Mon DOSSIER SANTÉ

Sécurité de l'information et protection des données dans le cadre de Mon Dossier Santé

Pourquoi parler de sécurité informatique dans le cadre de Mon Dossier Santé ?

Suite aux dernières actualités dans le domaine de la cybersécurité et de la santé (cessation d'activité avec effet immédiat de mesvaccins.ch, piratage de données de la commune de Rolle, tentative de piratage de la BCN, etc.), il est nécessaire d'insister sur les mesures de sécurité mises en place pour assurer la sécurité de Mon Dossier Santé. Les données médicales qu'il héberge étant des données très sensibles, il convient de rassurer toutes les parties prenantes.

Qui propose le service Mon Dossier Santé ?

La plateforme Mon Dossier Santé est proposée par une communauté de référence (CR DEP NE) qui a été certifiée selon la Loi fédérale sur le Dossier Électronique du Patient (LDEP), c'est-à-dire répondant à plus de 440 critères techniques et organisationnels (cf. Annexe 2 ODEP-DFI). Cette certification a été obtenue après de nombreuses phases d'audit par un organisme externe accrédité par la Confédération, qui procède également à des contrôles réguliers.

Quelles sont les conditions d'accès à Mon Dossier Santé ?

L'accès à la plateforme est uniquement possible pour un utilisateur détenant un Moyen d'Identification Électronique (MIE) fourni par un éditeur certifié selon l'annexe 8 ODEP-DFI. Ceci s'applique aux patients, à leurs représentants, aux professionnels et auxiliaires de santé ainsi qu'aux administrateurs de Mon Dossier Santé. Seul un droit d'accès octroyé par le patient lui-même permet à un professionnel/auxiliaire de santé d'accéder à son Dossier Santé ; les assureurs maladie, l'employeur et l'État ne peuvent techniquement pas y accéder.

Où sont stockées les données médicales ?

Les données médicales des patients sont stockées sur des serveurs installés en Suisse, ce qui correspond à une obligation selon la LDEP, ses ordonnances et annexes. C'est par conséquent la loi fédérale sur la protection des données (LPD) et ses ordonnances qui s'appliquent.

Comment sont protégées ces données médicales ?

Les données médicales sont cryptées en transit (entre les terminaux) et au repos (sur les serveurs), grâce aux dernières technologies disponibles sur le marché (protocole TLS, pare-feu, clés cryptographiques de 4096 bits). De plus, les données cryptées et les clés cryptographiques sont stockées sur des environnements totalement séparés auprès du fournisseur de plateforme, qui est certifié selon la norme EN ISO/IEC 27001 : 2013 (exigences relatives à la gestion de la sécurité de l'information). Celui-ci garantit ainsi une redondance totale des centres de données informatiques concernés. Enfin, la séparation des tâches est strictement appliquée tant par Mon Dossier Santé que par le fournisseur de la plateforme, ce qui garantit qu'un utilisateur privilégié n'a pas d'accès superflus par rapport à ce qui est strictement nécessaire dans le cadre de son activité.

Comment être sûr-e que ces mesures de protection sont suffisantes ?

La plateforme Mon Dossier Santé a subi trois tests d'intrusion exécutés par trois prestataires distincts. La CR DEP NE a mandaté un prestataire externe spécialisé pour effectuer des tests d'intrusion avant l'ouverture du service. Le fournisseur de la plateforme mène également de nouveaux tests d'intrusion à chaque mise à jour majeure et teste régulièrement son plan de reprise d'activité. Il propose également un « Bug Bounty program » récompensant la découverte de bugs et/ou failles de sécurité, ainsi que des tests visant à empêcher les attaques ciblées (p. ex. phishing). Enfin, l'auditeur externe de la CR DEP NE procède à ses propres tests d'intrusion dans le cadre de sa certification.

Mon DOSSIER SANTÉ

Sécurité de l'information et protection des données dans le cadre de Mon Dossier Santé

Pourquoi parler de sécurité informatique dans le cadre de Mon Dossier Santé ?

Suite aux dernières actualités dans le domaine de la cybersécurité et de la santé (cessation d'activité avec effet immédiat de mesvaccins.ch, piratage de données de la commune de Rolle, tentative de piratage de la BCN, etc.), il est nécessaire d'insister sur les mesures de sécurité mises en place pour assurer la sécurité de Mon Dossier Santé. Les données médicales qu'il héberge étant des données très sensibles, il convient de rassurer toutes les parties prenantes.

Qui propose le service Mon Dossier Santé ?

La plateforme Mon Dossier Santé est proposée par une communauté de référence (CR DEP NE) qui a été certifiée selon la Loi fédérale sur le Dossier Électronique du Patient (LDEP), c'est-à-dire répondant à plus de 440 critères techniques et organisationnels (cf. Annexe 2 ODEP-DFI). Cette certification a été obtenue après de nombreuses phases d'audit par un organisme externe accrédité par la Confédération, qui procède également à des contrôles réguliers.

Quelles sont les conditions d'accès à Mon Dossier Santé ?

L'accès à la plateforme est uniquement possible pour un utilisateur détenant un Moyen d'Identification Électronique (MIE) fourni par un éditeur certifié selon l'annexe 8 ODEP-DFI. Ceci s'applique aux patients, à leurs représentants, aux professionnels et auxiliaires de santé ainsi qu'aux administrateurs de Mon Dossier Santé. Seul un droit d'accès octroyé par le patient lui-même permet à un professionnel/auxiliaire de santé d'accéder à son Dossier Santé ; les assureurs maladie, l'employeur et l'État ne peuvent techniquement pas y accéder.

Où sont stockées les données médicales ?

Les données médicales des patients sont stockées sur des serveurs installés en Suisse, ce qui correspond à une obligation selon la LDEP, ses ordonnances et annexes. C'est par conséquent la loi fédérale sur la protection des données (LPD) et ses ordonnances qui s'appliquent.

Comment sont protégées ces données médicales ?

Les données médicales sont cryptées en transit (entre les terminaux) et au repos (sur les serveurs), grâce aux dernières technologies disponibles sur le marché (protocole TLS, pare-feu, clés cryptographiques de 4096 bits). De plus, les données cryptées et les clés cryptographiques sont stockées sur des environnements totalement séparés auprès du fournisseur de plateforme, qui est certifié selon la norme EN ISO/IEC 27001 : 2013 (exigences relatives à la gestion de la sécurité de l'information). Celui-ci garantit ainsi une redondance totale des centres de données informatiques concernés. Enfin, la séparation des tâches est strictement appliquée tant par Mon Dossier Santé que par le fournisseur de la plateforme, ce qui garantit qu'un utilisateur privilégié n'a pas d'accès superflus par rapport à ce qui est strictement nécessaire dans le cadre de son activité.

Comment être sûr-e que ces mesures de protection sont suffisantes ?

La plateforme Mon Dossier Santé a subi trois tests d'intrusion exécutés par trois prestataires distincts. La CR DEP NE a mandaté un prestataire externe spécialisé pour effectuer des tests d'intrusion avant l'ouverture du service. Le fournisseur de la plateforme mène également de nouveaux tests d'intrusion à chaque mise à jour majeure et teste régulièrement son plan de reprise d'activité. Il propose également un « Bug Bounty program » récompensant la découverte de bugs et/ou failles de sécurité, ainsi que des tests visant à empêcher les attaques ciblées (p. ex. phishing). Enfin, l'auditeur externe de la CR DEP NE procède à ses propres tests d'intrusion dans le cadre de sa certification.