保健医療福祉分野における個人情報保護の取り扱いに関する研究

主任研究者　山本　隆一　　東京大学大学院情報学環　助教授
分担研究者：
大江　和彦　東京大学付属病院企画運営情報部　教授
開原　成允　(財)医療情報システム開発センター　理事長
清谷　哲朗　関西労災病院医療情報部　部長
公文　　敦　(財)医療情報システム開発センター　課長

A．研究目的

高度情報通信社会の急速な進展、個人情報保護への関心の高まり、データ保護に関するＥＵ指令やHIPAA法に関連した諸外国のプライバシー保護、セキュリティの規制の変化等から、我が国においても保健医療分野での個人情報保護のあり方に関して、国際動向や現在のセキュリティ技術水準を踏まえた一定の方向性を示すことが緊急かつ重大な課題となっている。来年年４月に完全実施される個人情報保護関連についても、各分野ごとにガイドラインを作成する等の対策が求められている。

本研究は、保健医療分野における個人情報の取扱い上の課題を整理し、ガイドラインを研究することにより、保健医療分野の個人情報保護対策の推進に資するものである。

B．研究方法

平成15年度

（１）個人情報保護関連法制定に関する現状及び問題点に関する調査

成立し、基本理念と行政の施策に関する部分１～３章は即日実施されたが、あくまでも個人情報保護の基本を定めた法律であり、すべて実施された場合でも、各分野での具体的対策はかならずしも明確ではない。そこで本研究では保健医療福祉分野における個人情報保護に関する論点を整理し、医療分野、特に臨床現場及び診療報酬請求過程における個人情報の取扱いに関し、運用及び技術面での対応や課題の解決策について検討する。

（２）米国HIPAA法施行後の状況に関する調査

平成15年４月より、米国HIPAA法に関連したプライバシー保護基準が施行されるにともない、政府側の広報や普及策を調査する。また、医療機関、保険会社、代行機関における実施状況や今後の課題を調査する。必要に応じて、米国内での研究成果を取り入れるとともに、米国で調査を行う。

（３）米国以外の国おいての診療情報と個人情報保護の関連について調査するとともに、ISO TC215で作成が検討されている国際間の診療情報交換におけるデータ保護指針についてもISO国内対策委員会等を通じて調査を行う。

C．研究結果

（１）米国におけるHIPAA法の施行状況の調査

分担研究者の清谷と公文が2003年9月にBaltimoreで開催されたNational HIPAA SUMMITに参加し、米国のHIPAA法および関連規則の制定に中心的役割を果たしているBraithwaite博士、the Centers for Medicare & Medicaid Services (CMS)のDr. Stanley Nachimson, HIPAA Privacy Standardsの米国大学関連病院での対策ガイドライン作りに中心的役割を果たしたDuke UniversityのDr. J. David Kirbyにインタビュー調査を行った。これらのインタビュー結果には個人情報保護面だけではなく、電子請求や標準化に関するものを多く含まれるが、ここでは個人情報保護

に関連する結果を以下に示す。
A. Privacy Standards について（Dr. Kirby）
○HIPAA Standards では診療基本３目的（Treatment, Payment, Operation）に関する患者の了承がオプショナルになったが、州によっては書面での了承を求めている。
○患者の関心は高い人と低い人に分かれる。高い人には芸能人や社会的地位の高い人が含まれる。
○UCLA の研究によれば、電子カルテを扱う職員のうちの半分は、スクリーニングサービスを行うためにアクセス権を利用しているという結果が出ている。
○HIPAA 法では、法違反に対する罰則が極めて厳しくできている。（意識の低い覗き見－innocent record reviewer も対象となっている）
○ハーバード大の実験（システム）では、患者は、誰が自分の記録にアクセスしたのかを確認することができるようになっている。米国では医療機関内で、一人の医療記録にアクセスするヒトは平均して 50 人ほどいるといわれているが、ハーバードの場合は、上記のシステムを導入して2-3か月でアクセス数が減少する結果がみられた。とはいえ、1年に 2-3 回は、患者のいとこ、前夫といった資格の人間が患者の状態を確認しようとする現象がおこっている。
○以前は、（患者の知名度高い場合や事件性がある場合などの）場合によって、患者の容態について記者発表することがあったが、HIPAA 法施行後は全くなくなった。ただし、公衆衛生上のプライオリティが高いときなどは例外である。
○HIPAA 法 Privacy Standards 施行の準備期間の目安と予測については、200 床未満の小規模医療機関では約 1 年間、大学病院クラスでは 3-4 年間と考えられる。
○大学病院クラスの場合、システムの変更や研修など、直接的な投資が 100 万ドル、間接的な投資は 20-40 ドル×全従業員数／年と考えられている。
○Privacy 保護に関する有能なコンサルタントは極めて少ない。
B. Medicare, Medicaid から見た医療機関の準備状況（Dr. Nachimson）
○多くの医療機関が HIPAA 法全体への準備不足の状態にあると考えられるが、そのなかでは Privacy Standards への対応に対する努力が優先されているようだ。
○準備は、ソフトの組込みやシステムの変更等が困難で、予測を上回る作業量となっている。また医師が医療機関に Social Security Number を知らせることを拒んでいる。これらの理由により、医師や医療機関における実証テストの導入そのものが難しく、テスト期間が長引いている状況にある。

（２）個人情報保護のための既存基準や指針の調査

個人情報保護のための基準や指針がわが国をはじめ諸外国、および国際団体に存在する。その代表的なものとして、JIS Q 15001 とそれに基づくプライバシーマーク認定制度および米国の HIPAA Privacy Standards に関して調査を行った。

イ．　JIS Q 15001 とプライバシーマーク

日本において OECD の個人情報保護に関するガイドラインと同時に作成された勧告、つまりガイドラインに従った制度整備を行うために導入された基準および認定制度で、財団法人日本情報処理開発協会（JIPDEC）が管理と運用を行っている。JIS Q 15001 自体は汎用的な基準であるが、同協会が医療関連機関向けのガイドラインを作成し、それにしたがった認定も開始している。
基準の内容は一般論としては充実しており、個人情報保護関連法の要求を満たすものと考えることができる。一方で基準自体には例えばプライバシ

一に機微な情報として思想や信条とともに医療に関する情報があげられ、原則収集禁止とするなど、保健医療福祉分野にはそのまま適用することが難しい項目が含まれている。主任研究者の山本および分担研究者の清谷が参加して JIPDEC が作成した医療関連機関向けの指針にはこのような問題点が一応は解決されている。ただし次項で述べる米国の HIPAA Privacy Standards に比べると、具体性と詳細性の程度はやや低いと考えられる。
この指針はA．JIS Q 15001 の要求事項、B．医療機関としての解釈、C．最低限のガイドライン、D．推奨されるガイドラインの４つの項目に構造化されており、これは主任研究者の山本も参加して作成した後述する米国大学関連病院の HIPAA Privacy Standards 適合のための指針と同じ構造をとっている。
たとえば JIS Q 15001 4.4.2.3 の情報収集禁止の項では以下のようになっている。

A．JIS Q 15001 の要求事項
次に示す内容を含む個人情報の収集、利用又は提供は行ってはならない。ただし、これらの収集、利用又は提供について、明示的な情報主体の同意、法令に特別の規定がある場合、及び司法手続き上必要不可欠である場合は、この限りでない。
a）思想、信条、及び宗教に関する事項。
b）人種、民族、門地、本籍地、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項。
c）勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。
d）集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。
e）保健医療及び性生活。
B．医療機関としての解釈
４．４．２．３の項目は一般的な情報収集と保健医療福祉分野での情報収集でもっとも大きな違いが見られる事項である。人種、民族、身体・精神障害および保健医療に関する情報収集は診療の遂行に関して必須であり、保健医療福祉分野では特別に扱う必要はないと考えられる。また思想、信条、犯罪歴でさえも精神疾患などでは収集目的の達成のために必要な場合がある。したがってこれらの禁止項目は保健医療福祉分野の場合、取得目的の範囲を超えた場合のみに適用されると考えるべきである。ただしこれらは特にプライバシーに敏感な項目であるために挙げられたことに十分留意するべきで、これらの項目を収集する場合は特に利用範囲が診療の遂行のための限度内であることを確認する必要がある。
プライバシーに敏感で医療の遂行上必要な情報は少なからず存在する。これらの情報収集には慎重でなければならないが、複雑な手続きを規定すると診療の遂行が困難になることもあり得る。このような情報は診療の専門性によってもことなるために一概に判断することは困難である。その医療機関の実態をよく把握し、日常的な情報収集で少しでも曖昧さがある場合はあらかじめ倫理委員会で方針を決めるなどの、説明可能な対策が求められる。
特殊な例として、宗教法人が運営する医療機関などで信者か否かを受診時に確認する場合がある。これも宗教に関する情報収集にあたる。医療面からの必要性は乏しく、安易に収集すればプライバシーの侵害にあたる。このような場合は、初診申し込み前に宗教に関する質問があることを通知し、回答を拒否できるようにするべきである。またホスピス等で本人の宗教によってケアが異なる場合ために情報を収集する場合がある。診療上の必要性はあると考えられるが、止むを得ないかどうかは判断が困難である。このような場合にも、事前に通知し、回答を拒否できるようにしておくべきある。
C．最低限のガイドライン
以下のａ～ｅの項目については、原則として情報を収集してはいけない。ただし診療の遂行上情報の収集を避けられない場合はその理由が自明でない限り、その理由を診療録等に明記した上で収集することができる。その場合も利用は診療上必要な範囲内

にあることに特に注意しなければならない。診療上の理由が自明とは性生活そのものが健康上の問題である場合の性生活に関する情報や、思想、宗教、犯罪歴などが妄想などの精神症状に強く関連している場合であって、安易に自明と判断してはいけない。

a） 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。

b） 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。

c） 思想、信条、及び宗教に関する事項。

d） 門地、本籍地、犯罪歴、その他社会的差別の原因となる事項。

e） 性生活。

D. 推奨されるガイドライン

C. に加えてこれらの項目の情報収集を行う場合、診療上の必要性が自明でない場合、可能な限り事前に倫理委員会の了承を得る。事前に倫理委員会に諮ることが出来なかった場合は事後に倫理委員会に報告し、その際、不適と判断された場合は当該情報を抹消する。

例えば不妊外来での性生活に関する情報収集のように診療上の必要性があって、かつ日常的に収集されることが予想される場合は、あらかじめ一括して倫理委員会等で検討を行い、必要性を明確にし、個人情報保護上の配慮を具体的に定めておく。このような過程を経た情報収集はその必要性と配慮がある前提で、個々に特別な手続きを経ずに収集することができる。

ロ．米国 HIPAA 法 Privacy Standards

米国 HIPAA 法の Privacy Standards（以後 Privacy Standards）は 2001 年に一度制定され実施が決まったが、米国連邦政府の政権交代にともなって見直されたもので、最終版は 2002 年 12 月に改定され、大規模医療機関では 2003 年 4 月から実施されている。2001 年版は診療に関わるすべての情報の取得段階で診療をはじめとするすべての利用目的を本人に提示し、文書による同意を義務付けていたが、2002 年版は診療自体、診療報酬請求、および医療機関の組織の維持運営管理の 3 つの利用目的に限って同意は必須ではなくなったことが主な変更点である。Privacy Standards 自体は前文を合わせると 3 段組で 400 ページ程度あり、条文だけでも 30 ページを越える。以下に主な項目の邦訳をあげる。

1．プライバシールールの規制機関・対象機関・提携事業者

1-1 規制機関

1-2 対象事業者

1-3 提携事業者

2．プライバシールールで保護される情報・保護されない情報

2-1 個人識別医療情報と保護対象医療情報

2-2 個人匿名化情報

3．医療情報の利用および提供

3-1 基本原則

3-2 診療、支払、または医療機関業務での利用・提供

3-3 同意または異議申し立ての機会を伴う（簡易な許可でよい）利用および提供

3-4 公益目的での医療および提供

3-5 限定されたデータセット

Privacy Standards の特徴は極めて詳細かつ具体的であることで、医療分野に特化して作成されているために、現場が遭遇する場面を網羅することを目指している。ただし、詳細かつ具体的である反面、微妙な例外事態が起こることが予想され、かえって現場が判断に迷う可能性もある。米国では大学関連病院がさらに詳細に起こりうる事象を検討し、対策をまとめた指針を作成しているが、このような可能性に配慮したものであろう。ただし、この指針は 1000 ページを越える大部である。

D．考察

平成 15 年 5 月に個人情報保護関連 5 法案が成立し、17 年 4 月の実施が決定された。保健医療福祉分野では何らかの具体的指針を至急に検討する必

要がある。2003 年 4 月から米国では HIPAA Privacy Standards が発効し、実際の運用が始まっている。本年度の研究でこの状況を調査したが、現時点では大規模医療機関に限定されているとは言え、先進的な少数の医療機関を除いて対応にかなり苦慮している状況があきらかになった。経費も数億という推定もあり、が国でも十分な配慮のもとに個人情報保護対策の指針等を作成しなければ、混乱を来たす可能性は否定できない。

実際に指針を作成するにあたってはある程度は具体的なものでなければ現場が対応に苦慮することは明白であるが、どの程度詳細で具体的にするかは慎重に検討する必要がある。また当初より高度な確実性を求めるか、漸進的な手法をとるかも重要な判断となる。米国の Privacy Standards は具体的な条件や対策を詳細に記述しているが、罰則を背景とする規則である以上は確実性を求めている。つまり Privacy Standards が実施された時点で、そこに記載されている要件は確実に満たさなければならない。したがって米国政府は Privacy Standards を Minimal standards と捕らえている。これに対して JIS Q 15001 は詳細な実施計画（コンプライアンスプログラム）の作成とその実施が主体であり、コンプライアンスプログラムには「計画→実施→監査→計画の見直し→実施・・」といった見直しを含む繰り返し(PDCA サイクル)を基本にしている。つまり、継続的に改善することを保障する体制に主体が置かれている。このような手法は ISO 9000 シリーズにおける品質管理や、BS 7799 における情報セキュリティマネージメントと基本的に同様な手法で、確実性は保障されない反面、新たな事態に容易に対応できる利点がある。わが国の保健医療福祉分野では理論的な個人情報保護の状況は前述の先行研究を見ても十分とは言えないが、実際に患者との間で深刻な問題になっている事例は極めて少なく、また一方で多くの保健医療福祉機関は経済的にも人的にもそれほど多くの余力はない。このような状況でのさらなるプライバシー保護の達成のための戦略は保障レベルの設定と対策体制のバランスに十分考慮したものにする必要がある。

F．発表

【学会発表】

1．　第 7 回日本医療情報学会春季学術大会チュートリアル「医療と個人情報保護法」、2003 年 6 月、小倉

2．　医療のセキュリティと個人情報保護、開原成允、樋口範夫編、有斐閣、東京、2003、ISBN 4641129339

3．　第２３回医療情報学連合大会チュートリアル「診療情報のセキュリティと個人情報保護」

【書籍】

1．　開原成允、樋口範夫編、「医療の個人情報保護とセキュリティ」、有斐閣、東京、2003、224 ページ

【雑誌】

1．　山本隆一、医療情報のセキュリティとプライバシー保護、映像情報 Medical、Vol. 35、No. 14、2003

2．　山本隆一、個人情報保護の観点からの診療情報開示と記録整備のあり方、看護展望、Vol. 29、No. 2、2004