

診療記録に対する情報トリアージによる個人情報管理の提案

A Privacy-Sensitive Information Control Method for Medical Record Cloud by 'Information Triage'

山崎 重一郎^{*1}
Yamasaki Shigeichiro

^{*1}近畿大学
Kinki University

We propose an effective private information control method for the medical record in time of large-scale disaster. A typical application of our proposal is to deliver the urgent medical supplies for the people who refuge the shelters according to their medical records. We propose 'information triage' method, which classify the medical records from the point of the view of the risk of the patient's life and distinguish the way of the control for the records according to the classification. We have implemented the reference systems and evaluate them.

1. はじめに

本研究は、医療機関の診療記録のバックアップを行うクラウド型サービスに対する大規模災害を想定した効果的な個人情報管理方法の提案である。提案するシステムの典型的な用途は、大規模災害時にクラウドにバックアップされた診療記録に基づいて避難所に緊急性の高い医療関連物資を迅速に配送することである。

本研究では、生命の危険に対する重要度に応じて診療情報を分類し、非常時における管理方法を分ける「情報トリアージ法」を提案し、これに関連するシステムの参照実装を行い、その実現可能性の評価を行った。

2. 個人情報の分類の必要性

2.1 デフォルトの権利が本人や社会にとって有害な場合

著作権とプライバシーは、どちらも個人に帰属する情報のコントロールに関する権利という側面を持ち、その権利は情報の発生と同時に自動的に生じる。これは必要な特質ではあるが、状況によっては、本人にとっても社会にとっても有害になることがあり、制限が必要となることがある。

例えば、オープンソースのソフトウェアはライセンスによって、デフォルトの著作権を弱め、一定の条件下での、利用、改変、利用、再配布などを許可することによって利用コミュニティにおける価値を高めている。

個人情報も、目的外使用や第三者提供の禁止、適正な収集、管理、開示、訂正、削除を請求する権利などが自動的に発生するが、この権利のために、診療記録のような生命にかかわる個人情報が必要なときに必要な場所で利用できないという状況が発生する可能性がある。

2.2 大規模災害における診療記録の有効利用

病院の診療記録は、個人情報保護法の下で運用されている。医院や病院は個人情報取扱事業者となっており、診療記録の目的外利用や第三者提供は制限されている。

しかし、大都市の直下型地震や巨大津波などの大規模災害発生時には、病院や医院自身が被災する可能性もあり、患者は病院だけでなく、避難所において生命に関わる医療物資を必要としている可能性もある。このようなときに診療記録の第三者

提供が必要になるケースが考えられる。

2.3 個人情報保護法の例外規定

個人情報保護法には、「本人または第三者の生命、身体又は財産その他の権利利益を害するおそれがある場合」についての例外規定が存在する。これは、個人情報取扱事業者の目的外使用、通知公表、第三者提供禁止に対する例外として規定されている。したがって、個人情報を生命や身体の危険に関するものだけに限定し、適正な管理を行えば、合法的に個人情報を第三者に提供できる可能性がある。

3. 情報トリアージ法

我々は、緊急時における生命への危険度の視点で診療記録を3種類に分類し、生命への危険が高いものから順に赤、黄色、緑の色で分類を表示する方法を考えた。我々はこの手法を「情報トリアージ法」と呼んでいる。

救急医療における「トリアージ」は、多数の患者が発生する事態が起き、必要な医師や治療設備などが提供不可能になったときに、優先的に治療行為を行う患者を選別するという方法である。これに対して本研究は患者の選別ではなく情報の必要性の分類に限定しているという点で概念的に大きく異なる。ただし、非常事態においてのみ適用されるという点では共通している。

赤:直ちに生命の危険がある

黄:数日で重大な健康被害の可能性はある

緑:本人のコントロールに任せる

3.1 医師による情報トリアージの付与

診療記録の情報のトリアージは、医師が診療記録作成時に、医師の判断として処方や検査の付加情報として色分け情報を付与することを前提条件とする。

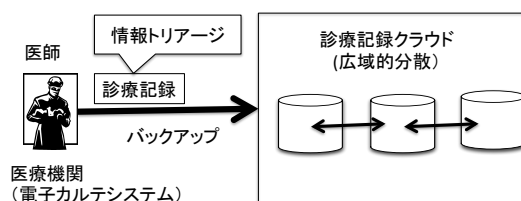


図1 医師による情報トリアージの付与

1.近畿大学産業理工学部情報学科, 福岡県飯塚市柏の森 11-6,
0948-22-5655, 0948-23-0536, yamasaki@fuk.kindai.ac.jp

3.2 情報トライアージが付与された情報の利用ポリシー

オープンソースのライセンスのように、赤や黄のトライアージが医師の判断により付与された診療記録は、それぞれ公開された利用ポリシーに基づいて管理される。そのポリシーの中には「どんな状況において」「誰が」「用途の範囲」などが定義される。

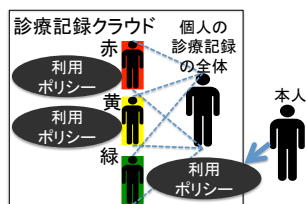


図2 情報トライアージに対する利用ポリシー

4. 参照実装

4.1 診療記録利用の参照実装の全体構成

ここでは、非常時における診療記録クラウドの個人情報と安否確認システムから利用する場合の全体像を、本提案の参照実装に沿って説明する。

この参照実装のシナリオは、大規模災害発生時に避難所で利用される安否確認システムにおいて、避難所の管理者が、避難者の名簿と診療記録クラウドの情報を同期させることによって、命に関わる医療物資の必要性が即時にわかり、それを要請できるようにするというものである。また、緑の情報についても、本人が非常時の流通を望むものと望まないものに分けて流通されるべきである[内山 2004]。

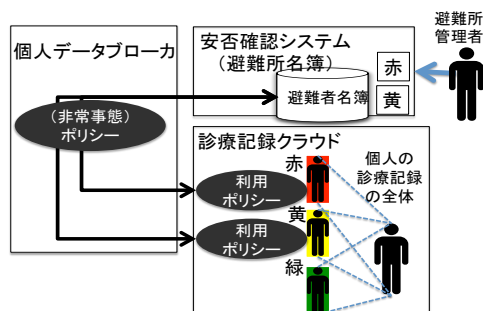


図3 参照実装の全体構成

4.2 診療記録クラウド

地域拠点病院などの連合体が蓄積データを冗長管理するクラウドサービスを想定する。医療機関の電子カルテシステムなどから診療記録の基本情報とそのメタ情報として情報トライアージが付与された情報を管理する。また、Web APIを備え、利用ポリシーに沿って診療情報へのアクセスを可能にする機能を持つ。

4.3 個人データブローカー(情報連携基盤)

診療記録クラウドの個人情報とそれを利用するアプリケーションの間で個人の照合などの情報の横串を通すためのシステムである。

(1) 平常時

情報連携を禁止する。

(2) 非常事態発生時

認定したアプリケーション間の情報連携を活性化する。情報連携を活性化する前に、利用するアプリケーションの登録や利用者の登録、本人確認などを要求する。

(3) 電子令状発行と平常復帰

診療記録情報の流通は非常時のみに許可される。したがって非常時と平常時の区別は非常に重要である。非常時の定義は、災害対策基本法に基づく総理大臣による災害緊急事態の布告に基づくことが自然であろう。また、非常事態が全面的、もしくは部分的に終息したときにも、範囲を指定した明示的な宣言が行われ、平常状態に復帰させて診療記録の流通が停止されることも重要な要件である。

我々は、個人データブローカーの状態を非常事態に変更する操作は、電子令状で行うものとした。典型的にはデータブローカーが行政サービスで、電子令状は裁判所などの司法機関が実施することを想定した。電子令状の記載内容や様式などについては、さらに詳細な検討が必要である。

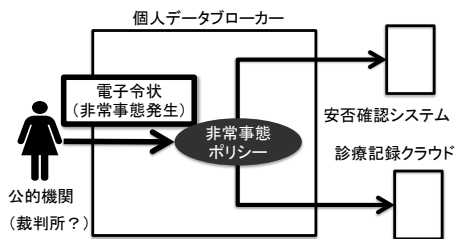


図4 電子令状

(4) 個人識別の突き合わせ

日本人の氏名は異体字を尊重する文化が存在するために照合が難しい。避難所で作成された名簿と診療記録の照合を迅速かつ正確に実施することが本システムの重要な要件となる。

我々は、基本 4 情報(氏名、性別、生年月日、住所) + 氏名の読み仮名、保険証番号、マイナンバー制度などを利用して、避難所名簿と診療記録クラウドの個人照合を行う方針をとった。

5. 評価実装と課題

参照実装は、それぞれのシステムのプロトタイプを Ruby on Rails 3.2 による RESTful な Web アプリケーションとして実装し、API として機能を提供することに主眼をおいた。DB の頑強性は mongo DB のリプリケーション機能を利用して実現した。Web アプリケーションを横断するユーザ認証と認可は、OpenID と OAuth の双方を利用した。これらの Web でよく利用されている技術を利用することは、セキュリティ上の利点と将来にわたるシステムの維持コストの削減の効果を持つ。

我々のシステムへの要求仕様となる、データ規模や性能の想定は難しいが、首都直下型地震や南海トラフによる津波被害などを想定すると、72 時間以内に数万人から数十万人の診療情報の照合が必要となる可能性がある。またクラウドの頑強性と性能評価の前提には電源喪失や通信回線の途絶などの条件も加わる可能性がある。これらは今後の課題である。

また、同性同名などによる個人照合の誤りなどが発生すると、個人情報の漏洩よりもさらに深刻な生命の危険が発生しうするため、速度と正確さの両方が強く要請されるが、この問題も今後の課題である。

参考文献

[内山 2004] 内山映子, 宮川祥子, 太田喜久子 サービス利用者のプライバシーポリシーに基づくインターネットを利用した在宅ケア情報共有システム, 電子情報通信学会論文誌, J87-D-I(12), 1098-1109, 2004-12-01, 2004 年.