Patientory: Un Réseau de Stockage pair à pair de dossiers médicaux

Chrissa McFarlane, Michael Beer, Jesse Brown, Nelson Prendergast

Avril 2017

Résumé

Un système d'Echange de Données Médicales (EDM) soutenu par la blockchain peut libérer les vraies valeurs de l'interopérabilité et de la cybersécurité. Ce système a le potentiel d'éliminer les frictions et les coûts des tiers intermédiaires en matière de gestion de la santé de la population. Il assure une amélioration de l'intégrité des données, de réduction des coûts, de décentralisation et d'une désintermédiation de confiance. Être capable de coordonné les soins aux patients via la blockchain EDM permet de diminué drastiquement le nombre de services non nécessaire tels que la duplication de test, diminuant ainsi les coûts et améliorant l'efficacité du cycle continuum santé tout en respectant toutes les règles et standards de l'HIPAA [1]. Un protocole centré sur les patients et soutenu par la technologie blockchain, Patientory, est en train de changer la façon des intervenants de la santé de gérer les données médicales et d'interagir avec les équipes cliniques.

1 Introduction

1.1 Qu'est-ce que la Blockchain ?

La derrière la monnaie virtuelle bitcoin. La naissance de la blockchain est attribuée à la personne (ou groupe) caché derrière le pseudo Satoshi Nakamoto. Depuis 2009 la blockchain n'a cessé de se répandre davantage dans l'industrie de la finance, avec une variété de nouvelles blockchains orientées business et services entrant sur le marché. La technologie blockchain est utilisée pour partager un registre de transactions à travers un réseau commercial sans être contrôlé par une seule entité. Ce registre rend plus facile la création rentable de liens commerciaux où toute chose de valeur peut être virtuellement suivi et échangé sans requérir un unique point de contrôle. La technologie met la confidentialité et le contrôle des données dans la main de tout les individus. L'intégrité est établie sans dépendance avec des parties tierces.

1.2 Infrastructure de santé actuelle

Les prestataires de soins doivent coopérer afin de traiter avec précision les patients à la fois après et entre les diagnostiques. Le besoin d'une coopération entre prestataires de soins de santé allant des spécialistes, médecins généraliste, mais encore à d'autre secteurs comme les nutritionnistes ou les infirmières en rééducation conduisent à l'augmentation de l'utilisation des technologies digitales. Le suivit et l'efficacité des soins c'est considérablement amélioré grâce aux technologies

digitales. En effet, elles ont résulté en la création de regroupements d'informations médicales telles que les dossiers médicaux informatique.

Le secteur de la santé et les organisations gouvernementales dépensent beaucoup de temps et d'argents à mettre en place et à gérer les systèmes d'échanges de données et d'informations ; et demandant des ressources pour la résolution des problèmes, la mise à jour des champs, la réalisation de sauvegardes, et l'extraction d'informations pour analyse.

Les lois fédérales et les programmes incitatif ont rendu les données de santé plus accessible, en réponse à la marche arrière des hôpitaux sur l'implémentation des dossiers médicaux informatique. En revanche, la majorité des systèmes hospitalier ne peuvent toujours pas facilement (ou de manière sûre) partager leurs données. Conséquence, les docteurs passent plus de temps à écrire qu'à parler avec leur patient. Le burnout chez les médecins généraliste a bondit de 45 à 54 pourcent entre 2011 et 2014 [2].

Bien qu'il existe la notion d'information de santé « individualisé » d'un point de vue clinique ou bien-être, cela n'a pas été traduit en traitements « personnalisé ». De plus, même si il y a pléthore de données, l'ensemble de l'écosystème de santé est incapable de réaliser convenablement une prédiction (ou risque trop de données) sur les futurs besoins médicaux d'un patient.

D'où les solutions actuelles poursuivies par l'industrie technologique de services médicaux ont abouti à un choix difficile entre la violation de la vie privée/la fraude économique et les soins. Nous voyons ce problème s'étendre parallèlement à l'accroissement des données créées par l'industrie. La technologie sécurisé de la blockchain, ses propriétés, et de par sa nature décentralisé peut aider à réduire les coûts, améliorer l'efficacité de ces opérations ainsi que fournir une architecture sécurisé.

1.3 Relation Patient-Prestataire

Le nouveau paradigme de la santé exige le besoin d'une prestation efficace et optimale pour les patients afin d'obtenir de meilleurs résultats en matière de soins. Cela nécessite que les principaux prestataires de soins puissent coordonner et collaborer avec d'autres prestataires de soins impliqués et avec des organismes de santé auxiliaires comme les laboratoires et les pharmacies. Bien sûr, pour que cela soit efficace, les dossiers des patients doivent être mis à jour et modifiés en temps opportun.

Les logiciels de gestion des dossiers médicaux informatique ne permettent pas l'efficacité de la relation patient-prestataire. De plus, ces logiciels ne fournissent que des possibilités d'échanges limités d'un système à un autre et nécessite généralement une personne capable de faire un tel transfert d'information. Cela entraine un retard de plus en plus grand pour les organisations quant à la capacité à rapidement prendre en charge les patients mais aussi à une diminution générale de la qualité de la prestation de service qui leur ai délivré. En outre, comme les prestataires de soins passent plus de temps dans la coordination des soins, leur efficacité à traiter les patients à diminuer tandis que leur travail a considérablement augmenté, ce qui est un impact contre-intuitif par rapport au résultat attendu.

De plus, étant donné que beaucoup de médecins ne veulent pas que leurs patients aient accès à leur dossier médical informatique, ceux-ci ont un rôle passif dans le contrôle de leur santé. Ils ressentent donc évidemment un manque de contrôle sur leur santé et l'amène à être frustré et moins engagé dans ses soins. Bien qu'il y ait une récente augmentation des applications mobile aidant les personnes à surveiller leur santé, ceci ne s'est pas traduit par l'amélioration de leurs soins et de leurs traitements car les résultats ne sont pas intégrés dans leur dossier médical informatique.

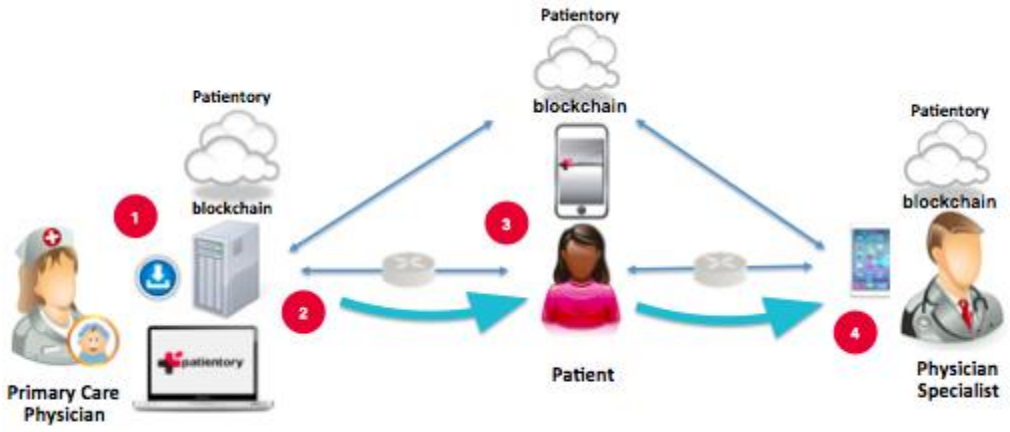

Figure 1 : Schéma de Patientory

2 Vue d'ensemble du système

Ces problèmes peuvent être résolus en utilisant « the Patientory Blockchain Network » (le réseau blockchain Patientory). Les dossiers médicaux informatiques sont centralisés dans des centres de stockages et donc sujet au piratage, à des règles strictes et à des frais onéreux. En mettant en place la blockchain Patientory, les prestataires vont voir la disparition des failles de sécurité et un salon facilitant la coordination des soins ce qui améliorera les résultats. On peut avoir ci-dessus (figure 1) un schéma décrivant l'infrastructure de la blockchain Patientory et son interopérabilité auprès des patients et de leurs fournisseurs.

3 Implémentation du système

3.1 Réglementation HIPAA et directives de conformité

Avant toute discussion sur l'implémentation du système, les restrictions imposées par les lois de l'HIPPA doivent être abordés. Les principales règles reposent sur la confidentialité, la sécurité et le Cloud Computing. Le but de ce livre blanc n'est pas d'effectuer une étude complète de la loi sur l'HIPPA mais des points qui se trouvent être pertinent avec l'implémentation du système doivent être abordé.

A. Règle de confidentialité.

Le business modèle de Patientory implique que certaines exigences en termes de confidentialité soient respectées en raison du stockage et des transmissions informatiques d'informations sur la santé. La loi sur la confidentialité est résumé par « La règle de confidentialité … s'applique aux régimes de santé, aux centres de soins, et à tout organisme de soin qui transmet des données médicales sous forme informatique » [3][4]. En plus de ses agents, d'autres parties qui agissent en leur nom comme prestataires de service sont soumis à l'HIPAA. Ces agents sont appelés Business Associates (BA) et les documents légal auxquels le BA doit adhérer est le Business Associate Contract (BAC). L'HIPAA impose des exigences strictes quant à la nature de ces accords.

Ce qu'il faut retenir de ce premier point, sont les exigences pour avoir l'autorisation d'utiliser des informations anonymisées et la définition de l'information privée. Les données médicales personnelles (DMP) sont définies comme « toutes données médicale individuellement identifiable à une personne détenues ou transmise par une entité [5] ou son BA, que ce soit sous forme informatique, papier ou orale. » [4][6]. Les données médicales anonymisées sont définies elles comme « Donnée médicale n'étant pas identifiable à un individu et à l'égard de laquelle on ne peut pas raisonnablement croire que l'information pourrait être utilisée pour identifier un

individu » [4][7]. Les restrictions d'utilisation des données anonymisées sont les suivantes : « Il n'y a aucune restriction quant à l'utilisation ou à la divulgation de données médicales anonymisées. Celles-ci n'identifient ni ne permettent, sur une base raisonnable, d'identifier un individu. ». [8][9] La frontière entre données identifiable à un individu et non identifiable est définie comme toute information qui peut restreindre le nombre possible d'individus auquel une collecte d'informations est associée à moins de 0.04% de la population totale des Etats-Unis.

B. Règle de sécurité et directives sur le Cloud Computing.

En raison de la taille de ce sujet, seul les éléments les plus importants seront abordés. Ces éléments sont les suivants : « Lorsqu'une entité achète les services d'un fournisseur de service Cloud (FSC) pour créer, recevoir, conserver ou transmettre des DMP (pour les traiter ou les stocker), le FSC est un BA devant suivre la réglementation HIPAA. Ainsi, lorsqu'un BA fait sous-traiter par un FSC, pour créer, maintenir ou transmettre des DMP en son nom, le sous-traitant FSC est aussi lui-même un BA, même si celui-ci ne fait que traiter et stocker les DMP de façon crypté et sans la clé de cryptage. Le fait de ne pas posséder la clé de cryptage n'exempt pas le FSC de ses obligations envers l'HIPAA. Par conséquent, l'entité (ou le BA) et le FSC doivent conclure un « Business Associate Agreement » (BAA) [10] respectant l'HIPAA. Le FSC est à la fois responsable de façon contractuelle du respect du BAA mais aussi directement responsable du respect de ses obligations envers l'HIPAA. » [9][11]

Les entités utilise souvent des FSC pour stocker les informations médicales, en grande partie parce que cela leur est plus économique (moins de coût IT (Information Technology)). Cependant, en procédant ainsi, les consommateurs abandonnent tout contrôle direct sur les données et, par conséquent, ne savent pas qui y a accès et où. Même si un contrat est signé entre le BA et le FSC, celui-ci défini uniquement qui assume les responsabilités en cas de fuite des données médicales. Le consommateur pourrait éventuellement avoir un certains contrôle sur ses données, mais dépend du FSC pour en obtenir les privilèges.

Bien que l'utilisation du cloud soit devenue populaire pour stocker des données, il existe encore un certain nombre de risques auquel le consommateur doit faire attention quand il s'agit d'une utilisation pour des données personnelles. De par le fonctionnement du cloud, les données sont répliquées et déplacées fréquemment, augmentant ainsi les risques de fuites des données ou, plus globalement, d'utilisation non autorisées de celles-ci.

Références

[1]. HIPAA, acronyme anglais de Health Insurance Portability and Accountability Act, loi votée par le Congrès des Etats-Unis en 1996 et qui concerne la santé et l'assurance maladie.

[2]. « A Begoyan. An overview of interoperability standards for electronic health records. » In: (2007.).

[3]. "The Privacy Rule … (applies) to health plans, health care clearinghouses, and to any healthcare provider who transmits health information in electronic form"

[4]. Charles N Mead et al. "Data interchange standards in healthcare itcomputable semantic interoperability: Now possible but still dicult. do we really need a better mousetrap?" In: (2006.).

[5]. A propos des entités : https://privacyruleandresearch.nih.gov/pr_06.asp

[6]. "all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral"

[7]. “Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.”

[8]. “There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual”

[9]. Thiago Vieira Joe Paradiso Andrew Lippman Ariel Ekblaw Asaf Azaria. “MedRec”. In: (2016). www.pubpub.org/pub/medrec.

[10]. http://searchhealthit.techtarget.com/definition/HIPAA-business-associate-agreement-BAA

[11]. https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html