Mise en place de workflows numériques en conformité avec le RGPD pour les prestataires de soins de santé

Amélioration des soins et de la relation avec les patients grâce à une approche de sécurité centrée sur les données et les utilisateurs

virtru

Table des matières

Exploitation des opportunités relatives aux soins de santé sans compromis sur la conformité au RGPD et la confidentialité des patients

Les progrès en matière de technologies médicales et de systèmes d'information modernes ont permis de faire évoluer le secteur de la santé. Alors que les prestataires répondent aux exigences significatives en matière de processus et évoluent vers des systèmes de santé fondés sur la valeur, la mise en place de nouveaux modèles de prestations de soins de santé numériques, d'applications sur le cloud et d'équipements médicaux connectés s'est accompagnée d'opportunités et de défis particuliers.

Reflétant la tendance du travail à distance adoptée par d'autres secteurs, les workflows numériques du domaine de la santé facilitent la coordination des soins entre équipes de prestataires de soins de santé décentralisées ainsi que l'interaction avec leurs patients, ce qui se traduit par de meilleurs résultats. Toutefois, cette tendance compromet considérablement la confidentialité des patients. Les environnements cloud multiples utilisés pour les prestations de soins de santé numériques exposent les informations de santé protégées (PHI) à des risques. Il en résulte des préoccupations en ce qui concerne la confidentialité des patients et le respect des réglementations.

Le secteur de la santé est habitué aux réglementations relatives à la confidentialité. Aux États-Unis, ces réglementations relatives à la confidentialité dans le domaine médical sont regroupées dans la loi Health Insurance Portability and Accountability Act (HIPAA). Dans le reste du monde, les prestataires de santé étaient souvent tenus de respecter un ensemble de réglementations, avant la mise en place du règlement général sur la protection des données (RGPD).

Le RGPD vise non seulement à renforcer les réglementations relatives à la confidentialité, mais également à élargir la portée de la protection des données. Toutes les données en lien avec la santé physique ou mentale, la composition génétique ainsi que les caractéristiques physiques ou comportementales d'une personne sont considérées comme personnelles et protégées en vertu du RGPD.

Risques inhérents dans le cloud

Malgré sa capacité à faire évoluer les opérations, l'utilisation du cloud s'accompagne de risques importants.

Tous secteurs confondus, les organisations utilisent en moyenne 78 applications différentes dans le cloud chaque semaine. Les professionnels de la sécurité ne connaissent toutefois que 38 % des applications utilisées par les administrateurs informatiques.

SOURCE : Data Security & Privacy in The Digital Workplace

Les professionnels de santé ont besoin de partager rapidement les informations de santé protégées, parfois dans des situations où la rapidité d'accès a une incidence sur la vie du patient. C'est l'une des raisons pour lesquelles plus de 60 % des violations de données signalées au premier semestre 2019 ont été causées par une erreur humaine et le domaine médical a été touché plus durement que tout autre secteur.

SOURCE : Healthcare IT News

Une adoption généralisée des systèmes de dossiers médicaux électroniques (DME) a joué un rôle clé dans l'accessibilité et la sécurité des informations de santé protégées. Cependant, il existe de nombreux cas dans lesquels un accès immédiat aux informations de santé protégées est nécessaire. Ainsi, les professionnels de santé choisissent la solution de facilité et utilisent des systèmes de messagerie et de fichiers pour partager ces informations, plaçant la protection des e-mails et des fichiers au centre des programmes de confidentialité des patients et de conformité au regard du RGPD.

Les exigences des organisations de santé modernes révèlent les faiblesses des approches traditionnelles en matière de protection des données tout au long du parcours de soins. Ce guide vous offre l'analyse d'un scénario fictif fondé sur des cas d'utilisation réels dans le domaine médical. Il identifie les principales difficultés rencontrées avec les méthodes traditionnelles de protection des données. Il dévoile également la manière dont les protections centrées sur les données et les utilisateurs aident à accélérer les prestations de soins de santé pour optimiser les résultats et garantir la confidentialité tout comme la conformité des données des patients.

Exigences de conformité au regard du RGPD

Afin de respecter le principe de sécurité du RGPD, des « mesures techniques appropriées » doivent être prises pour assurer la sécurité des données médicales confidentielles :

- **Chiffrement :** le RGPD exige expressément de considérer le chiffrement des données à caractère personnel comme une obligation générale d'adopter des technologies reflétant « l'état des connaissances » en matière de sécurité. Par conséquent, le chiffrement est effectivement obligatoire pour le partage des données confidentielles, telles que les informations de santé protégées.

- **Gestion des clés :** l'approche axée sur les risques liés à la cybersécurité du RGPD oblige implicitement les organisations à intégrer la gestion des clés (en particulier dans le but d'empêcher l'accès au fournisseur cloud) dans le cadre de leurs politiques globales pour la protection des données à caractère personnel.

- **Contrôles d'accès :** il exige que les organisations prennent le contrôle des données personnelles qu'elles gèrent. Les organisations doivent prouver qu'elles ont adopté des politiques et des procédures pour garantir le contrôle des données à caractère personnel. Il s'agit notamment des autorisations et des restrictions relatives à l'accès aux informations par les professionnels de santé.

- **Audit :** le RGPD met l'accent sur la responsabilité et l'audit des données. Il s'agit notamment du développement de processus qui prennent en charge l'analyse des activités dans les systèmes d'information qui contiennent ou utilisent des informations de santé protégées, en particulier pour détecter les éventuelles violations des informations de santé protégées. Les organisations doivent conserver des enregistrements permettant de démontrer qu'elles respectent les exigences du RGPD et mettre ces enregistrements à la disposition des régulateurs.

Le scénario : prestation et coordination des soins de santé numériques

Acme Health

Acme est une organisation de santé de taille moyenne axée sur la santé comportementale et les soins personnalisés, qui a pour mission d'aider ses patients à atteindre leurs objectifs à long terme en matière de santé et de leur offrir de meilleures conditions de vie. Acme a récemment mis en place plusieurs outils technologiques numériques pour participer à la rationalisation des prestations de soins de santé chez les équipes de prestataires décentralisées et, par conséquent, pour améliorer les interactions avec les patients. Ces outils viennent compléter G Suite pour favoriser la productivité et la collaboration du personnel décentralisé d'Acme.

L'engagement d'Acme auprès des patients ne s'arrête pas seulement aux prestations de santé physiques. L'organisation s'engage également sur le plan numérique, et en particulier sur le respect de la confidentialité, de la vie privée et de la sécurité des patients. La confiance est essentielle à la relation entre patients et prestataires, particulièrement lors d'un programme à long terme sur la santé comportementale. C'est pourquoi Acme estime que la sécurité des informations de santé protégées est un facteur clé pour gagner la confiance des patients. En plus d'être un devoir, la confidentialité des patients est également une obligation légale. L'équipe de direction d'Acme prend la conformité au regard du RGPD au sérieux, car outre leur impact sur les bénéfices, les violations compromettent la confiance des patients et ont une incidence négative sur leurs objectifs.

Risques en matière de conformité au RGPD

Les organisations ne respectant pas le RGPD sont passibles d'amendes allant jusqu'à 20 millions d'euros ou 4 % de leur chiffre d'affaires annuel si ce montant est supérieur.

Les dommages causés par les violations ne sont pas uniquement financiers : une étude a révélé qu'au cours des trois années suivant une violation de données, la qualité des prestations de santé diminuait et les taux de mortalité des patients augmentaient.

SOURCE : Data breach remediation efforts and their implications for hospital quality

Le cas d'utilisation : partage d'informations de santé protégées en externe et en interne

Les parties prenantes

Pénélope est administratrice des soins de santé chez Acme. Elle aide les médecins et les prestataires spécialisés à coordonner la prise en charge des patients tout en favorisant les interactions avec les patients. Lorsque l'équipe informatique d'Acme a commencé à cibler les exigences requises pour l'implémentation d'un nouveau système de dossiers médicaux électroniques (DME) ainsi que d'un portail patients, Pénélope a joué un rôle important en participant à une étude pour déterminer comment intégrer les programmes destinés aux patients aux nouveaux workflows numériques. Elle partage régulièrement des informations de santé protégées en interne entre plusieurs services, ainsi qu'en externe, à la fois avec des patients et avec le réseau étendu de prestataires spécialisés d'Acme.

Brittany est une patiente quinquagénaire qui a fait appel aux services de santé d'Acme sur les conseils de son médecin traitant, car elle court le risque de développer du diabète et de l'hypertension. Son programme Acme Health comporte des visites de contrôle numériques hebdomadaires par le biais de services de télémédecine et de communications via un portail patients, ainsi que des visites en personne avec son spécialiste.

Mélissa est une spécialiste expérimentée dans divers secteurs de soins. Mélissa joue également un rôle de liaison entre les patients prioritaires et les prestataires de santé d'Acme, aussi bien en interne qu'en externe. Elle aide à adapter les prestations de soins et à optimiser le modèle de santé comportementale d'Acme. Comme Pénélope, Mélissa est une professionnelle de santé férue de technologie qui accorde une importance primordiale à la prise en charge des patients. Mélissa s'occupe du programme de santé de Brittany et fait appel à des prestataires externes en cas de besoin.

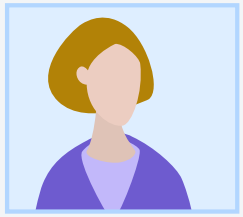
Evan est médecin et endocrinologue. Il fait partie des prestataires de santé externes d'Acme les plus fiables. Evan travaille en tant que prestataire externe d'Acme afin de développer son expertise et ses services au-delà de son petit cabinet privé solidement implanté.

Profils des utilisateurs

Pénélope, administratrice des soins de santé chez Acme

- Professionnelle de santé de 34 ans.
- Elle a 10 années d'expérience dans l'administration des soins de santé et travaille chez Acme depuis six ans.
- Elle maîtrise une vaste gamme de systèmes informatiques et d'outils numériques de santé.

Brittany, patiente



- Patiente de 55 ans exposée à des risques en matière de diabète et d'hypertension.
- Elle a fait appel à Acme pour prendre sa santé en main de manière proactive.
- Elle maîtrise les workflows numériques, mais a cependant des difficultés à gérer plusieurs comptes. Elle oublie souvent ses noms d'utilisateur et ses mots de passe.

Lors de sa visite de contrôle hebdomadaire, **Brittany** a indiqué s'être sentie léthargique au cours de la semaine passée. L'équipe d'Acme lui a donc prescrit un rapide examen ainsi que des analyses sanguines.

Pénélope doit maintenant partager les informations de santé protégées encore plus souvent, pour informer Brittany de ses résultats d'examens et de toute modification apportée à son programme de santé actuel. Elle doit également partager ces informations en interne avec Mélissa.

Mélissa doit partager les résultats d'examens et le dossier médical de Brittany avec **Evan**, afin qu'il puisse analyser les résultats en fonction des antécédents médicaux et de l'état de santé de la patiente. Evan recommandera ensuite des modifications à apporter à ses soins de santé et les implémentera avec l'aide de Mélissa.

Faiblesses des approches traditionnelles

Alors que Pénélope commence à partager les résultats d'examens avec Brittany, elle se rappelle avoir déjà essayé d'envoyer des informations importantes par le biais du portail patients, en vain. Le compte de Brittany est souvent bloqué en raison de l'oubli de son nom d'utilisateur et de son mot de passe. Elle a aussi parfois du mal à se connecter à cause des périodes de maintenance programmée.

Brittany préfère généralement communiquer par e-mail, car il s'agit de l'outil numérique qu'elle maîtrise le mieux. Lorsqu'elle ressent de la frustration envers le portail patients, elle choisit la solution de facilité et utilise sa messagerie pour contacter Pénélope.

Pénélope se souvient qu'Acme a prévu une maintenance informatique au cours des prochains jours et décide d'envoyer simplement les résultats d'examens à Brittany via Gmail en espérant que son équipe informatique a intégré des protections dans les workflows de messagerie. Elle souhaite que Brittany ait facilement accès à ses résultats d'examens et ne veut pas entraîner un retard dans ses prestations de soins.

Mélissa et Pénélope doivent également déterminer comment partager les résultats d'examens et les antécédents de Brittany avec Evan. Mélissa n'est pas sereine à l'idée de partager des informations de santé protégées avec des prestataires externes sans protections.

Profils des utilisateurs

Mélissa, spécialiste et prestataire de soins de santé chez Acme

- Prestataire de santé de 38 ans.
- Elle a 15 ans d'expérience dans diverses fonctions du secteur médical et travaille depuis trois ans chez Acme.
- Elle maîtrise une vaste gamme de systèmes informatiques et d'outils numériques de santé, mais elle a dû faire appel au support technique pour régler des problèmes d'interopérabilité entre les DME et le portail patients.

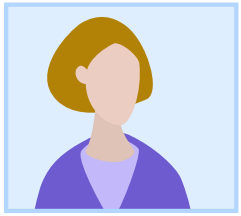
Evan, prestataire externe

- Médecin et endocrinologue de 55 ans.
- Il s'est associé à Acme afin d'apporter son expertise en médecine spécialisée.
- Il possède et gère également un petit cabinet médical.
- Il maîtrise peu les outils de santé numériques. Il utilise toujours le fax et les dossiers papier pour la plupart de ses workflows et préfère les e-mails pour coordonner les soins numériques.

Ressenti des utilisateurs avant

Pénélope est inquiète :

- Elle est consciente qu'il existe des risques relatifs à la conformité au RGPD si elle partage des informations de santé protégées par e-mail. Elle les ignore cependant pour rester en adéquation avec sa philosophie : faire passer les patients avant tout.
- Elle pense que ce scénario va à l'encontre de la mission d'Acme, qui est de répondre aux besoins des patients, en raison des risques de violation des informations de santé protégées. En faisant passer les besoins de la patiente avant tout et en assurant l'accessibilité à ses données, elle compromet la sécurité d'Acme.



Brittany se sent frustrée et impuissante :

- Elle souhaite interagir avec l'équipe d'Acme, mais le portail patients semble rarement fonctionner.
- Le portail patients lui semble superflu : elle reçoit une notification par e-mail l'informant que des messages l'attendent sur le portail, alors pourquoi ne pas directement les envoyer par e-mail ?

Ressenti des utilisateurs avant

Mélissa n’est pas sereine :

- De précédentes violations du RGPD ont fait comprendre à Mélissa que la protection des informations de santé protégées était primordiale. C’est pourquoi elle décide que la meilleure approche immédiate consiste à fournir à Evan un nouveau compte au sein du système de DME d’Acme.
- Après plusieurs refus, l’équipe informatique d’Acme accepte exceptionnellement de déroger à ses politiques et crée le compte d’Evan. Bien qu’elle ait respecté les règles en matière de sécurité et de conformité, elle a dû demander avec insistance à l’équipe informatique de fournir un nouveau compte de DME à Evan.
- Elle se souvient qu’Evan a peu d’expérience avec les DME, elle craint donc que cette étape lui demande du temps et entraîne des retards coûteux dans les prestations de soins.

Evan est frustré :

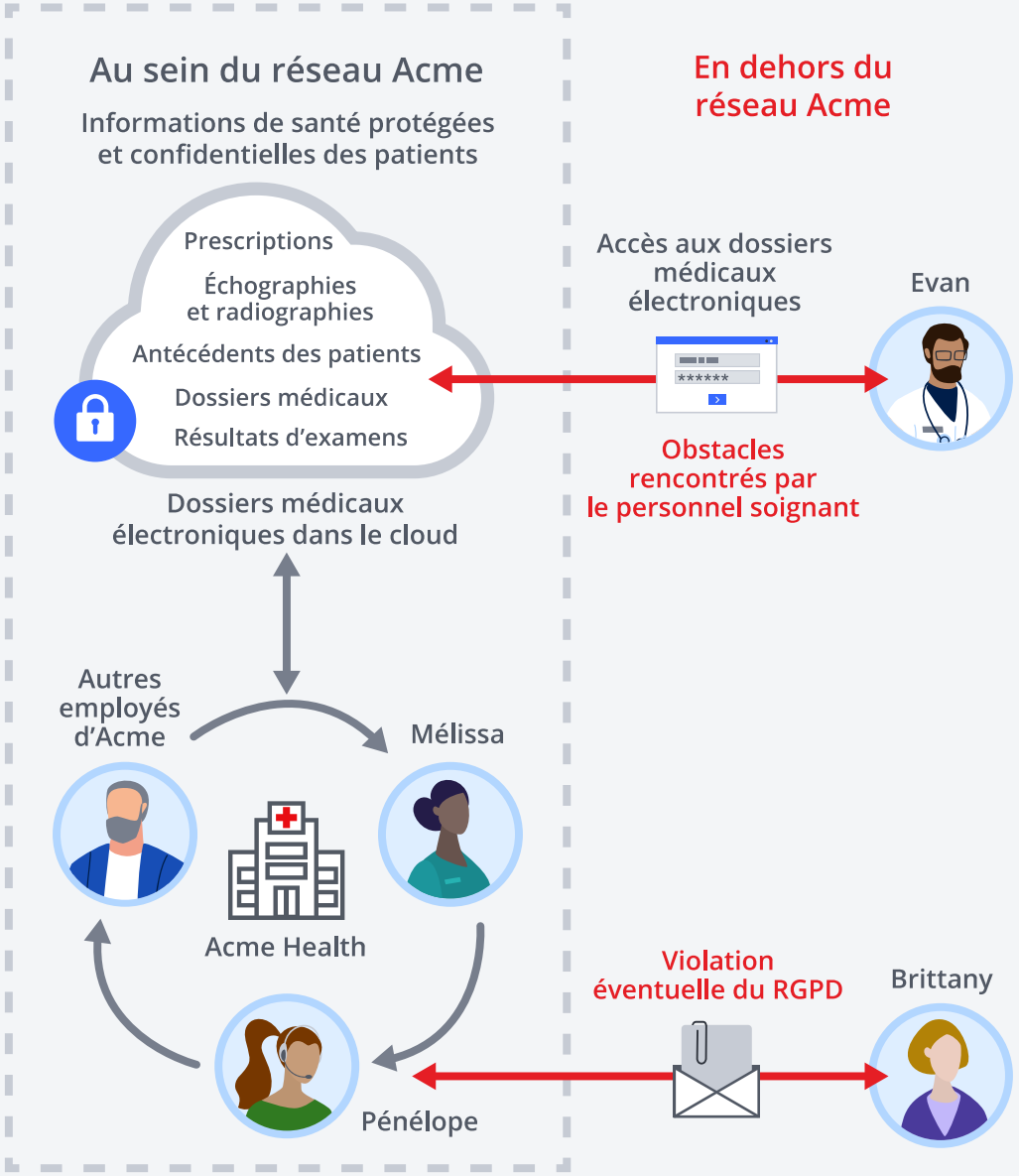
- Evan n’a jamais eu d’expérience positive avec les systèmes de DME. Selon lui, ils constituent un obstacle à la prestation des soins. Il préférerait coordonner les soins comme il en a l’habitude : par fax, e-mails et appels téléphoniques.
- Evan démarre à contrecœur l’inscription à son compte de DME, mais l’application s’interrompt à plusieurs reprises au cours du processus. Il est contraint de passer presque une heure en compagnie du support technique.
- Tandis qu’Evan essaie de résoudre ces problèmes techniques, son travail en retard s’accumule. Il doit donner la priorité aux patients de son cabinet. Par conséquent, il n’examine les résultats d’examens et les antécédents médicaux de Brittany que le lendemain du partage de Mélissa.

Les conséquences

Acme n'aura aucun contrôle ni aucune visibilité sur ce que fait Brittany avec les dossiers médicaux. Pénélope espère que Brittany n'expose pas sans le savoir ses informations de santé protégées au risque d'un accès non autorisé (en compromettant ainsi la conformité d'Acme au regard du RGPD). Les désagréments que Brittany rencontre détériorent petit à petit sa relation avec Acme, ce qui pourrait également avoir une incidence sur sa santé.

Les problèmes informatiques relatifs à la mise en place d'un accès aux résultats d'examens et aux antécédents médicaux de Brittany font perdre un temps précieux à Mélissa et à Evan. Si les analyses sanguines révèlent un problème de santé grave, la journée supplémentaire passée à examiner et à prescrire des soins aura entraîné un retard dans la mise en place d'un traitement.

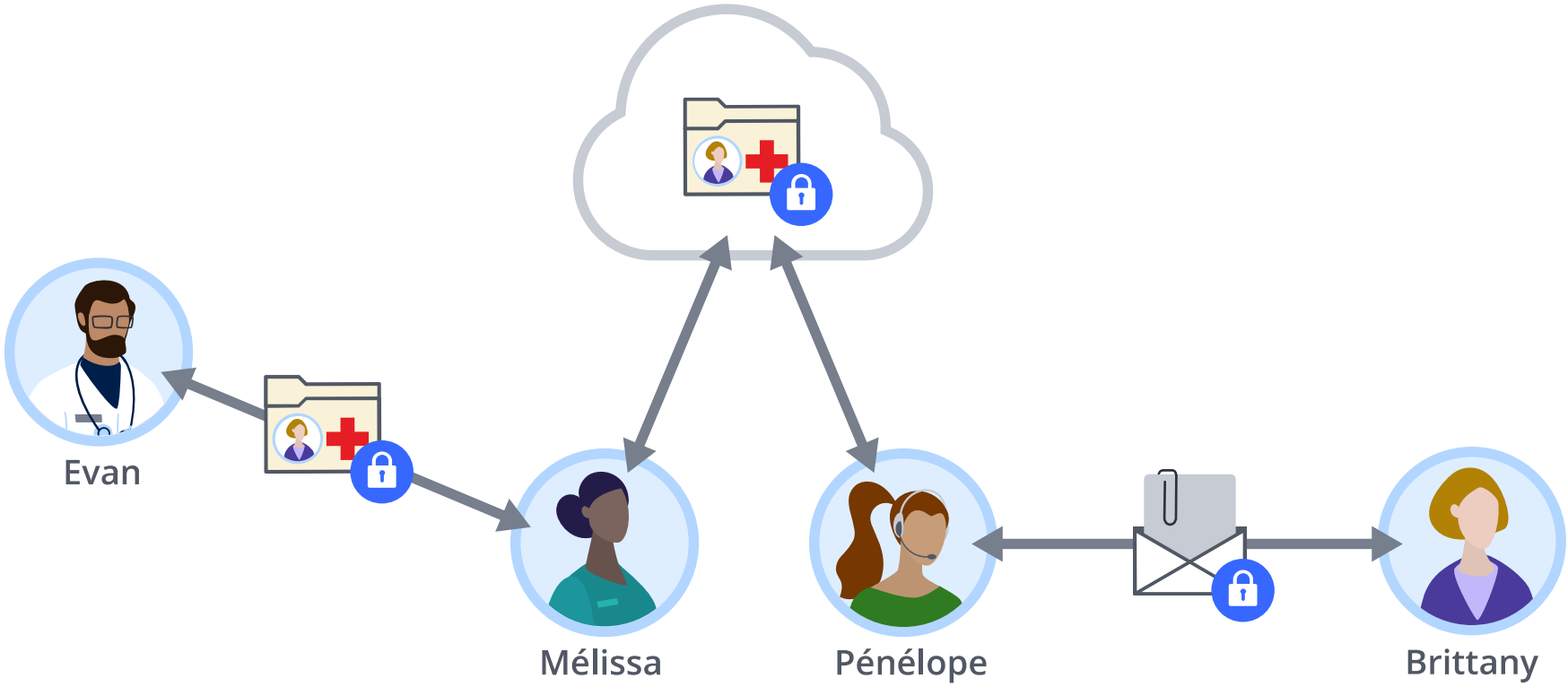
Les éventuels risques et pénalités causés par la non-conformité au RGPD persisteront tout au long du parcours de soins, tandis que le manque d'accès fluide et sécurisé aux informations de santé protégées dégrade la relation avec les patients et se traduit par une prise en charge des patients non optimale.



Une solution plus efficace : l'approche centrée sur les données et les utilisateurs

La protection des e-mails et des fichiers de Virtru apporte une sécurité centrée sur les données grâce au chiffrement de bout en bout qui empêche tout accès non autorisé et assure une visibilité ainsi qu'un contrôle persistants lors du partage des informations de santé protégées. La mise en place de la sécurité centrée sur les données préserve la protection, le contrôle et la visibilité tout au long du parcours de soins. Ainsi, les professionnels de santé sont en mesure d'améliorer la relation avec leurs patients et la collaboration avec leurs collègues, sans sacrifier la confidentialité des patients ni la conformité avec les réglementations. L'approche de Virtru centrée sur les utilisateurs garantit également l'intégration des protections directement dans les workflows de messagerie et de fichiers d'Acme, mais aussi en dehors de G Suite, partout où les informations de santé protégées sont partagées.

Désormais, Pénélope peut partager de manière aisée et sécurisée les résultats d'examens avec Brittany et gérer ses rendez-vous de suivi par e-mail, puis importer les données médicales de Brittany dans un dossier sécurisé partagé avec Mélissa sur Google Drive. De la même manière, Mélissa peut facilement partager les résultats d'examens et les antécédents médicaux en externe par e-mail, l'outil numérique qu'Evan privilégie pour accélérer la prise en charge.

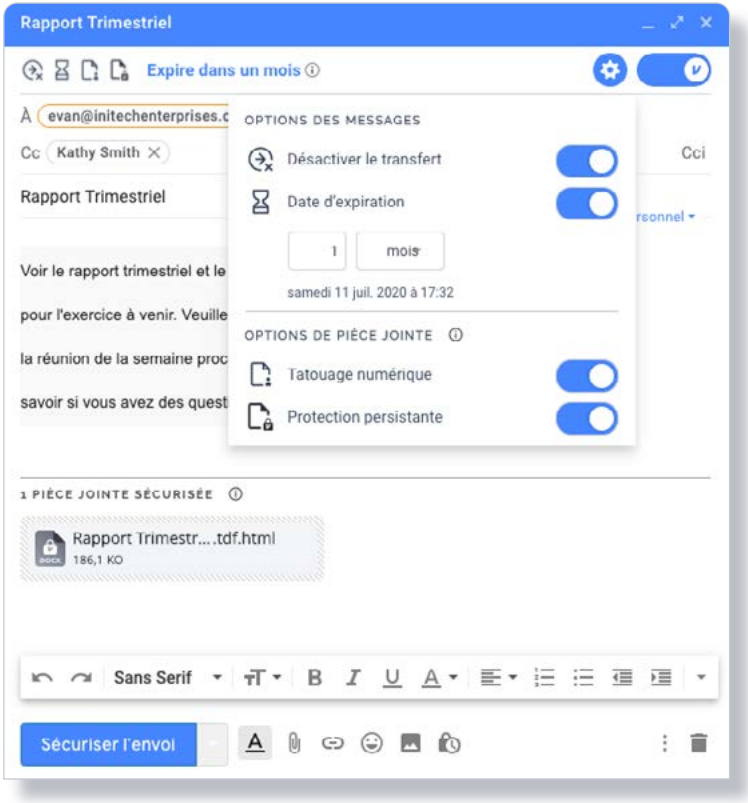


Ressenti des utilisateurs après

Pénélope estime **QUE SON TRAVAIL EST VALORISÉ.**

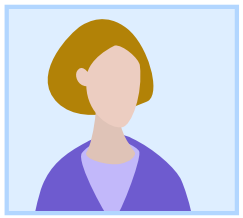
- Pénélope joint simplement les résultats d'examens dans un message Gmail et active le chiffrement de bout en bout de Virtru afin d'empêcher l'accès des tiers non autorisés pour garantir la confidentialité et la conformité au RGPD.

- Grâce aux contrôles d'accès granulaires de Virtru, Pénélope est également en mesure de réaliser les actions suivantes :
  - Définir une autorisation d'accès d'une durée de six mois, valide jusqu'à la fin du programme initial de Brittany.
  - Ajouter un tatouage numérique, qui consiste à intégrer le nom des destinataires en arrière-plan du fichier pour prévenir les fuites de données.
  - Mettre en place une protection persistante pour assurer la confidentialité et la conformité des résultats d'examens au-delà de l'e-mail initial, dans le cas où Brittany les télécharge sur son bureau.
- Tout au long du parcours de soins, Acme préserve la visibilité ainsi que le contrôle, et peut toujours adapter les contrôles d'accès si nécessaire.



Le chiffrement de bout en bout facile d'utilisation de Virtru protège les informations de santé confidentielles partagées dans les e-mails et les fichiers pour garantir la confidentialité des patients et la conformité au regard du RGPD.

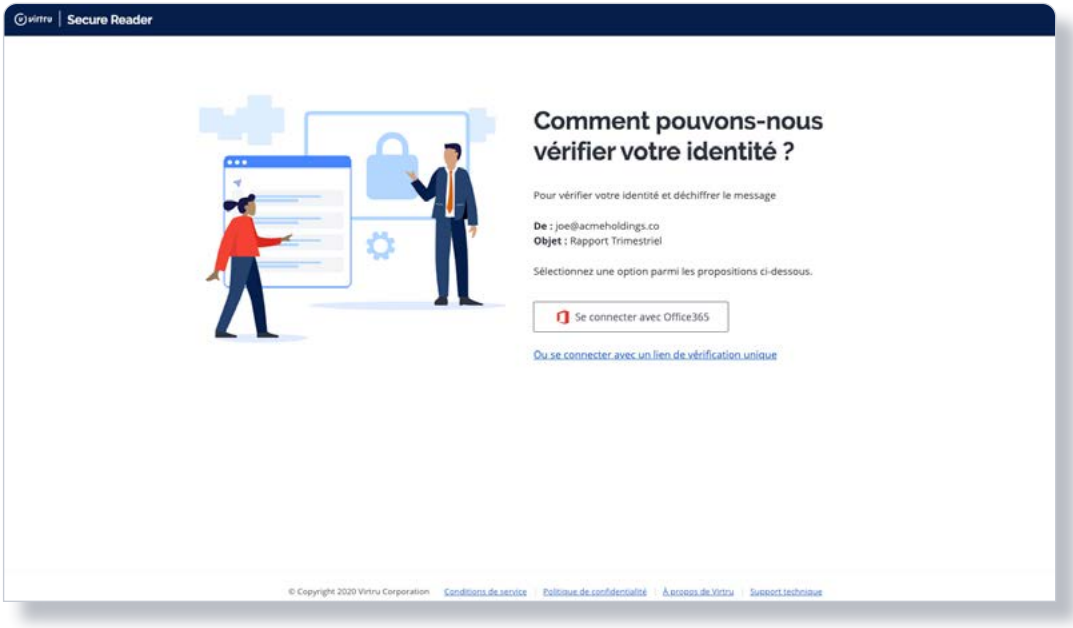
Ressenti des utilisateurs après



Brittany se sent plus **CONFIANTE** vis-à-vis de son programme de soins.

- Elle reçoit ses résultats d'examens presque immédiatement par e-mail, accompagnés d'un message de Pénélope lui indiquant clairement les étapes qu'elle doit suivre ensuite.

- Elle n'est pas contrainte d'utiliser une application supplémentaire, de gérer un nouveau compte ou de se souvenir d'un autre mot de passe. Elle accède en toute simplicité aux résultats d'examens grâce à Virtru Secure Reader.

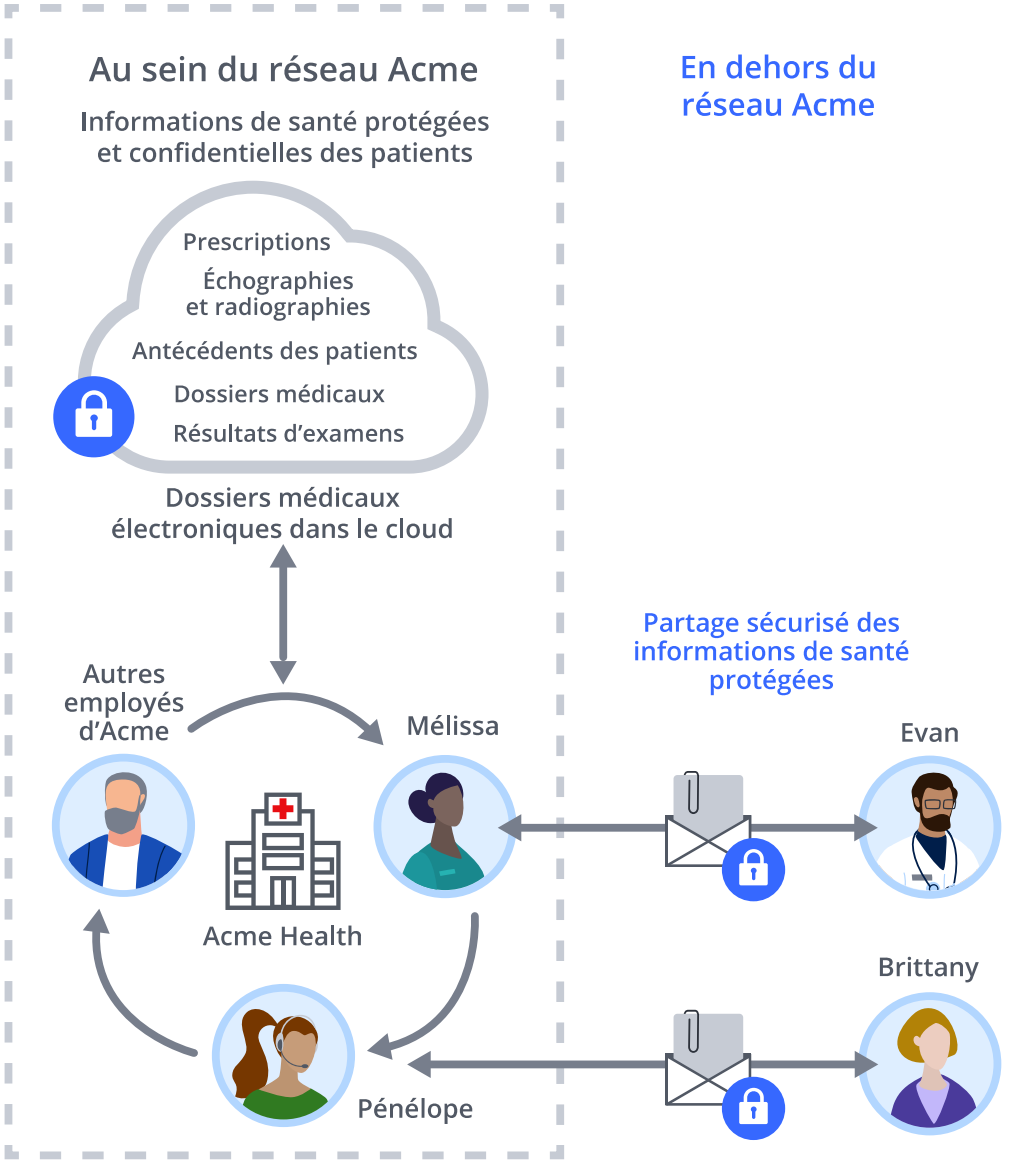


L'approche centrée sur l'utilisateur de Virtru offre un accès simplifié grâce à l'utilisation de comptes et d'identifiants existants qui facilite les interactions avec les patients.

Ressenti des utilisateurs après

Mélissa et **Evan** estiment également **QU'ILS TRAVAILLENT PLUS EFFICACEMENT.**

- Mélissa partage simplement les antécédents médicaux et les résultats d'examens de la patiente avec Evan via un e-mail protégé. Elle n'a plus besoin de supplier l'équipe informatique de créer un compte de DME pour un utilisateur externe.
- Mélissa utilise un workflow semblable à celui de Pénélope afin d'améliorer le contrôle et la visibilité pour assurer la conformité au regard du RGPD. Après avoir chiffré le message, elle ajoute un tatouage numérique et empêche le transfert des informations de santé protégées.
- Evan est soulagé en constatant que ce workflow s'aligne avec ses méthodes de travail. Il peut rapidement accéder aux résultats d'examens et les étudier, puis collaborer avec Mélissa et l'équipe d'Acme pour identifier les soins de santé qui limiteront les risques de diabète et d'hypertension de Brittany.



Les conséquences

Au lieu de ressentir un sentiment d'inquiétude, de frustration et d'impuissance, tous les acteurs ont les clés en main pour avancer sereinement tout en offrant une prise en charge efficace et rapide à Brittany. Pénélope fournit à Brittany l'assurance et la confiance dont elle a besoin pour optimiser l'impact du programme de santé comportementale d'Acme. Evan élimine les éventuels décalages avec l'équipe d'Acme en adoptant les workflows existants. L'approche de Virtru centrée sur l'utilisateur garantit que toutes les parties sont sur la même longueur d'onde afin de prescrire rapidement de nouveaux soins de santé à Brittany.

La sécurité centrée sur les données donne la possibilité aux professionnels de santé de collaborer sur des processus numériques en se conformant au RGPD. Ainsi, Acme et Brittany sont confiants d'atteindre les objectifs fixés pour améliorer son état de santé.

Amélioration de la relation avec les patients et optimisation des soins grâce à une protection des informations de santé protégées centrée sur les données et les utilisateurs

Les workflows numériques et les systèmes dans le cloud offrent de nombreuses opportunités aux organisations de soins de santé. Ils peuvent néanmoins exposer les patients à des risques élevés en matière de confidentialité et de non-conformité. Comme l'illustre l'expérience d'Acme, les méthodes traditionnelles de protection ne répondent pas au besoin de dynamisme et de rapidité nécessaires aux collaborations dans le domaine médical, ce qui est source de frustration pour les utilisateurs et peut nuire aux prestations de santé.

L'association de protections centrées sur les données et d'une approche au service de l'utilisateur en matière de préservation des informations de santé protégées permet aux organisations de santé d'optimiser leurs prestations de soins. Les équipes informatiques et de sécurité peuvent proposer aux utilisateurs des workflows de collaboration médicale sécurisés, qui permettent de garantir la rapidité des prestations de soins et d'améliorer la relation avec les patients, tout en protégeant les informations de santé confidentielles afin d'empêcher tout risque d'amendes de non-conformité.

Si vous souhaitez découvrir comment Virtru peut aider votre organisation à moderniser ses prestations de soins, contactez-nous pour avoir un aperçu de la facilité de préservation des données confidentielles des patients et de la conformité apportée par nos solutions. virtru.com/contact-us

Chez Virtru, nous permettons aux organisations d'exploiter leurs données en toute simplicité tout en gardant le contrôle, quel que soit l'emplacement où elles sont stockées et partagées. Notre portefeuille de solutions et d'outils, fondés sur notre plateforme de protection des données ouverte, régit les données tout au long de leur cycle de vie. Plus de 20 000 organisations font confiance à Virtru pour la sécurité des données et la protection de la confidentialité.

Rendez-vous sur virtru.com/fr ou suivez-nous sur Twitter @virtruprivacy.