東京海上日動リスクコンサルティング（株）
情報グループ
セイフティーコンサルタント　岡村　裕之

医療機関における個人情報保護と情報セキュリティーについて

１.インターネットの普及と意識変革

我が国の２００５年のインターネットの対人口普及率は６６．８％となり、インターネットの利用人口はおよそ８,５２９万人（対前年度比５８１万人増）と推定されている。２０００年の利用人口はおよそ４,７０８万人であったことから、ここ５年間でおよそ倍増したことになる。（情報通信白書平成１８年度版より）また、インターネット利用端末別の利用人口は、２００５年にパソコンが６,６０１万人、携帯情報端末が６,９２３万人となり、２０００年対比では、それぞれ２～３倍に増加している。これは、米国のインターネットの利用人口の１億６３０万人に迫るものであり、生活における情報通信メディアの重要性が、ここ数年間で、急速に増していることを裏付けている。このことは、私たちが情報を入手するときの媒体が、従来のメディアであるテレビ・新聞・ラジオ・書籍・雑誌等から、インターネット・携帯電話等へと拡大しつつあり、今日、これらの媒体は、他の情報通信メディアを脅かす存在にまで成長し、私たちの生活に必要不可欠なものとなってきていることを示している。子供からお年寄りまで、知りたいことはキーボードを叩き、Ｗｅｂに聞くような環境にある。このような環境変化のなか、わが国は、かつて経験したことのない少子高齢化社会に突入し、今や多くの国民の最大関心事は「健康」であり、国民の医療に対する意識は近年大きく変化し、国民が医療に求める品質も年々厳しくなってきている。

インターネットの普及により、従来はできなかったインタラクティブな検索が可能となり、インターネットで病院の手術歴を調べる、医師をチェックする、薬を購入する、人間ドッグを予約するなどインターネットと医療との係わり合いが深まり、信頼のできる医療情報が求められるようになってきている。また、医療機関と個人（患者）との関係も、医療機関と医療消費者（コンシューマー）という立場へと変わりつつあり、個人が、医療健康Ｗｅｂサイトに自らアクセスし、個人情報を登録する機会も増えている。インターネットで商品を購入する（電子商取引）際に感じる一抹の不安（漏洩・目的外使用等）も同様に抱いていることが窺われる。このような環境変化のなか、医療機関における最近の個人情報の漏洩事件は次節のようなものがあり、インターネット利用人口に比例して増加している。

http://www.tokiorisk.co.jp/

２.医療機関の個人情報漏洩事件

近年、医療機関の個人情報漏洩事件は、電子商取引における漏洩事件と同様に多発しており、ここ数ヶ月間でも、以下のような事件が起こっている。　個人情報保護法が完全施行された２００５年前後以降、医療福祉分野における個人情報に係わる漏洩事件件数（インシデント）も、大幅に増加している。医療機関における電子カルテ・オーダリングシステム等の導入等により、ネットワーク化が進み、医療機関同士の情報化の進展とともに、個人情報が病院内のみならず、病院間、病院調剤薬局間、病院から審査支払い機関へと送信（紙ベースでは年間３億５千万枚相当）され、情報の迅速化・医療事務の効率化が図られつつあるが、その一方では、個人情報漏洩リスクも情報化の進展と相俟って高まりつつある。医療機関の個人情報の安全性・情報セキュリティーの脆弱性等をどう克服するかが今後の課題であり、医療機関はその対応に迫られている。

【事件例】（ホームページより）

１月１０日　Ｔ大学医学部付属病院：医師が、２００４年から約３年間４１７人の個人情報を誤送信。

３月１２日　株式会社Ｔ：医師４８名分の個人情報の記録されたＰＣを紛失。

３月２６日　東京Ｎ病院：患者１６４人分の個人情報が記録されたＰＣ及び患者１名の画像診断記録が保存されたＣＤを遺失。

４月　７日　Ｒ病院：退職した医師のＰＣ２台が盗難にあい、患者情報１４４名分の個人情報が漏洩。

４月１３日　Ｋ医科大学付属病院：患者情報２４８名分を含む看護職員の私有パソコンが盗難。

【医療福祉分野の個人情報漏洩インシデント件数の経年変化】

（２００２年～２００６年）

(件)

	2002 年	2003 年	2004 年	2005 年	2006 年
個人情報漏洩インシデント件数	62	57	366	1032	933
うち医療　福祉分野のインシデント件数（割合から算出）	―	2	21	54	39

（出典：NPO ﾈｯﾄﾜｰｸｾｷｭﾘﾃｨｰ協会 2002 年～2006 年個人情報漏洩インシデント調査結果）

個人情報漏洩事故は、紛失、不正アクセス等の人為的なものが多く、その結果、金と信用と多くの時間を失うことになる。例えば、お詫びのための心付けの支払い、事件のための報道機関向けの対策も必要となる。また、被害者から損害賠償請求があれば、慰謝料、弁護士費用、損害賠償金、訴訟費用等の支払いもしなければならない。原因究明のための調査費、従業者再教育費用、セキュリティー再構築費用等もかかる。対外信用の失墜、減少する患者、院内信用の失墜、従業者モチベーションの低下も考えられ、被害者への対応、再発防止対策会議等にも時間がとられ、その損害は多大である。

３.医療機関の情報化動向

医療機関において患者等の個人情報は、院内では、主に診療記録（カルテ）や診療報酬請求書（レセプト）、オーダリングシステム、部門システム、ホームページ等で扱われるが、医療・保健・福祉分野の情報化は、２００６年１月１９日の政府ＩＴ戦略本部において、今後の重点施策のひとつに取り挙げられている。医療分野の情報化は、一般企業と比較して、遅れていると言わざるを得ない状況にあるため、今後情報化が進展するなか、個人情報の漏洩、ネットワーク上での成りすまし、ホームページ・サーバーの改竄等の事故が起こり、対応によっては社会問題化するものも増加すると思われる。今後の１０年乃至１５年が医療機関情報化の正念場であり、個人情報保護を含む安全で安心な情報提供ができる体制作りが急務となっている。厚生労働省は、「保険健康分野の情報化に向けてのグランドデザイン」を２００１年に策定し、その中で、電子カルテは、２００４年度までに全国２次医療圏[1]毎に少なくとも１施設の普及を図り、２００６年度までに全国４００床以上の病院と全診療所の６割以上に普及させる計画を立て、レセプト電算処理システムは、２００４年度までに全国の病院レセプトの５割以上、２００６年度までに７割以上に普及させる計画を立てた。しかし実際は診療報酬の改定が行われるなか、多くの病院は経営も苦しく、一部の病院では統廃合が起こるなど、医療機関の情報化は２００１年のグランドデザインよりも遅れ気味の感がある。このような状況下、先のＩＴ戦略本部において、ＩＴによる構造改革が謳われ、２００６年度からの（２００７・３・２７発表）の「医療・健康・介護・福祉分野の情報化グランドデザイン」が策定された。このなかで、前述のレセプトオンライン化等の推進も含め、生涯を通じた健康情報の電子的収集と活用が謳われ、日常の健康状態や診療の場で活用するための検診情報・診療情報等を書き込んだ「社会保障番号」の制度化が検討されている。社会保障番号は住民基本台帳カードに近いものであるが、個人の医療情報から被保険者証、年金、介護保険証書、雇用保険証等の情報も入力され、高度でかつセンシティブな個人情報が収集されることとなり、そのカードの意義は大きいが、情報漏洩時のリスクも大きく脅威となる。医療情報のネットワーク化に対応した個人情報保護や情報セキュリティーへの対策が今後の重要なタスクになる。そこで個人情報保護と情報セキュリティーの観点から、インターネットの急速な普及と今後の医療制度改革を睨んで、医療機関の個人情報保護とセキュリティーについての考え方について以下に考察してみる。

４.医療機関における個人情報保護と情報セキュリティーについての留意点

１）医療機関における個人情報保護及び情報セキュリティー関連法規

医療機関における個人情報保護と情報セキュリティーに関する関連法規を上位法規から考えてみると、憲法では「個人情報」という文言はどこにも出てこないが、１３条に幸福追求権としてのプライバシー権が謳われている。しかしレセプトの被保険者番号や請求金

[1] 健康増進から予防・診断・治療・リハビリに至るまでの包括的医療サービスを提供する医療単位　全国３６０圏　（概ね県のなかを４～５分割してある）

額等まで、憲法で謳われているプライバシー権であるかと考えると、少し距離があると思われる。時折、個人情報保護とプライバシー保護を混同している発言が聞かれるが、プライバシーに係わる情報は「みだりに人に知られたくない、開示を望まない、私生活を公開されない権利」であるが、個人情報であるにも拘わらず、プライバシーに係わる情報と誤解していることもある。では刑法で考えてみると、１３４条の医師等の秘密漏洩罪が個人情報漏洩を規制するものとして考えられるが、Ｗｅｂや携帯電話で他人のメールアドレスを送信した場合などを考えると、秘密漏洩という概念とはかけ離れていて、不十分である。民法上の不法行為、善管注意義務違反等による損害賠償請求も考えられるが、挙証責任のハードルは高く、民法のみでは適切でない。このような状況下、２００３年に成立した個人情報保護法は、我が国の法律としては珍しく、行政法とも民法とも言えず、消費者の立場から謳われ、時代の趨勢を感じさせる法律のひとつであった。当初は米国のように医療（ＨＩＰＡＡ[2]）、通信、金融の各セグメント別の個人情報保護関連法規が作られる予定であったが、結果的には１つで全体をカバーすることになった。医療機関も例外となることなく、本法律及び「同施行令」の適用となった。個人情報保護法ではこの法律に加え、厚生労働省「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」で患者と医療機関に関する個人情報の適切な取扱いが求められている。その他、日本医師会「診療情報の提供に関する指針（２版）」、厚生労働省「医療情報システムの安全管理に関するガイドライン（２版）」等もある。（国公立病院等は別の法令等でカバーされるが、同様に遵守することが期待される。）また日本規格協会の「個人情報マネジメントシステムJISQ15001」並びに「情報システムマネジメントシステム（JISQ27001）」、「医療機関向けＩＳＭＳユーザーズガイド」等も考慮に入れる必要がある。

２）医療機関における個人情報保護に係わる用語の適用対象

医療機関に係わる個人情報保護に関する用語及びその適用には、その特殊性並びに特異性があり、以下にその幾つかを紹介する。

①個人情報

個人情報保護法では生存する個人の情報を指すが、医療機関においては、死後を含む患者等の個人を特定できる情報のすべてをその範囲とすることが求められている。（氏名、生年月日から既往症、診察の内容、検査結果さらに診断、評価等）

②匿名化（無名化）

新薬治験等で、医学研究・学術研究のために個人情報を提供する場合は、個人情報の一部又は全部を削除又は加工し、特定の個人を識別できない状態にする。（他の業種でも同様な対応が考えられ、リスクの低減に有効である。）

③診療情報等

診療過程での記録で、患者基本情報（識別記号・番号、保険者、有効期限、氏名、年齢、生年月日、住所、電話番号等）診療録、手術記録、麻酔記録、画像データ、検査記録、看

[2] Health Insurance Portability and Accountability Act「医療保険の移転とそれに伴う責任に関する法律」

護記録、紹介状、同意書、介護記録、相談記録、処方箋、調剤録、健康保険証、生活背景情報（生活パターン、家族構成）等で個人を特定できる全ての診療記録を指し、センシティブな情報である。

④従業者

院内で直接間接に事業者の指揮・命令下で業務に従事するもの全員であり、正職員、嘱託職員、派遣職員、臨時職員、理事、監事等を指す。守秘義務の側面から考えると退職者も考慮する必要がある。業務委託契約を結んだ事業者に雇われ、業務に従事する者は、委託先事業者において、医療機関の定めた規則と同程度の扱いを定め、管理する必要がある。

３）医療現場における個人情報の取り扱い

医療機関で扱う個人情報は、患者の診察時のみならず、職員の他施設への異動時にも取り扱われ、医療機関内の異動や新人の募集、退職時等さまざまな局面で扱われる。紙ベースのものもあれば、データとして保管されるものもある。これらの膨大な個人情報を適切に管理するためには、院内の体制作りが必要であり、具体的には、最高責任者は院長、管理責任者は事務長（ＣＰＯ[3]の設置）、実施責任者は各部門長、監査責任者は理事または外部監査機関が担当し、関連規程策定の上、実行を担保することが第一である。

患者の個人情報は、診療過程において、診療の申し込みや患者の診療情報を通して蓄積され、その個人情報が利用・提供・開示されることを告知する必要がある。特に他の医療機関や委託業者、薬局、検査委託機関へ個人情報が提供される場合、どのような個人情報をどのような目的で利用するのかを、プライバシーポリシーとは別に、ホームページ（又はパンフレット）等に掲載する必要がある。また、よく議論になる患者名札の扱いについても、医療過誤からの事故防止を優先し、病室、ベッド脇に表示することをホームページ（又はパンフレット）に掲載し、患者が容易に知り得る状態にしておくことが望ましい。また、病院の構造設計上の問題ではあるが、仕切りがカーテン１枚であるため、医師の診療内容が待合室に漏れる点などは、情報漏洩リスクとしての配慮が必要である。診療過程以外でも個人情報は、医療費請求、医学研究、教育、行政機関等に開示・利用・提供するので、どのような個人情報が、何の目的でどこへ提供されるのかを同様に掲載する必要がある。例えば、レセプト情報を、医療費請求のため審査支払い機関や保険者へ提供する、新薬治験のため匿名化した個人情報を製薬会社へ提供するなどである。また、患者の権利として、個人情報の所有者である患者は、当該個人情報の訂正・追加・削除、消去、利用停止、第三者提供の停止並びに開示請求を、医療機関に対し一定の条件のもと、請求できることも明示すべきである。特に診療録等の開示については、内規に基づき、担当医師の説明の上、写しの提供ができることを記載すべきである。

４）医療現場における情報セキュリティー

医療現場のＩＴ・ネットワーク化は、前段で記述したように遅れてはいるが、仮に政府の計画に従い実行されるならば、この１０年くらいで、相当なネットワーク化が進むだろ

[3] Chief Privacy Officer

う。しかし情報の進展化に伴い不正アクセス、ウィルス、内部犯罪、システム障害、盗難等の問題が発生し、例えばＳＱＬ（データの検索、変更、削除をする言語）注入によるデータ改竄、搾取やＷｉｎｎｙ（ファイル交換ソフト）による情報漏洩、サーバー・ＨＰへの攻撃等の対策等が必要となる。また、情報資産を保全するために、ＩＤ、パスワード管理の徹底、入退室記録の聴取、業務委託時の契約締結、カルテ保管庫の施錠、医師・看護師等のクリアデスク、クリアスクリーンの徹底等も推進すべきである。コンピュータに格納された診療録等は、機械的故障により情報が消失したり毀損したりしないよう各部署において適宜バックアップの措置を講ずる必要もある。またＰＣ本体の管理、紛失などにも注意を払い、情報資産に無頓着と言われることのないようにする教育も重要である。

これらを徹底するために

①情報資産管理台帳を作成し、資産の価値をグレード分けする。

②職員の対応が鍵となるので、守秘義務契約等の人的セキュリティー対策を行う。

③防火、防水、耐震、施錠等の物理的なセキュリティー対策を行う。

④情報処理設備の管理とアクセスの管理を行う。

⑤システム開発時には、セキュリティーの概念を予め盛り込み開発する。

等を実施すると供に、定期的なセキュリティー監査が、リスク軽減のポイントとなる。

５）個人情報漏洩事件や情報セキュリティー問題が発生した場合

仮に個人情報漏洩事件や情報セキュリティー問題が発生した場合、対処すべきこととして、まず漏洩継続の阻止を図ることであり、次に当事者・被害者・患者家族等への連絡を行い、新たな被害を防止する必要がある。さらに類似案件の発生回避の観点から可能な限り事実関係を公表することである（隠すことはマイナス）。また、苦情対応セクション（患者相談窓口）を設け、真摯な対応が必要である。例えば、通話料は着払いとし電話番号はＷｅｂ上の見やすいところに明記し、無用なトラブルをさけるように心掛けたい。一方、漏洩者が媒体ごと持ち出した場合は窃盗罪で、データを持ち込んだ媒体にコピーして持ち出した場合は不正競争防止法で処罰できる。また不正アクセス禁止法によってハッカー等の行為は罰せられるので、捜査機関との連携も必要である。事故発生後の記者会見（大組織の場合）では、経緯を説明し謝罪する必要がある。賠償請求に備えて、保険加入等も考慮し、またコンサルタント等の専門家を入れ、再発防止策を策定し、院内に徹底することも重要である。

５.最後に

インターネットの普及、国民の医療に対する意識の変革、少子高齢化、医療費の抑制、医療機関の情報化が進展するなか、医療関連機関（介護、薬局、保険者、審査支払い機関、製薬会社、ＳＭＯ[4]、ＣＲＯ[5]、健康産業等）も含め、情報セキュリティー、個人情報の取り扱い等の問題が目に付くようになってきた。情報化の現実から後戻りはできない状況下、

[4] Site Management Organization(医療機関の治験業務を支援する機関（会社）)

[5] Contract Research Organization(製薬企業からの開発業務受託機関（会社）)

http://www.tokiorisk.co.jp/

一人ひとりの日頃の行動・意識改革を含め、如何に現実的にこの問題に対処していくかが、今後の課題である。

以上

参考文献　資料　医療の個人情報保護とセキュリティー（有斐閣）開原成允 樋口範雄 著
医療バイオ医療ＩＴ入門（薬事日報社）真野俊樹 著
日本医師会、国内各病院　患者さんの個人情報の保護に関する院内規則
東京都済生会中央病院　「個人情報のお取り扱いについて」