaboratrices pensent généralement avoir ouvert le bon dossier patient.

Étant donné qu'il n'existe pour l'heure que très peu de recherches concrètes sur cette thématique, il est particulièrement important de prendre en compte les observations et les déclarations des collaborateurs/collaboratrices afin de dégager des constellations d'erreurs typiques.

<u>Utilisation des postes de travail IT par plusieurs personnes en alternance</u>

Généralement, plusieurs collaborateurs/collaboratrices se partagent des postes de travail IT et les utilisent en alternance. Lorsque les changements sont particulièrement fréquents, il s'ensuit une constellation d'erreurs typique. Par manque de temps, la personne qui vient d'inscrire un élément dans l'ordinateur néglige souvent de fermer sa session – comme elle devrait normalement le faire –, et celle qui l'avait précédée part de l'idée qu'à son retour, le dossier qui s'affiche est celui qu'elle avait ouvert auparavant.

L'utilisation du même login par plusieurs personnes constitue une autre constellation particulière d'erreurs, car le passage constant d'un dossier patient à l'autre augmente le risque d'erreurs.*

<u>Ouverture simultanée de plusieurs dossiers patients</u>

De plus en plus de systèmes permettent l'ouverture simultanée de plusieurs dossiers patients. Dès lors, le passage entre différents dossiers graphiquement très semblables augmente le risque d'erreurs [9].

* Indépendamment du fait que l'utilisation du même login par plusieurs personnes contrevient aux règles fondamentales de la documentation des patient-e-s, ce fonctionnement comprend des risques juridiques : si un crime ou un délit commis au sein d'une entreprise ne peut être imputé à aucune personne physique déterminée, l'entreprise peut être punie d'une amende de cinq millions de francs au plus (Code pénal, art. 102).

Utilisation de plusieurs systèmes en parallèle
À côté des dossiers patients – principale plateforme de documentation –, il existe généralement de nombreux « sous-systèmes » (logiciels d'anesthésie, de radiologie, de laboratoire, etc.). Pour consulter des informations, reporter des données, inscrire des demandes ou des prescriptions, il est souvent nécessaire d'utiliser plusieurs de ces programmes en parallèle, faute d'interfaces entre eux. Si, en outre, plusieurs dossiers patients sont ouverts en même temps dans les diverses applications, il peut facilement y avoir confusion entre les multiples fenêtres.

Erreurs dans l'utilisation des menus déroulants
La recherche manuelle de patient-e-s dans le système s'effectue en principe au moyen d'une liste déroulante prédéfinie (aperçu de la division, planification des rendez-vous, etc.), ou par le biais de fonctions de recherche, où l'on saisit le nom, la date de naissance, le numéro de cas ou d'identification du patient/de la patiente, etc. De façon générale, de telles méthodes de sélection sont sources d'erreurs. Lorsqu'on utilise les fonctions de recherche en particulier, toute une série d'occurrences s'affichent. Dès lors – le phénomène est bien connu –, on a tendance à sélectionner le premier résultat qui apparaît. S'ajoute à cela le risque de cliquer involontairement sur la mauvaise ligne.

Changement de dossier non achevé
Dans les systèmes de mauvaise qualité et/ou lorsque les performances du réseau sont insatisfaisantes, le passage d'un dossier patient à l'autre peut prendre du temps. Tant que cette procédure n'est pas achevée, il se peut que l'ouverture d'une autre interface (p. ex. aperçu de la médication) prenne le pas sur l'ordre de fermer la fenêtre précédente et que, dès lors, le dossier patient que l'on voulait fermer reste ouvert. Le changement d'affichage à l'écran peut donner faussement l'impression que le changement de dossier a bel et bien eu lieu, alors que le dossier d'origine ne s'est en réalité pas fermé.

Recommandations – L'essentiel en bref

Que peut-on faire ?

1. **Au niveau de l'utilisation (médecins, soignant-e-s, AM, TRM, etc.) :**
   - Vérifiez toujours l'ID du patient/de la patiente dans le dossier que vous venez d'ouvrir. Ce faisant, prêtez une attention particulière aux noms identiques ou similaires, utilisez au moins deux caractéristiques d'identification indépendantes et contrôlez en cas de doute.
   - Assurez-vous dans tous les cas, après une interruption ou autre événement ayant détourné votre attention, que le dossier qui s'affiche est bien celui dont vous avez besoin.
   - Fermez votre session dès que vous quittez le poste de travail IT pour empêcher que des collègues puissent traiter les dossiers que vous avez ouverts ou changer de dossier patient.
   - Évitez de travailler sur plusieurs dossiers patients en parallèle et focalisez votre attention sur la personne dont vous vous occupez sur le moment.
   - Partagez avec vos collègues votre expérience en cas de confusion entre patient-e-s liée à l'utilisation d'outils numériques, afin d'attirer leur attention sur ce risque. Rapportez ce type d'événements dans le système interne de déclaration des erreurs (p. ex. CIRS) en décrivant également les circonstances qui ont joué un rôle dans la survenue du problème.
   - Faites preuve d'ouverture face à l'introduction de nouvelles fonctions et règles de sécurité destinées à vous préserver des erreurs.
2. **Au niveau de l'institution (hôpitaux, EMS, aide et soins à domicile, cabinets médicaux, etc.) :**
   - Recueillez les déclarations d'erreurs ou d'événements indésirables concernant la confusion entre patient-e-s liée à l'utilisation d'outils numériques dans l'ensemble de votre institution, et analysez-les avec l'aide d'expert-e-s (gestion de la qualité et des risques, exploitabilité, informatique, etc.).
   - Partagez les conclusions avec le personnel afin de sensibiliser à ce risque.
   - Examinez, en coopération avec votre division informatique et les fournisseurs de logiciels, les possibilités d'amélioration en vue d'éviter des erreurs (« mesures fortes »), demandez l'introduction de telles solutions et priorisez leur mise en œuvre.
   - Formulez des directives contraignantes relatives à l'utilisation de systèmes IT cliniques qui contiennent des règles fondamentales destinées à éviter des confusions entre patient-e-s liées aux outils numériques.
3. **Au niveau de la production et du développement des logiciels (fournisseurs de logiciels, divisions IT, etc.) :**
   - Demandez activement un retour des utilisateurs/utilisatrices et des institutions sur l'exploitabilité et le design de vos produits afin de relever les constellations d'erreurs ayant conduit à des confusions entre patient-e-s liées aux outils numériques.
   - Examinez de façon proactive s'il est possible d'intégrer dans vos systèmes des fonctions permettant d'éviter des confusions entre patient-e-s liées aux outils numériques.
   - Utilisez les conclusions du design des facteurs humains et évaluez vos systèmes sous l'aspect de leur application dans la pratique.

Recommandations

Les types et constellations d'erreurs se traduisant par la confusion entre patient-e-s liée aux outils numériques montrent une telle diversité qu'il n'est pas possible de maîtriser l'entier de la problématique au moyen de mesures isolées. L'association de plusieurs approches qui se complètent l'une l'autre a bien davantage de chances de succès. L'efficacité escomptée de chacune des solutions doit constituer l'un des critères de choix.

Mesures au niveau du comportement

Il est connu que les stratégies de sécurité reposant exclusivement sur un comportement exempt d'erreurs de la part des personnes concernées sont relativement peu efficaces et n'ont pas d'effet à long terme. Il est néanmoins important d'attirer l'attention sur la problématique des confusions et leurs conséquences possibles, par exemple en instruisant les collaborateurs/collaboratrices sur les constellations typiques d'erreurs et les manières de les éviter. Il est notamment essentiel d'évoquer les répercussions que peuvent avoir des interruptions ou des distractions, de manière à sensibiliser les utilisateurs/utilisatrices à leur fréquence et à leur importance au quotidien. Ce savoir doit par ailleurs être transmis non seulement au fil de la vie professionnelle, mais à titre préparatoire durant la formation/les études déjà.

Il incombe également aux cadres d'œuvrer pour éviter les erreurs. Certes, il ne faut pas surestimer l'efficacité de la standardisation et de la réglementation et il faut garder à l'esprit que la limitation de la marge de manœuvre du personnel peut aussi comporter des désavantages. Toutefois, il est important d'attirer l'attention sur les procédures particulièrement sources d'erreurs afin de les réduire autant que possible :

- Ne jamais utiliser de comptes de groupe ou le login d'autres collaborateurs/collaboratrices pour intervenir dans les dossiers patients.
- Toujours fermer sa session lorsque l'on quitte le poste informatique (même pour une absence de courte durée).
- Ne pas ouvrir plusieurs dossiers patients simultanément dans le même système – ou en limiter le nombre.
- Ne pas utiliser alternativement ou en parallèle plusieurs programmes pour des patient-e-s.

Soutien technique – fonctions techniques

En raison des propriétés de base fonctionnelles requises pour les applications des systèmes cliniques, il est techniquement presque impossible d'exclure totalement les erreurs d'utilisation. Toutefois, des fonctions de soutien bien conçues peuvent fortement contribuer à les réduire. À première vue, l'investissement pour y parvenir semble certes très élevé. Toutefois, vu que de telles interventions ne reposent pas sur l'action d'individus ou de groupes de personnes, mais qu'elles ont un impact systémique, on peut en attendre une efficacité bien meilleure et à plus long terme. Dans une évaluation coûts-bénéfice, il faut en effet se demander s'il est vraiment judicieux d'opter pour des procédures reposant sur des méthodes potentiellement sources d'erreurs, alors que des solutions plus efficaces seraient à disposition.

Les moyens techniques mis en place doivent aider le mieux possible les collaborateurs/collaboratrices à éviter les erreurs. En les choisissant, il faut cependant tenir compte du fait que, dans de nombreuses applications, les utilisateurs/utilisatrices font déjà face à des insatisfactions, des lenteurs et des problèmes importants [1]. Si l'utilisation des logiciels est rendue plus compliquée encore par l'implémentation de mesures de précaution supplémentaires, il peut en résulter des problèmes d'acceptation, mais aussi des tentatives de contourner ces fonctions de sécurité. Il convient donc d'associer l'efficacité avec le minimum d'inconvénients en termes d'utilisation.

Nous présentons ci-après des méthodes qui permettent de réduire le risque de confusion entre patient-e-s liée au numérique grâce à l'implémentation de nouveaux logiciels, mais aussi à des adaptations apportées après coup aux configurations en place. À noter que ces solutions ont été très peu introduites jusqu'ici. Les sociétés qui développent des logiciels peuvent apporter en la matière une contribution importante si elles focalisent leurs systèmes sur les risques existants et les adaptent en conséquence. Pour leur part, les institutions qui achètent et exploitent les logiciels doivent exiger plus fermement des vendeurs de telles améliorations afin d'attirer l'attention sur ce besoin.

<u>Adaptation des interfaces utilisateur</u>
La bonne lisibilité des données relatives à l'identité des patient-e-s sur l'interface utilisateur est une condition essentielle pour améliorer la sécurité sur ce point. Dans la majorité des systèmes actuels, la surface réservée à ces éléments est toutefois très réduite et les caractères utilisés se distinguent optiquement très peu des autres saisies. Du point de vue de la planification, cela s'explique par le fait qu'à côté de l'ID, une grande quantité d'autres informations doivent trouver place sur un très petit espace. En créant le design des interfaces, les développeurs de logiciels partent en outre du principe qu'avant toute saisie, la personne a ouvert le bon dossier patient et que, dès lors, la lisibilité de l'ID est plutôt d'importance secondaire. Les collaborateurs/collaboratrices ayant également, dans la grande majorité des cas, cette certitude, la technique ne les aide pas à la remettre en question.

De nombreuses descriptions d'événements montrent au contraire à quel point cette hypothèse est éloignée de la réalité. Pour éviter les confusions entre patient-e-s liées au numérique, il convient d'accorder davantage d'importance à une meilleure lisibilité des données d'identification. Cela nécessite de leur réserver plus d'espace et d'adapter la taille des caractères, mais aussi de délimiter clairement ces champs, graphiquement, par rapport aux autres champs. L'objectif est d'attirer davantage l'attention sur ces informations afin d'accroître les chances de repérer l'éventuelle ouverture du mauvais dossier.

Aides supplémentaires à l'identification

De nombreuses déclarations CIRS le montrent : les soignant-e-s partent du principe qu'ils ont toujours ouvert le bon dossier patient, sans pour autant aller jusqu'à vérifier consciemment les données qui le confirmeraient (nom, prénom, date de naissance). De telles fautes d'inattention se produisent en particulier sous stress et en période de surcharge. Il est possible de réduire ces erreurs non seulement en améliorant la lisibilité du texte, mais aussi en ajoutant des éléments d'identification. On utilisera pour ce faire des caractères connus de tous, comme les symboles habituels indiquant le genre de la personne (♀, ♂, ⚧). Cela peut être particulièrement utile lorsque plusieurs patient-e-s portent un patronyme identique ou similaire, ou que le prénom ne permet pas d'identifier le genre avec certitude.

L'insertion de la photo des patient-e-s dans le champ réservé à l'identité s'avère encore plus efficace (fig. 5). À ce sujet, des expériences positives montrent qu'il serait judicieux d'intégrer ce paramètre [10,11]. L'enregistrement d'une photo de la personne ne peut toutefois se faire qu'avec son assentiment et dans le strict respect du but de la démarche [12]. La déclaration de consentement nécessaire n'exige cependant pas de forme particulière et peut également se faire oralement. Si la personne refuse l'intégration de sa photo, le fait doit être documenté. Des expériences de différents secteurs de prise en charge dans lesquels l'insertion d'une photo est prévue dans le système à des fins d'identification montrent un degré élevé d'acceptation, en particulier lorsque le sens et le but de la mesure ont été clairement expliqués. Ces mêmes institutions confirment en outre l'efficacité de la mesure et précisent que l'investissement nécessaire au moyen du logiciel correspondant se situe dans des limites raisonnables.

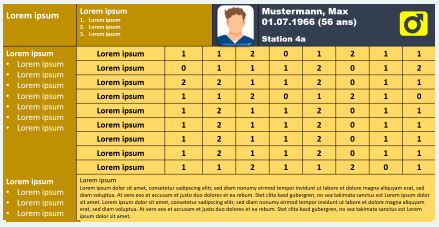


Fig. 5: Mise en évidence du champ ID sur l'interface utilisateur (image d'illustration)

Fenêtre de vérification d'ID

Une phase d'inactivité sur un logiciel IT – par exemple aucune saisie faite et aucun mouvement de souris détecté – signifie souvent que l'utilisateur/utilisatrice a été interrompu-e ou que son attention a été détournée. Il est connu que ces facteurs d'influence contribuent beaucoup à la survenue d'erreurs. De nombreuses déclarations CIRS décrivent un taux particulièrement élevé de confusions entre patient-e-s liées aux outils numériques au moment de la reprise d'une activité précédemment interrompue. C'est pourquoi il est judicieux de revérifier l'identité du patient/de la patiente au moment de reprendre cette activité. Comme il n'est pas réaliste de compter sur la seule autodiscipline des utilisateurs/utilisatrices pour le faire, des fenêtres pop-up qui, après un certain laps de temps, s'ouvrent automatiquement à la reprise de l'activité sur le système IT, peuvent jouer une importante fonction de rappel [13]. Ces fenêtres ont pour but de mettre clairement en évidence l'identité des patient-e-s afin d'éviter une confusion avant toute saisie ou utilisation des données dans le dossier. Leur application s'avère judicieuse dans différentes situations :

- Réouverture du dossier patient dans le système IT
- Reprise de l'utilisation IT après une interruption
- Changement d'utilisateur/utilisatrice (avec et sans login / logout)

Il est connu que l'effet des fenêtres pop-up comprenant des alertes est susceptible de s'atténuer assez rapidement. Le risque est alors grand d'une confirmation trop rapide et sans vérification de leur contenu. Pour obtenir une efficacité à long terme, les fenêtres doivent être configurées de façon à ce que l'identité du patient soit clairement reconnaissable, même d'un coup d'œil superficiel. Cela nécessite non seulement une police de caractères et un champ suffisamment grands, mais aussi l'insertion de symboles graphiques et, si possible, de la photo de la personne (fig. 6).

Fig. 6: Fenêtre de vérification avec mise en évidence de l'ID patient et de sa photo (image d'illustration)

Sélection assistée de patient-e-s

La sélection manuelle de patient-e-s à partir d'une liste ou de la fonction recherche est connue comme une source potentielle d'erreurs importante. Il serait donc illusoire d'espérer atteindre une sécurité absolue en la matière. Toutefois, certaines fonctions d'assistance peuvent contribuer à réduire le taux d'erreurs lors de l'ouverture des dossiers.

Des fonctions d'alerte bien conçues pourraient par exemple attirer l'attention – au moment d'ouvrir la liste déroulante déjà – sur les risques de confusion liés à des noms ayant la même orthographe ou la même consonance, dans les listes de la division ou de la clinique, les tableaux de programmes opératoires ou les planifications de rendez-vous, etc. (fig. 7). Ces fonctions devraient signaler clairement le risque, par exemple en surlignant dans la liste déroulante l'élément semblable. Jusqu'ici, ces fonctionnalités ne sont pratiquement pas implémentées dans les systèmes cliniques. Au vu de la fréquence des erreurs liées aux outils numériques, il serait bon d'étendre leur application.

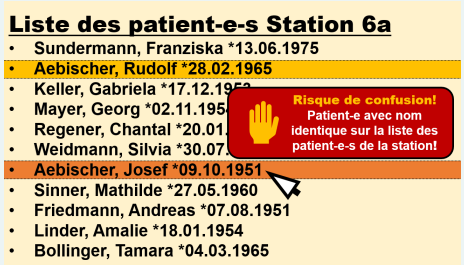


Fig. 7: Mise en garde contre une possible erreur d'identification dans la liste déroulante (image d'illustration)

Le risque d'erreurs pourrait également être abaissé par un raccourcissement des listes déroulantes. Lors d'une recherche par portion de nom, date de naissance, numéro de cas ou de patient, etc., les systèmes fournissent inutilement de nombreuses occurrences qui rendent la

Remarque : les données personnelles figurant dans le présent document sont imaginaires. Toute ressemblance avec des personnes existantes ou ayant existé est purement fortuite et involontaire.

sélection plus difficile et peuvent ainsi être à l'origine d'erreurs. Des fonctions d'arrière-plan conçues de manière intelligente permettraient de réduire considérablement ces énumérations. Il serait par exemple possible de relever et de filtrer de nombreuses entrées illogiques (cas ambulatoire dans un traitement stationnaire, cas déjà clos). Si la recherche n'inclut pas les dossiers déjà clôturés, ceux-ci ne devraient pas figurer du tout dans les occurrences.

Fonctions de protection en cas de changement de dossier patient

De nombreuses déclarations CIRS relatent que le traitement simultané de plusieurs dossiers patients dans le même logiciel est une source fréquente d'erreurs. Il en va de même lorsqu'il s'agit de passer d'une application à l'autre pour la même personne. Étant donné que dans le domaine de la santé, les utilisateurs/utilisatrices des outils informatiques sont régulièrement interrompus et leur attention est souvent détournée, et qu'en outre, ils accomplissent en parallèle d'autres activités, le risque de telles erreurs doit être considéré comme très élevé.

Si un logiciel permet le traitement simultané de plusieurs dossiers patients, il convient de sensibiliser les utilisateurs/utilisatrices au risque que cela comporte. Cela étant, la probabilité de confusion entre patient-e-s reste cependant réelle et l'idéal serait de renoncer par principe à ouvrir plusieurs dossiers en même temps. Les solutions offrant le plus de sécurité sont celles qui reposent non sur le comportement et l'autodiscipline des utilisateurs/utilisatrices, mais sur des fonctions techniques qui empêchent le traitement simultané de plusieurs dossiers [14].

Étant donné que l'implémentation a posteriori de telles fonctions peut signifier une surcharge de travail pour les collaborateurs/collaboratrices, le passage d'un dossier à l'autre doit être le plus sûr et le plus rapide possible. Il faut pour cela garantir, d'une part, un chargement rapide des données afin de réduire le temps d'attente et l'agacement. D'autre part, la technique doit assurer que, lorsque le passage d'un dossier patient à l'autre n'est pas achevé, l'action sur une autre interface n'a pas pour effet d'ignorer l'ordre précédent en ramenant au dossier patient qui aurait dû être fermé (voir p. 3). À cette fin, les mécanismes techniques à mettre en place doivent empêcher l'appel de fonction jusqu'à ce que le changement de dossier ait eu lieu.

Si, dans certains systèmes, le chargement lors du passage d'un dossier à l'autre est lent, plusieurs contenus issus de différents dossiers s'affichent simultanément.* Le plus souvent, on voit apparaître à l'écran tout d'abord les données ID du patient dont on est en train d'ouvrir le dossier, tandis que des contenus du dossier précédent sont encore visibles. Cela comporte des risques très élevés. En conséquence, il convient d'exclure de façon fiable de telles constellations. Étant donné que les situations décrites se déroulent principalement lorsque le réseau est très chargé (p. ex. en début de matinée), ce type de problèmes devrait être pris en compte dans les scénarios de test pour le développement des logiciels en simulant une forte sollicitation du réseau. Il convient également de prendre en compte les remarques des utilisateurs/utilisatrices à cet égard.

Fonctions login et logout

L'utilisation en alternance des ordinateurs par plusieurs collaborateurs/collaboratrices conduit régulièrement à la consultation du faux dossier après un changement de personne. Fermer systématiquement sa session au moment de quitter le poste de travail informatique constitue une mesure de prévention efficace. En raison du risque susmentionné, la plupart des systèmes ont intégré une fonction de déconnexion automatique après une phase d'inactivité sur l'ordinateur. Le laps de temps prévu en la matière est cependant en général trop long pour empêcher de façon sûre l'utilisation de la session par d'autres personnes. Les collaborateurs/collaboratrices sont dès lors invités à fermer manuellement leur session dès qu'ils quittent le poste de travail informatique. L'expérience et nombre de déclarations CIRS montrent cependant que cette procédure est souvent négligée dans la pratique.

Pour mieux maîtriser les risques liés aux changements fréquents d'utilisateurs/utilisatrices des postes de travail IT, il est indispensable d'implémenter des solutions techniques modernes. Celles-ci doivent permettre un login et un logout sûrs, sans pour autant contenir des contraintes supplémentaires. En la matière, bon nombre des systèmes actuels ont encore une marge de progression. La procédure nécessitant le logout manuel et la reconnexion avec login et saisie du mot de passe est mal acceptée car jugée trop lente. Cela montre la nécessité de mettre en place dans ce domaine des techniques avancées.

Des approches déjà mises en œuvre avec succès dans d'autres branches mériteraient d'être examinées de façon approfondie – et au besoin adaptées – pour le secteur de la santé. Les fonctions à intégrer devraient permettre un logout automatique au moment de quitter le poste de travail informatique, mais garantir aussi une reconnexion simple et rapide. Cela pourrait passer par des solutions techniques existantes, comme des bandes magnétiques ou des puces RFID intégrées au badge des collaborateurs/collaboratrices. Des procédures entièrement nouvelles pourraient aussi remplir les conditions susmentionnées. Dans l'idéal, de telles méthodes devraient accroître le niveau de sécurité tout en déchargeant les collaborateurs/collaboratrices de tâches routinières inutiles.

Dans le domaine stationnaire en particulier, où de nombreuses disciplines collaborent autour des patient-e-s, plusieurs systèmes IT cohabitent généralement. Il n'est pas rare que les spécialités notamment (anesthésie, soins intensifs, médecine d'urgence et divisions diagnostiques, etc.) utilisent des logiciels spécifiques qui ne sont pas connectés – ou ne le sont que partiellement – avec les dossiers patients à proprement parler. Il s'ensuit que différents programmes doivent être consultés en parallèle pour la même personne. Outre le surcroît de travail

*Ces phénomènes sont parfois contestés comme n'étant pas réalistes. Or ils ont été confirmés par plusieurs personnes lors des entretiens menés pour l'élaboration de la présente Quick-Alert.

engendré et les dangers connus que cela comporte, le risque de confusion entre patient-e-s est élevé. C'est en particulier vrai lorsqu'il faut sélectionner et ouvrir les dossiers manuellement dans les différentes applications.

Vu le grand nombre de sous-systèmes, il n'y a souvent pas d'interfaces fonctionnelles vers les applications de base. Dès lors, il convient d'examiner au moins la possibilité d'ouvrir un autre logiciel à partir des différents programmes de façon à accéder automatiquement au dossier de la personne dont on est en train de s'occuper. À cet égard, les concepts d'identification sûrs constituent une ressource précieuse (p. ex. Master Patient Index), car ils relient de façon univoque à la bonne personne, indépendamment du système. Pour éviter les confusions entre patient-e-s, ces numéros d'identification peuvent également être saisis comme termes vedette lors d'une recherche manuelle de personnes.

Ouverture automatisée de dossiers patients

Malgré l'implémentation de diverses fonctions destinées à éviter les erreurs, la sélection manuelle de dossiers patients reste un processus qui manque de sécurité. Les procédures techniques où l'ouverture du bon dossier repose sur des caractéristiques ID sûres montrent beaucoup plus de fiabilité. Pour éviter des sources d'erreurs supplémentaires, ces marques d'identification doivent se trouver sur la personne des patient-e-s, p. ex. sur un bracelet. L'affichage automatisé du bon dossier par un scan du code-barres apposé sur le bracelet du patient/de la patiente est une des méthodes offrant aujourd'hui le plus de sécurité. La technologie pour la lecture des différents types de codes-barres ou de codes surface a fait d'immenses progrès ces dernières années, de sorte que ce procédé pourrait être implémenté rapidement, sans problèmes et sans appareils supplémentaires onéreux. L'insertion de puces RFID sur un bracelet apporte un niveau de sécurité comparable. Selon la technologie utilisée, il serait même possible de vérifier l'ID du patient sans la lire directement, mais uniquement en s'approchant de la personne.

Théoriquement du moins, l'utilisation de méthodes d'identification biométriques serait également envisageable. Outre le respect des dispositions légales sur la protection des données, certaines questions d'application pratique et, avant tout, d'adhésion des patient-e-s à de telles méthodes ne sont pas clarifiées. Le recours aux empreintes digitales, par exemple, pose non seulement des problèmes de pratique et d'hygiène, mais il est en outre associé à des images négatives et pourrait être mal perçu par les patient-e-s. Il en va de même d'autres paramètres biométriques. Par ailleurs, différentes technologies présentant un niveau élevé de sécurité pourraient probablement être mises en œuvre dans le secteur de la santé [15]. Au stade actuel toutefois, nous manquons d'expériences fiables indiquant dans quelle mesure ces procédures seraient effectivement applicables et si elles seraient acceptées par une grande partie des patient-e-s.

Évaluation et priorisation des mesures

L'évaluation ci-dessous montre que certaines mesures ont une efficacité relativement faible (fig. 8).

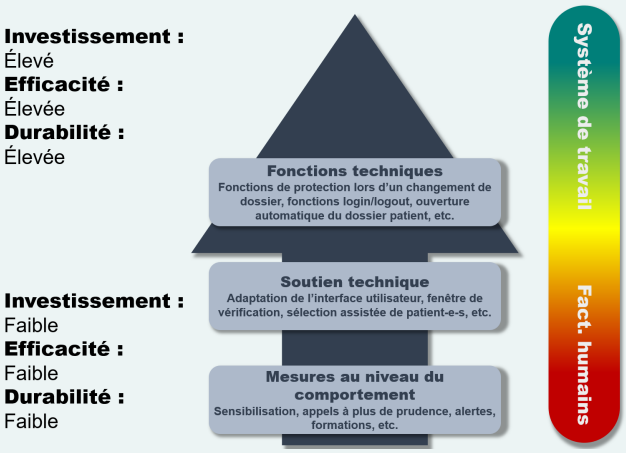


Fig. 8: Évaluation de l'efficacité des mesures (modif. d'après [16])

Il faut toutefois prendre en compte le fait que, même avec un degré très élevé de numérisation, l'utilisation des systèmes d'information clinique repose majoritairement sur des actions humaines et comporte, de façon inhérente, des risques d'erreurs. Pour cette raison, et de par les nécessités de l'application, il est pratiquement impossible d'éviter complètement les erreurs dues aux actions. Au stade actuel, il n'est dès lors pas possible d'offrir une sécurité totale par des mesures « fortes » empêchant la confusion entre patient-e-s liée aux outils numériques. C'est pourquoi il faut se donner toutes les chances de combattre les risques reconnus de la manière la plus globale possible. Il ne serait pas réaliste en la matière de placer de trop grands espoirs dans la mise en œuvre de recommandations isolées. Il s'agit bien davantage d'apporter la plus grande aide possible aux utilisateurs/utilisatrices pour éviter les erreurs en combinant différentes mesures entre elles.

Indépendamment de la mise en œuvre des recommandations émises, le renforcement de la sécurité passe aussi par le respect des exigences de base d'une exploitation IT exempte de problèmes. Parmi les qualités requises figurent notamment une performance suffisante du système et du réseau – même dans les moments de forte sollicitation –, une couverture WLAN réellement complète ainsi que du matériel et des logiciels appropriés. Il convient en outre d'accorder suffisamment d'attention aux facteurs non techniques : des mesures d'organisation du travail – locaux appropriés, procédures exemptes d'interruptions et d'éléments détournant l'attention du personnel – sont susceptibles d'améliorer grandement la sécurité dans l'utilisation de l'informatique. Actuellement, trop peu de ressources sont investies dans les moyens visant à éviter la confusion entre patient-e-s liée aux outils numériques. Des mesures relativement peu coûteuses peuvent contribuer en la matière à améliorer sensiblement la sécurité des patients.

CIRRNET®

Quick-Alert®

Bibliographie

1 Fischer S, Schwappach DLB. Efficiency and Safety of Electronic Health Records in Switzerland—A Comparative Analysis of 2 Commercial Systems in Hospitals. *J Patient Saf* 2022;**18**:645–51. doi:10.1097/pts.0000000000001009

2 Singh H, Sittig DF. Measuring and improving patient safety through health information technology: The health IT safety framework. *BMJ Qual Saf* 2016;**25**:226–32. doi:10.1136/bmjqs-2015-004486

3 Coiera E, Ash J, Berg M. The Unintended Consequences of Health Information Technology Revisited. *Yearb Med Inform* 2016;:163–9. doi:10.15265/iy-2016-014

4 Denham CR, Classen DC, Swenson SJ, *et al.* Safe use of electronic health records and health information technology systems: Trust but verify. *J Patient Saf* 2013;**9**:177–89. doi:10.1097/PTS.0b013e3182a8c2b2

5 Grissinger M. Oops, sorry, wrong patient!: A patient verification process is needed everywhere, not just at the bedside. *P T* 2014;**39**:535–7.

6 Emergency Care Research Institute (ECRI). Patient identification lessons learned from ECRI Institute's 2016 deep dive. *ECRI Inst* 2016;:9–10.https://www.ecri.org/components/HRCAlerts/Pages/HRCAlerts092816_PatientID.aspx

7 Fazekas M, Ettelt S, Newbould J, *et al.* IDENTITY CRISIS. 2010;:89.

8 Adelman JS, Kalkut GE, Schechter CB, *et al.* Understanding and preventing wrong-patient electronic orders: A randomized controlled trial. *J Am Med Informatics Assoc* 2013;**20**:305–10. doi:10.1136/amiajnl-2012-001055

9 Adelman JS, Berger MA, Rai A, *et al.* A national survey assessing the number of records allowed open in electronic health records at hospitals and ambulatory sites. *J Am Med Informatics Assoc* 2017;**24**:992–5. doi:10.1093/jamia/ocx034

10 Salmasian H, Blanchfield BB, Joyce K, *et al.* Association of Display of Patient Photographs in the Electronic Health Record with Wrong-Patient Order Entry Errors. *JAMA Netw Open* 2020;**3**:1–11. doi:10.1001/jamanetworkopen.2020.19652

11 Thomas JJ, Yaster M, Guffey P. The Use of Patient Digital Facial Images to Confirm Patient Identity in a Children's Hospital's Anesthesia Information Management System. *Jt Comm J Qual Patient Saf* 2020;**46**:118–21. doi:10.1016/j.jcjq.2019.10.007

12 Préposé fédéral à la protection des données et à la transparence. Guide relatif au traitement des données personnelles dans le domaine médical. https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2006/01/leitfaden_fuer_diebearbeitungvonpersonendatenimmedizinischenbere.pdf.download.pdf/guide_pour_le_traitementdesdonneespersonnellesdansledomainemedic.pdf

13 Brenowitz AGRB. Intercepting Wrong-Patient Orders in a Computerized Provider Order Entry System. *Physiol Behav* 2017;**176**:139–48. doi:10.1016/j.annemergmed.2014.11.017.Intercepting

14 Kannampallil TG, Manning JD, Chestek DW, *et al.* Effect of number of open charts on intercepted wrong-patient medication orders in an emergency department. *J Am Med Informatics Assoc* 2018;**25**:739–43. doi:10.1093/jamia/ocx099

15 RightPatient. Choosing The Most Effective Biometric Modality for Patient Identification in Healthcare - Assessing the characteristics and capabilities of biometric hardware. Atlanta: https://www.rightpatient.com/rightpatient-biometric-patient-identification-white-paper/

16 ISMP. Education is "predictably disappointing" and should never be relied upon alone to improve safety | Institute For Safe Medication Practices. https://www.ismp.org/resources/education-predictably-disappointing-and-should-never-be-relied-upon-alone-improve-safety

Auteurs et spécialistes ayant participé à l'élaboration du présent document

Helmut Paula, EMBA HSM
Fondation Sécurité des patients Suisse

Prof. Dr. Kerstin Denecke
Haute école spécialisée bernoise, Informatique médicale

Prof. Dr. Katrin Fischer
Haute école de psychologie appliquée FHNW

Prof. Dr. Sang-Il Kim
Haute école spécialisée bernoise, Informatique médicale

Nicole Stoller, MSc
Haute école de psychologie appliquée FHNW

Carmen Kerker-Specker, MScN
Fondation Sécurité des patients Suisse

Institutions ayant apporté leur soutien

Berner Fachhochschule
Haute école spécialisée bernoise
Bern University of Applied Sciences

Fachhochschule Nordwestschweiz
Hochschule für Angewandte Psychologie

La présente Quick-Alert® a été approuvée par les associations professionnelles / organes suivants :

Comité du CIRRNET

Remarque

Cette problématique a une importance qui dépasse le cadre régional. Merci d'en examiner la portée pour votre établissement et de veiller, le cas échéant en accord avec les organismes dont vous relevez, à ce qu'elle soit diffusée de manière ciblée et, si nécessaire, à un large public.

Les présentes recommandations visent à sensibiliser et à soutenir les institutions de santé et les professionnels actifs dans le domaine de la santé pour l'élaboration de directives internes à leur établissement. Il incombe aux fournisseurs de prestations de les examiner dans leur contexte local et de décider si elles revêtent un caractère obligatoire ou si elles doivent être modifiées ou rejetées. La forme spécifique et l'application à chaque cas selon les mesures de précaution en vigueur (en fonction des conditions locales sur le plan technique, entrepreneurial, légal, personnel et de la situation) relèvent exclusivement de la responsabilité des prestataires compétents.

Helmut Paula, responsable CIRRNET
paula@patientensicherheit.ch

Carmen Kerker-Specker, collaboratrice scientifique
kerker@patientensicherheit.ch

www.securitedespatients.ch/publications/quick-alert

Fondation Sécurité des patients Suisse
Asylstrasse 77
CH-8032 Zurich
T +41 43 244 14 80