

200401004A

厚生労働科学研究研究費補助金

医療技術評価総合研究事業

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

平成16年度 総括研究報告書

主任研究者 山本 隆一

平成17（2005）年4月

目 次

I.	総括研究報告書		
	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	-----	1
	山本 隆一		
	資料	-----	20
II.	分担研究報告書		
1.	米国 HIPAA Privacy Standards 実施状況の調査	-----	37
	清谷 哲朗、公文 敦		
III.	研究成果の刊行に関する一覧表	-----	47
IV.	研究成果の刊行物別冊	-----	48

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 総括研究報告書

主任研究者 山本 隆一 東京大学大学院情報学環 助教授

研究要旨 個人情報保護関連 5 法案が成立し、わが国も法律の裏づけを持って個人情報保護を考える時期に入った。本研究は扱う情報がほぼすべてプライバシー情報であり、利用目的が複雑で公益利用も重要な保健医療福祉分野での個人情報保護の取り扱いを研究することが目的で、法律の全面実施直前の現状調査、諸外国（特に米国の HIPAA Privacy standards）の調査などを通して保健医療分野で個人情報が適切に取り扱われるための施策を検討した。

分担研究者：

大江 和彦 東京大学附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 法に関連した米国規則など、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。また国会においては、平成 15 年 5 月に個人情報保護関連 5 法案が成立し、平成 17 年 4 月の実施が決定されており、保険医療福祉分野でもさまざまなガイドラインが作成されて実施されようとしている。

本研究は、保健医療福祉分野における個人情報の取扱い上の課題を整理し、米国の HIPAA Privacy Standards を含めて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。

なお本研究は分担研究者を4名おいているが、会合およびインターネット上での共同作業が大部分を占め、経費も一括計上としているために、報告書は一部の分担研究を総括報告書に含めて記載する。

B. 研究方法

B-1. 出版等による知識普及活動

昨年度に引き続き、医療における個人情報保護のあり方に関する出版を行い、また医療機関、医療関連職能団体、医療機器業界団体などで積極的講演会を開催し、医療における個人情報保護への関心の鼓舞と知識の普及に努めた。

B-2. 米国 HIPAA Privacy Standards 実施状況の調査

米国会計監査院によって、保健医療情報を保護するための医療機関、保険者等の責務について規定している HIPAA 法 Privacy 規則について、①医療機関と保険者における Privacy 規則遵守の実績、②公衆衛生関連機関、研究者、患者の代理人が患者の医療情報にアクセスする際の実績、③患者が自らの権利について理解する限界等について調査しており、この結果を分析した。

医療情報管理システム協会(HIMSS)によ

って、医療機関及び保険者等を対象に HIPAA 法準拠の状況について調査しており、この結果を分析した。

米国の医療機関及び保険者においては HIPAA 準拠のために弁護士等の資格を有するコンサルタントと契約する傾向にある。フロリダ州にある法律事務所で HIPAA 法専門の医療コンサルタントを行っている弁護士に、現在の医療機関等における HIPAA 法 Privacy 規則の遵守の状況や医療機関の負担と課題、実情について聴取した。

B-3. 医療情報システムの安全管理に関するガイドラインの検討

個人情報保護法（関連3法）は対象分野を限定しないために、きわめて抽象的で、情報セキュリティのように、あくまでも相対的な評価しかなしえない対策においては基準を定めることが難しい。そのために、関係省府は指針を定めている。本研究では経済産業省の指針と厚生労働省の医療・介護関係事業者における個人情報の適切な取り扱いに関するガイドラインを精査し、要件を抽出した。

平成6年に医用画像の電子保存を容認する通知が出され、その際に基準と指針が作成されている。また平成11年にいわゆる電子保存の容認通知が出され、基準と指針

が作成された。また海外では HIPAA 法の実施にあたって、米国厚生省が security standards を省令として定めている。これらを精査し、要件を抽出した。

以上で抽出した要件の中で、電子保存等の特別な行為に依存しない一般的な安全管理対策を基礎として、厚労省、経産省の2指針の要件を加味し、安全管理指針を作成した。

B-4. 医療機関における個人情報保護対策の実施状況の調査

全国の医療機関から 2000 件を無作為に抽出し、アンケート調査を実施した。3 月 15 日にアンケートを発送し、締め切りは 3 月 25 日に設定したが 3 月 31 日到着分までを分析対象とした。調査表（回答集計を含む）および回答表を資料として添付する。

C. 研究結果

C-1 出版等

昨年度上梓した「医療の個人情報保護とセキュリティ（有斐閣 2003）」の改定を行った。改定版は現在校正がほぼ終了し、出版準備中で 2005 年 4 月中に出版予定である。また主任研究者が「個人情報保護法対応マニュアル（日経メディカル編、日経 BP 社）」の第 3 章「医療情報システムの安全管

理に関するガイドラインとは何か」を監修した。

C-2 米国 HIPAA Privacy Standards 実施状況の調査

分担研究者の清谷と公文が昨年引き続き米国の HIPAA Privacy Standards の施行状況の調査をおこなった。具体的な問題点はいまでも存在するが、昨年の調査にくらべて医療機関の対応は進んでおり、いわば落ち着いた状況に移行しつつあると言える。詳細は分担研究報告書を参照されたい。

C-3. 医療情報システムの安全管理に関するガイドラインの検討

C-3-1. 個人情報保護法に関する指針等の安全管理義務にあたる部分の要件抽出。

厚労省、経産省のいずれの指針も組織的、人的、技術的、物理的対策を求めており、リスク分析を基礎に体系的な対策をとることを求めている。また、やや具体的なレベルとしてはアクセス制限、アクセス記録の採取と保存を求めている。その一方でアクセス制限やアクセス記録の基礎となる利用者の識別に関しては言及されていない。また平成 17 年 3 月末時点で公表されている Q アンド A では個人情報をコンピュータシステムへ入力する際に、入力やの記録は必ずしも必要でないとするなど、矛盾した対

応も見られる。

C-3-2. これまでに公表されている医療情報システムの安全管理に係る指針の調査

平成6年の医用画像の電子保存の指針は、基準自体がほぼ技術的対策に限定して述べられていることもあって、技術仕様書といっても良いものであった。情報の完全性や可用性に関しては技術のみでも対策は不可能ではないが、機密性や情報主権の勘案など個人情報保護の観点からの安全管理対策は情報の利活用の場面でも保障される必要があり、技術だけでは達成できない。その意味ではこの指針は現時点では著しく不十分といわざるを得ない。

平成11年の電子保存通知の際に作成された指針は技術と運用のバランスで安全管理を達成することを求めており、現実的な指針となっている。また組織的、人的、物理的対策にも言及はされている。しかしながら、技術面ではかなり厳格に中立的立場で書かれており、著しく具体性に欠ける。そのために、技術的対策と相補的に講じられるべき組織的、人的対策も、歯切れの悪い記載になっており、電子保存のように、ある程度技術力のある組織が実施する、いわば特殊な状況での指針としては機能するが、個人情報保護法への対応のように、医

療情報システムを導入しているすべての医療機関が対応しなければならない状況では不適切と考えざるを得ない。

米国のHIPAA Security Standardsも国際的に見れば重要な安全管理基準ではあるが、Privacy Standardsが医療情報全般を対象にして作成された汎用的なものであるのに比べて、Security StandardsはHIPAA法の一部である、オンライン診療報酬請求にかなり限定して定められたもので、また、内容は主にシステムのベンダー向けであり、抽象的である。米国ではHIPAA法の施行前はわが国ほどレセコン等の情報機器の導入は進んではなく、HIPAA法のオンライン診療報酬請求の義務化に対して導入を行う医療機関が多いために、このような基準で機能するのであろうが、わが国のようにすでに70%以上の医療機関に医療情報システムが導入している状況では、やはり具体性に欠けるといわざるを得ない。

なお、平成14年にわが国では外部保存に関する通知が出され、基準と指針が作成されているが、安全管理に関しては、平成11年の指針と大きく異なる点はないために、ここでは割愛する。

C-3-3. 個人情報保護法に対応する情報システムの安全管理指針の作成

C-3-2の結果から、平成11年の電子保存に関する指針から電子保存を行うか否かにかかわらず安全管理上必要な項目を抽出し、C-3-1の2つの指針の要件と和をとり、指針を作成した。概要をいかに示す。

1. 方針の制定と公表

電子保存の指針では透明性の確保は触れられていなかったが、個人情報保護の指針で、特に厚労省指針では透明性の確保は重視されており、追加した。

2. 情報の取り扱いの把握とリスク分析

リスク分析は安全管理上もっとも重要な初期ステップであるが、医療機関はスタッフの信頼関係を基礎に医療業務を行っている関係からか、リスク分析が不得意な傾向にある。したがってリスクを例示し、取り組み易さを目指した。以下の亜項目にわけて示している。

2. 1 取り扱い情報の把握

2. 2 リスク分析

3. 組織的安全管理対策（体制、運用管理規程）

体制は適応する組織の形態に大きく依存するし、運用管理規程も物理的な対策や技術的対策と相補的であり、具体的な記述が困難な部分であった。運用管理規程は物理的対策や技術的対策に応じて具体化される

べきもので、対応表形式で整備することが望まれる。

4. 物理的安全対策

情報システムの物理的安全対策は建物の立地条件から考慮されるべきであるが、すでに大多数の医療機関に導入されている医療情報システムの安全管理を扱う指針であることから、管理区分の設定と施錠、入退管理のみを記載した。

5. 技術的安全対策

平成11年の電子保存に関する指針が技術的中立性を基本としたために全体として理解しがたいものであったことを踏まえ、具体的な技術要素にできるだけ触れることとした。利用者の識別及び認証、情報の区分管理とアクセス権限の管理、アクセスの記録（アクセスログ）、不正ソフトウェア対策の4項に分けて指針を示した。もっとも重要な利用者の識別および認証においては、パスワード認証、生体計測認証、ICカード等の所持情報のそれぞれ技術的な特徴と採用する際の運用上の留意点を示した。また技術要素は現時点でのコストも勘案して記載したために、精度は高いものの高額のために、一般的な医療機関では採用が困難なものは除いて指針を示している。

6. 人的安全対策

医療機関の職員に対する対策と、第三者、特に情報システムの保守等の委託契約に対して言及している。

7. 情報の破棄

個人情報保護法が存在しなくても医療従事者の守秘義務の観点から重要な項目であるが、これまで存在する医療分野の指針では積極的に触れられていなかった項目である。内容は単純であるが、指針として明記した。

8. 情報システムの改造と保守

医療情報システムにとっては重要な項目であり、6の人的安全対策の委託契約と一部重複するが、しばしば実施される点数改定や制度の変更による情報システムの改造は、いわば日常茶飯事であり、それだけに指針として明示する必要がある。あくまでも医療機関が責務を全うするという観点から監督責任に重点をおいた指針とした。

9. 外部と個人情報を含む医療情報を交換する場合の安全管理

オンラインメンテナンスやネットワークを利用した医療連携が相当する。現時点でそれほど普及しているわけではないが、維持コストや連携密度を上げる観点から今後急速に普及すると思われるために、特に指針を示した。ただし、ASP型のレセコ

ンや電子カルテに代表されるオンラインの外部保存に関しては、単なる安全管理だけではなく、情報の二次利用の制限や責任分担などさまざまな問題があるために、安全管理の指針としては対象外としている。

なお、本指針案の作成は厚生労働省医療情報ネットワーク基盤検討会合同作業班の班員の多大な貢献があった。

C-4. 医療機関における個人情報保護対策の実施状況の調査

アンケート送付数は2000件であったが、あて先不明等で送付できなかったものが84件あり、送付対象は1916件で、うち、回答が返送されたものは450件(回答率23.5%)であった。

対象の規模は病床数19床以下の診療所が54.6%、病院が45.6%であった。また特定機能病院が3施設、地域医療支援病院が7施設含まれていたが、98%は一般病院または診療所であった。

個人情報保護法は医療機関の開設者によって適用される法律が異なるために、開設者の種別を聞いたが、独立行政法人が1.2%、地方公共団体が6.3%で、他は民間立であった。

個人情報保護法への対応に関する回答を図1に示す。少なくとも対応を始めている

施設が 32.5%に過ぎない。また内容をまったく知らない施設が 10%以上ある。

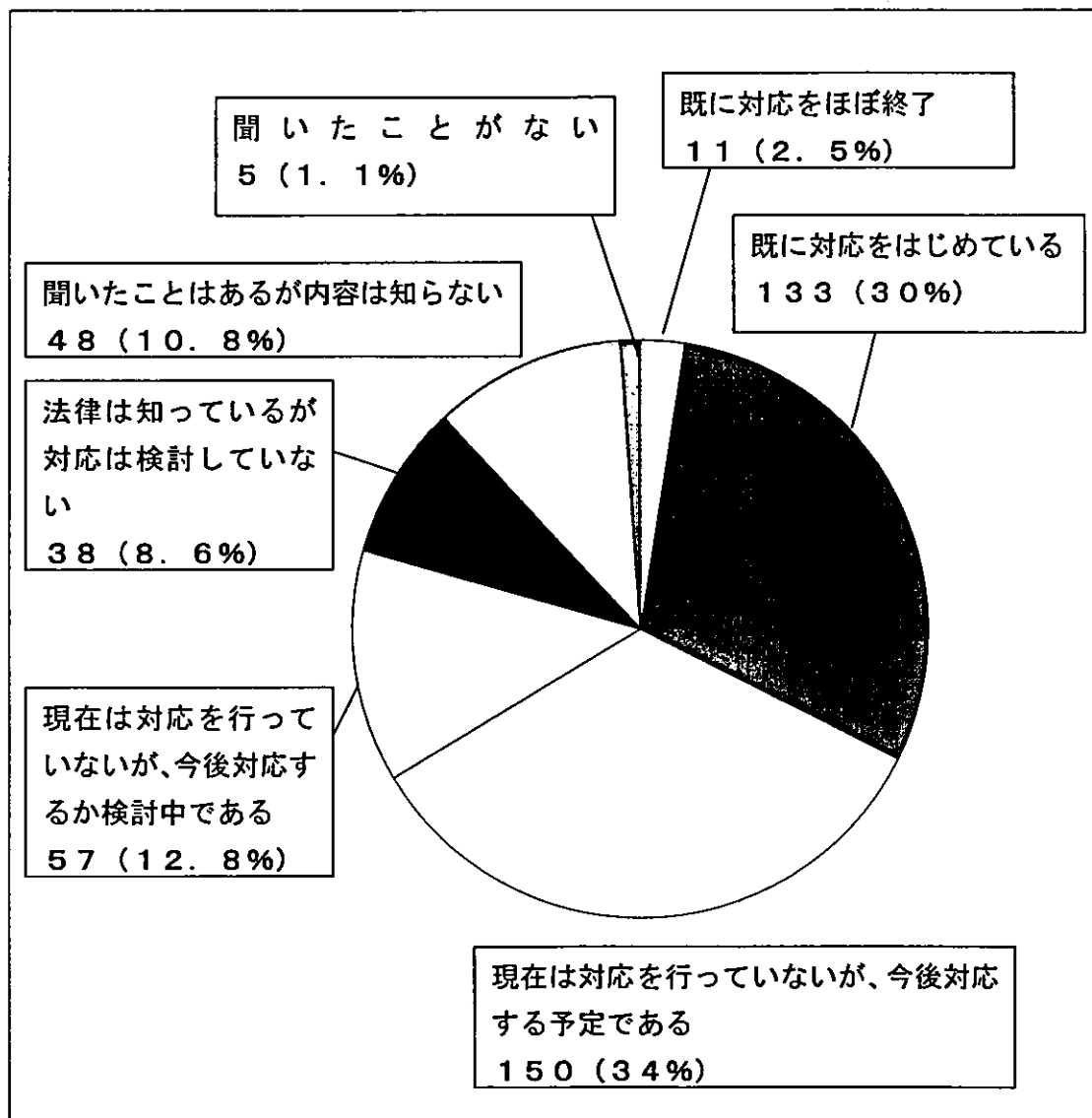


図1 個人情報保護法への対応について

また厚生労働省の「医療・介護関係事業者における個人情報保護の適切な取り扱いのためのガイドライン」の活用状況についての回答を図2に示す。ガイドラインを参

考にした、またはするつもり施設が72.3%でガイドラインを知らない施設が20.5%あった。

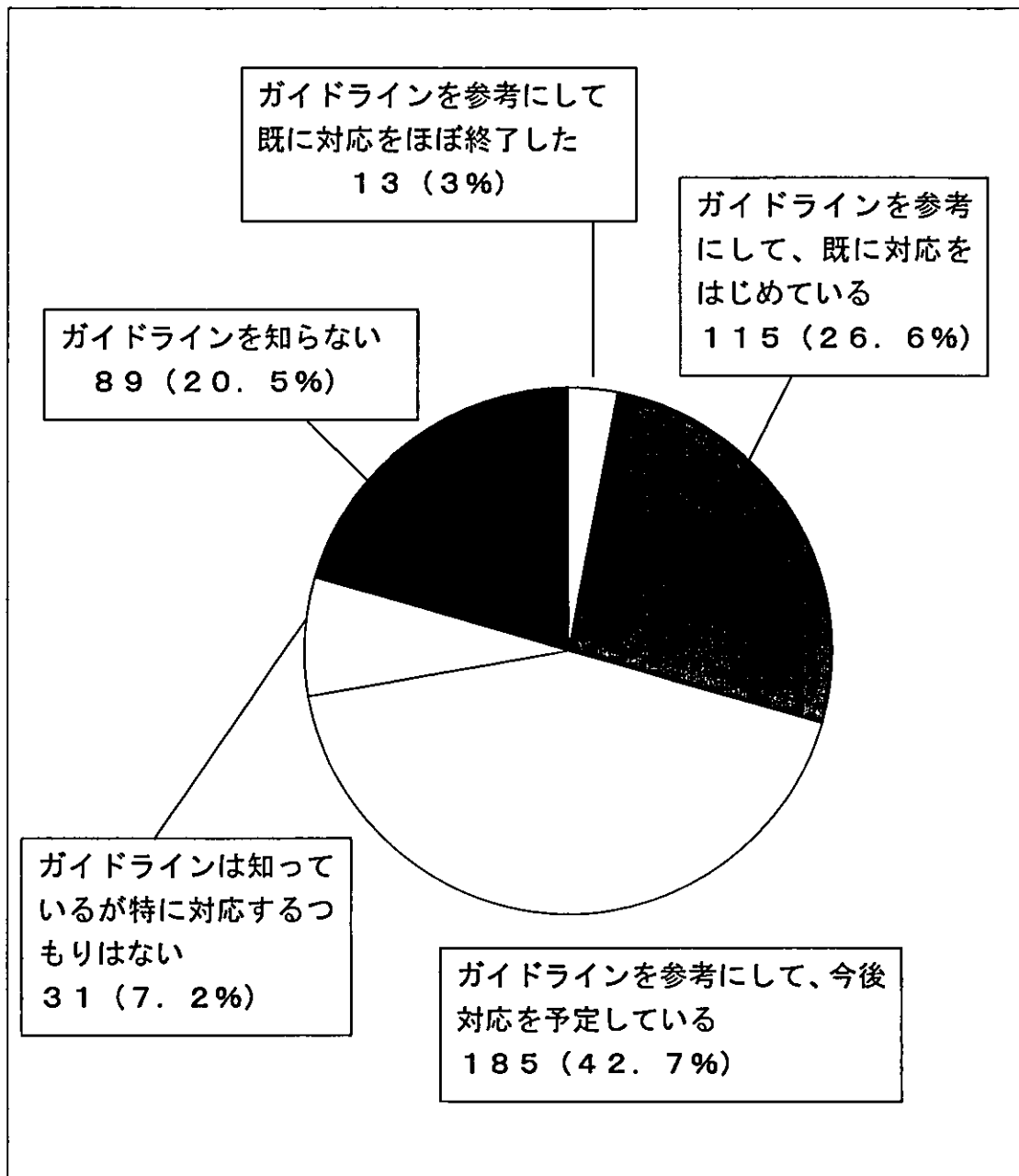


図2 「医療・介護関係事業者における個人情報保護の適切な取り扱いのためのガイドライン」について

対策の個別の項目についてはプライバシーポリシーの作成についての回答を図3に、利用目的の通知等に用いる院内掲示物に関

しては図4に、患者向けの配布物に関しては図5に、個人情報保護に関する院内規定については図6に示す。どの問いにも未作

成が約半数あった。対策をおこなっている施設では医師会等の団体が作成した雛形を
活用している施設が多い。雛形を当該医療機関向けに手を加えている施設はその中の
約半数であった。

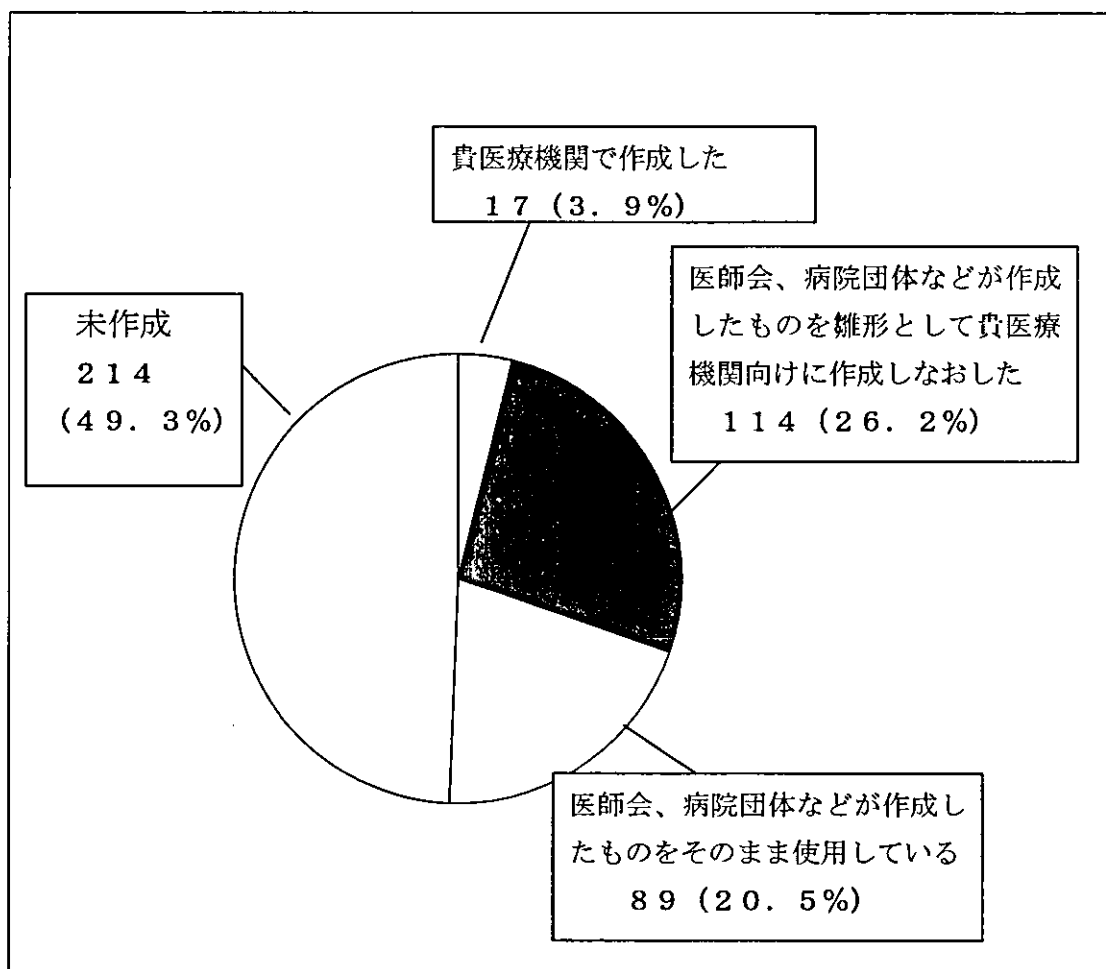


図3 プライバシーポリシーの作成状況について

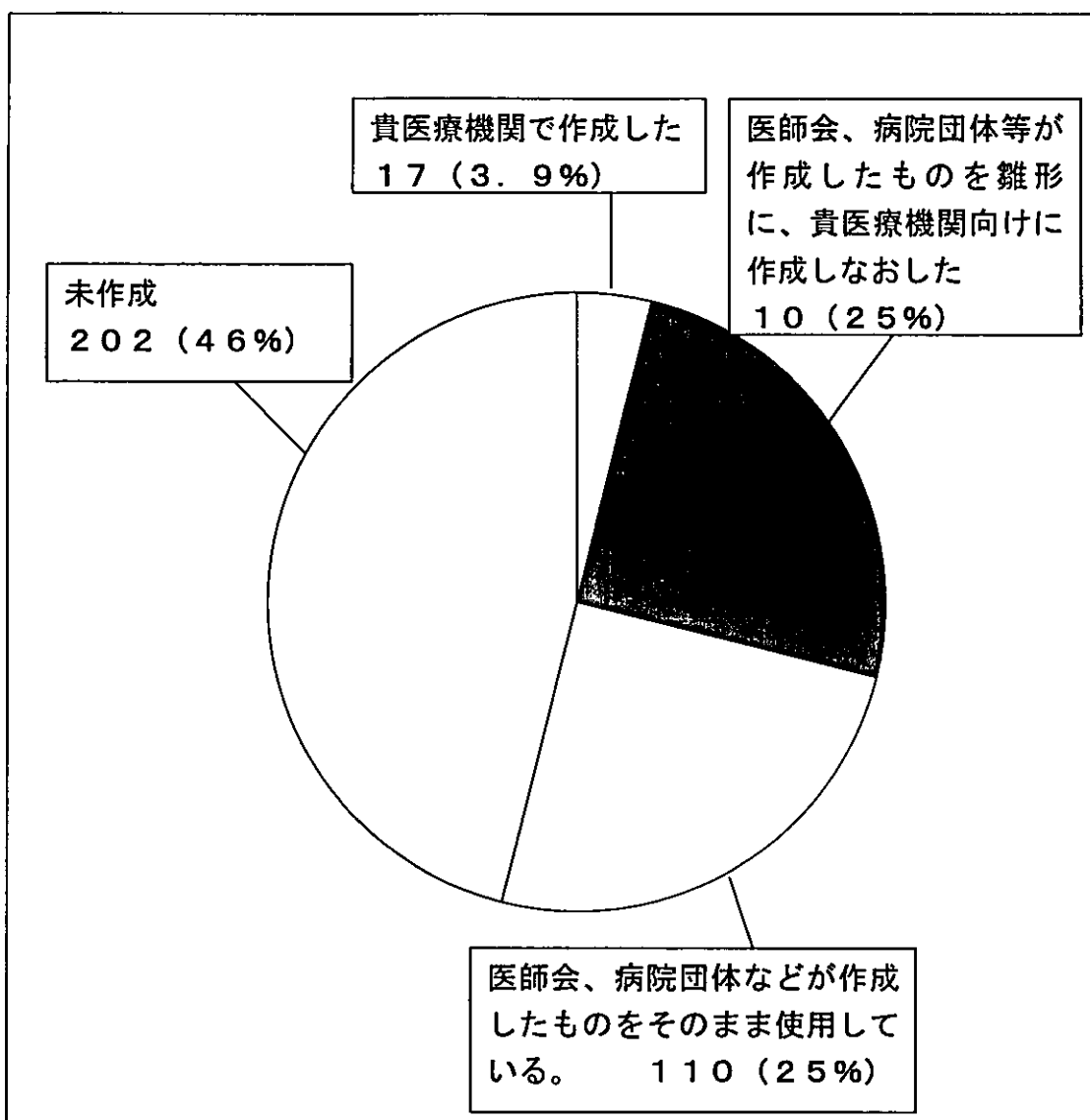


図4 個人情報の取り扱いに関する掲示物について

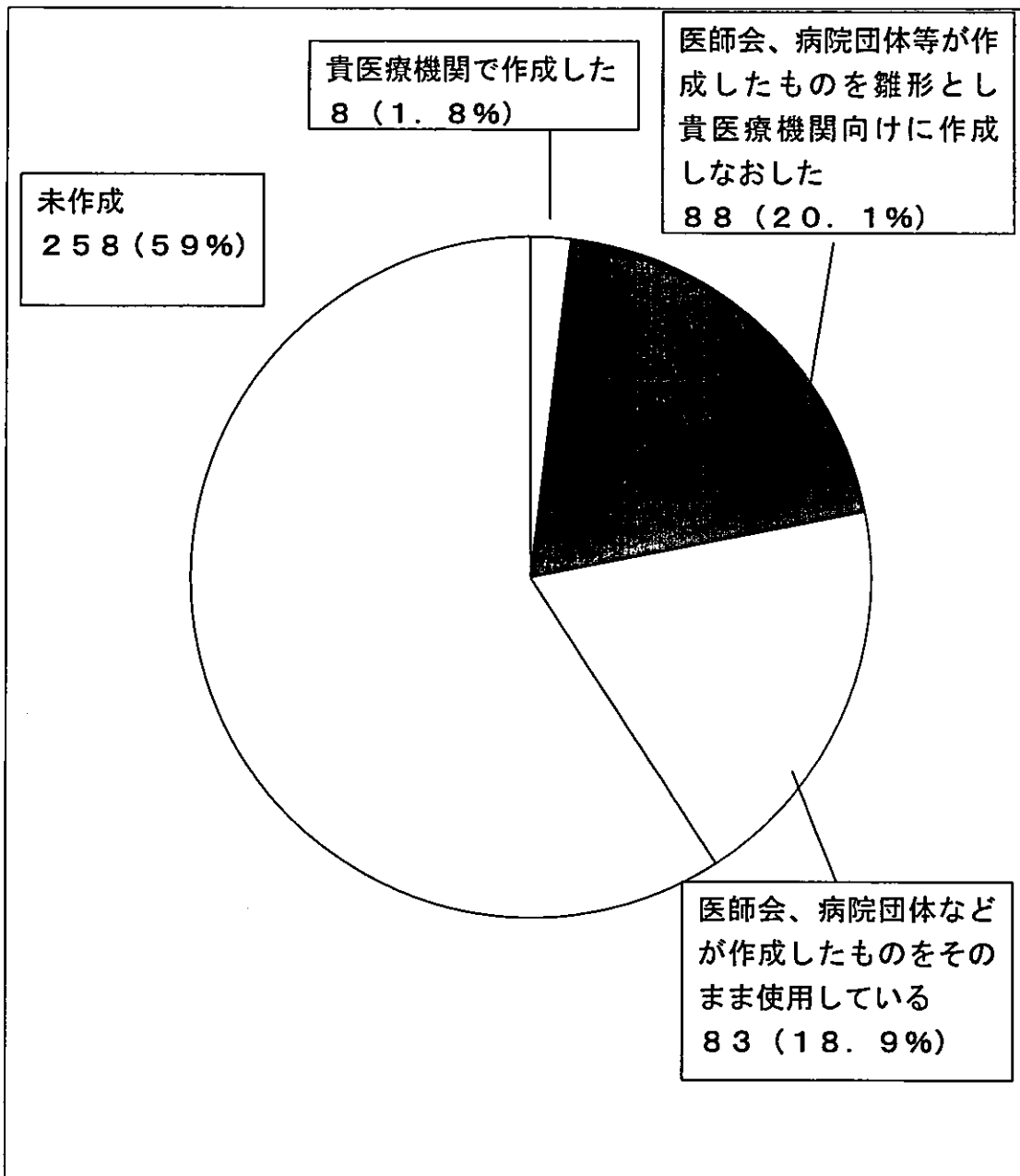


図5 患者むけの配布物（パンフレットや発行物）

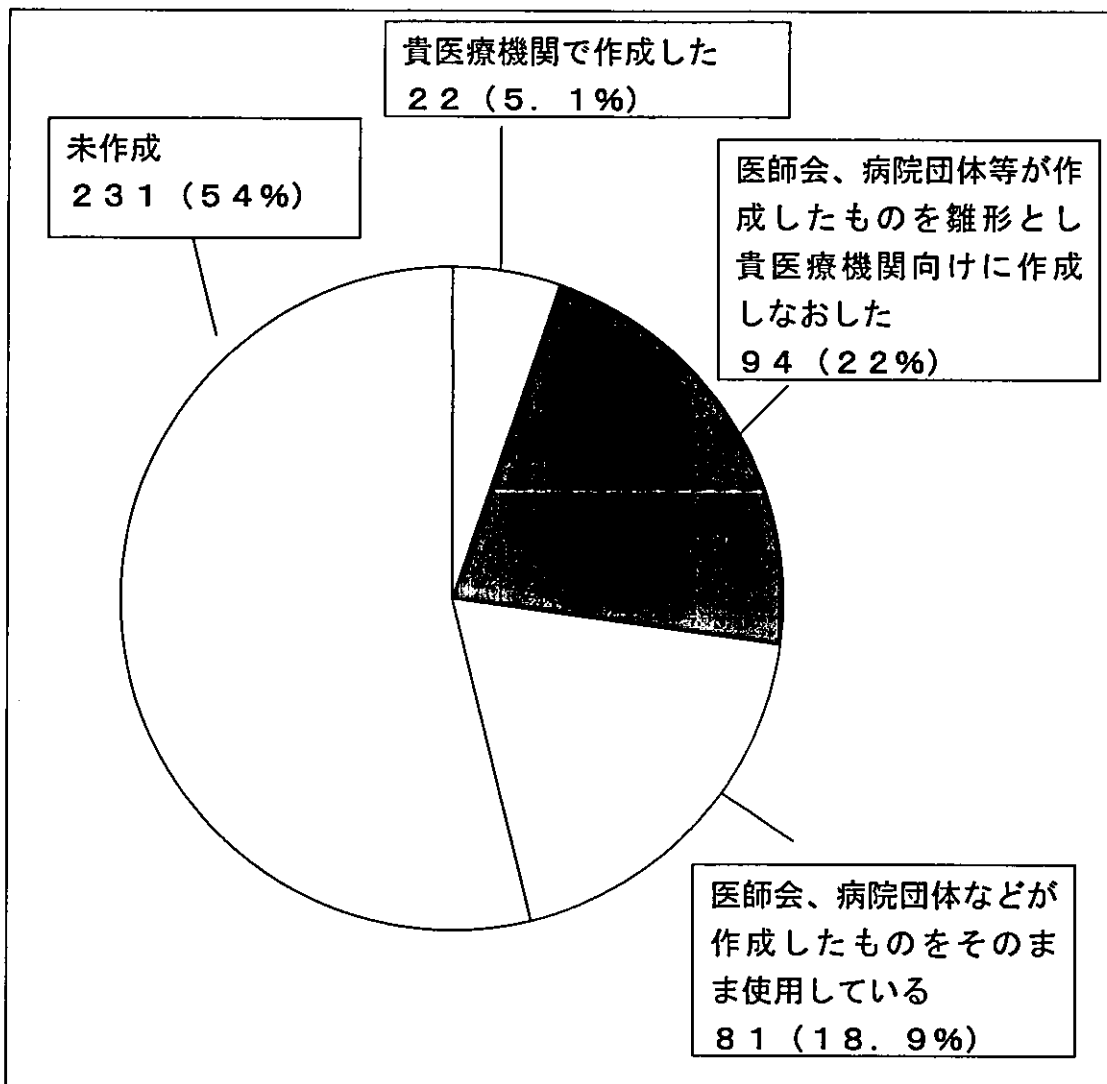


図6 院内の個人情報に関する各種の規定やマニュアルについて

また診療録の保有状況について聞いたが、大部分の施設で5年以上保持しており、5年以内の診療録数に比べて5年以上経過した診療録のほうが多い傾向にある。

外部委託に関する質問では、個人情報の取り扱い状況を確認して業者を選択している施設が14.7%と低く、また守秘契約を

している施設も31%に過ぎない。定期的に個人情報保護に関する報告を契約で定めている施設は2.2%に過ぎない。

患者の家族等への情報提供に関する回答を図7に示す。やく半数の施設がすでに提供をおこなっていい親族を患者に確認している。

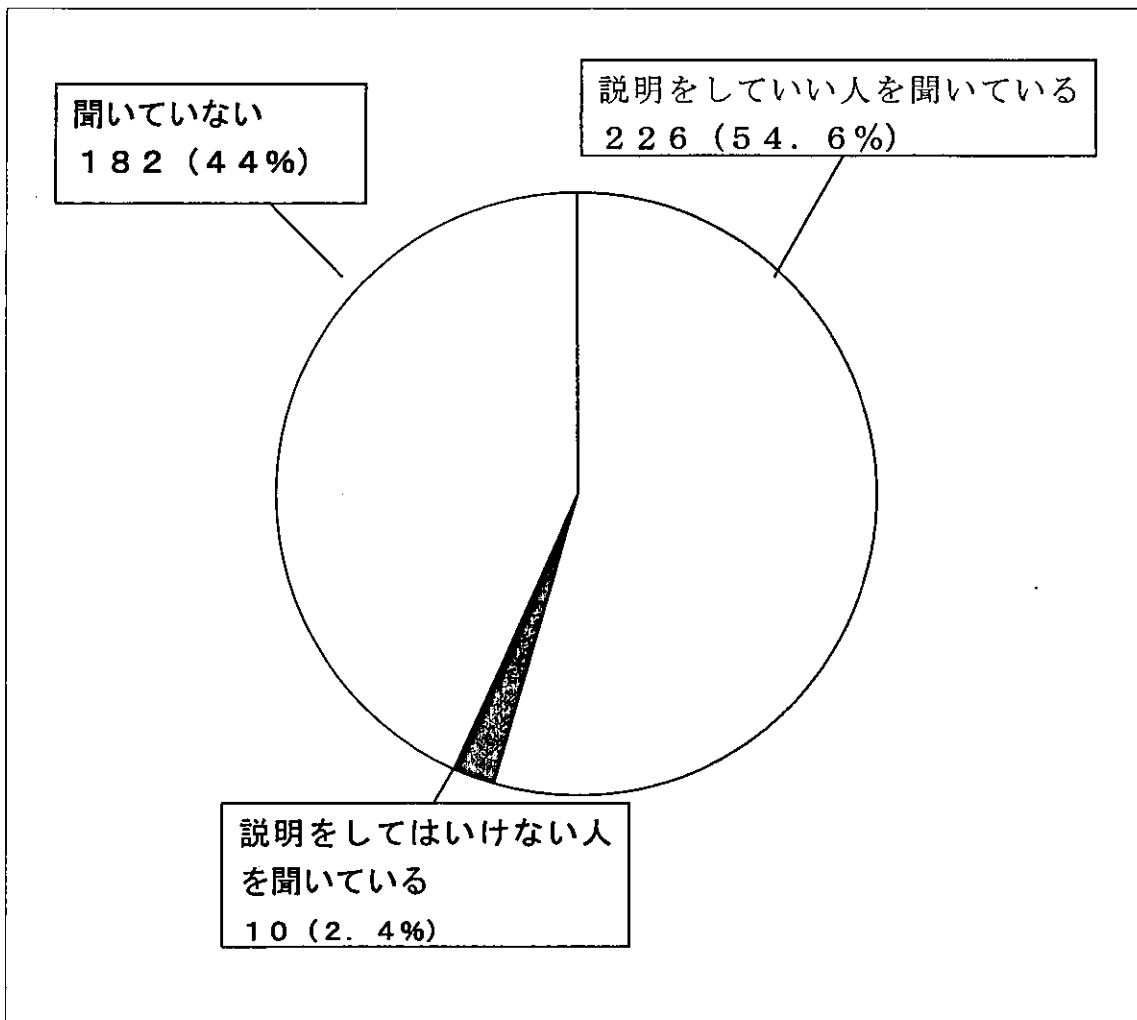


図7 病状説明を行う患者親族等についての患者への確認

プライバシーマーク認定制度についての回答を図8に示す。知らない施設が55.5%を占め認知率は低い、取得を目指してい

る、または希望している施設が21.3%を占めていた。

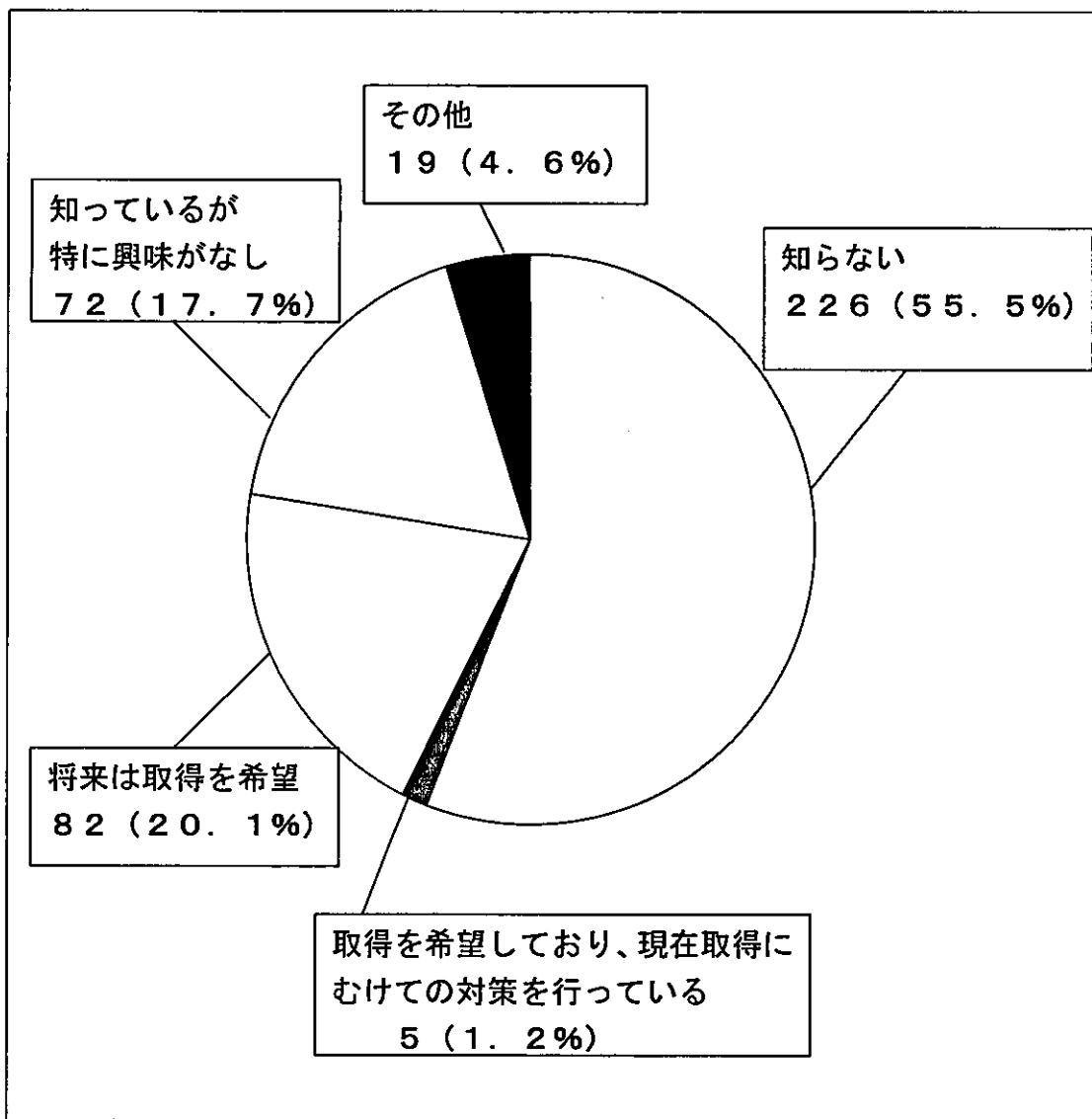


図8 プライバシーマーク認定制度について

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厚生労働省の指針等にしがたって、対策をとる必要がある。米国のHIPAA Privacy Standardsの施行状

況の調査では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らかになっていった。しかし米国では規則自体がかなり厳しいものであり、また医療に特化した規則で医療機関にとっても理解しやすいものであったためか、医療機関での対応は進み、今研究年度の調査では話題性

が低下しており、落ち着きを見せていた。わが国も1年程度で順調に対応が進むことが望まれる。

HIPAA Privacy Standardsは何度も述べているように医療に特化した Privacy に関する規則であり、日本では言えば省令に相当する。罰則も厳しい。日本ではこれに相当する強制力のある規則は存在しない。

平成17年3月に施行したアンケート調査では個人情報保護法への対応をまったくはじめていない医療機関が60%を超えていることは、法律の全面実施まで2週間という調査時期を考えれば深刻な事態と考えざるを得ない。

国家資格を持つ医療従事者には従来より罰則を伴う守秘義務が定められており、個人情報保護法制定以前から医療機関では患者のプライバシーは尊重されてきたので、法律への対応が不十分であることが、直接患者のプライバシーの侵害につながるものではないが、医療情報はきわめてプライバシーに機微な情報であり、また、保護と活用の高度なバランスを求められる。言い換えれば保健医療福祉分野はプライバシーに関する事象ではもっとも扱いの難しい分野といえる。それだけに個人情報保護法の全面実施を機会に対応の見直しや医療従事者

間を含めて社会的なコンセンサスを形成する必要があると考えられる。そのような視点に立てば法への対応に未着手の施設が60%を超えていることは重要視せざるを得ない。

この関心の低さにはさまざまな原因が考えられる。

そのもっとも大きな点は個人情報保護法自体にあると考えられる。法律は民間事業者、行政機関、独立行政法人、地方自治体と対象機関を設置母体でわけて規制しているが、対象となる分野は限定していない。したがって医療も商店の顧客管理も同様の法律が適用されることになる。そのために法律は抽象的で具体的対策につながりにくい。また商店の顧客管理情報と医療情報では一般的に人権としてのプライバシーに与える影響の大きさはまったく異なる。さらに顧客管理情報を第三者に提供することは通常の利用形態とはいえない場合が多いが、現在の医療は医療機関連携を基礎としており第三者への提供は日常的な行為である。このようにまったく扱い方の異なる情報を一つの法律で規制することは相当な困難があるのは当然で、それゆえに法律が難解なものにならざるを得ないのであろう。もっともこのような問題点は法の成立当時

から指摘されており、国会でも両院ともに付帯決議で医療を含む重要3分野では個別法の検討が求められている。しかし現実には個別法は制定されなかった。

それに代えて2004年4月の施行令では関係省府が指針を作成して法を実施することを求め、医療の分野でもいくつかの指針が作成された。もっとも重要なものが2004年12月に公表された「医療・介護関係事業者における個人情報の適切な取り扱いのガイドライン」であろう。このガイドラインは法律のわかりにくさを可能な限り平易に開設だけでなく、家族への情報提供や連携医療といった医療では日常的な第三者提供に特別な配慮をおこなうなど、かなり実質的な指針となっている。

ところが本研究で実施したアンケートでは20.5%にのぼる医療機関がこの指針の存在自体を知らなかった。一般企業における経済産業省の指針の活用比べて低いとはいえないが、前にも述べたように、医療情報が極めてプライバシーに機微であること、第三者提供を含む活用がスムーズに行えてこそ医療の水準を保つことができる場合が多いことを考えれば重要視せざるを得ない。

ポリシーの制定や利用目的等の掲示物の

準備状況も決して十分ではないが、その中で日本医師会等の関係団体が作成した雛形の利用が進んでいることがアンケートでは明らかになっている。個人情報保護法上の認定保護団体の認定はまだされていないものの、このような関係団体が積極的に取り組んでいることは意義深く、今後の対応の充実にも期待できる。ただ現状では医療機関は関係団体の作成した雛形をそのまま用いる傾向があり、本当にそのままで施設の運用形態に適合しているのであれば問題はないが、安易にそのまま用いている場合は現実と齟齬を来す可能性もある。注意喚起が必要であろう。

厚生労働省の指針の認知度に低さには、それが指針であるため、という面も考えられる。米国には包括的な個人情報保護法はなく、HIPAA Privacy Standardsはわが国の厚生労働省指針と同種の内容で、相違は規則として定められ罰則が適応される点にある。省令のような規則と指針では当然ながら関心をひく程度は異なる。指針はいわば解説書のようなとらえかたをされている可能性もある。さらに都道府県等のルートで周知は図られているはずではあるが、その重要性を考えると、周知不十分である可能性も否定はできない。例えば厚生労働省

の WEB ページでこの指針はダウンロードできるが、実際にダウンロードするためにはかなり努力して探さなければならない。

本研究では情報システムとしての個人情報保護のあり方も重要な研究目的であるが、本年度は医療情報システムの安全管理指針を検討した。

個人情報保護法に対応した安全管理は電子カルテのような高度な診療情報システムだけを対象にするわけにはいかない。各施設で用いているオーダリングシステム、医事システムなど、患者個人情報を扱うすべてのシステムを対象とする必要がある。

これまでも医療情報システムの安全管理指針はまったくなかったわけではなく、平成6年の医用画像の電子保存容認通知に伴う基準と指針、平成11年の診療録等の電子保存容認通知に伴う指針が存在した。しかしこれはいずれも、保存義務のある文書を電子媒体での保存で法的な責務を果たすという、いわば特殊な作業を行う場合の指針であり、個人情報保護の観点に立てば、個人情報を扱うすべての情報システムが対象になるのは当然で、その意味でこれらの指針は範囲が異なる。特に前者は技術的対策のみで安全管理を実現しようとしたもので、医用画像を電子媒体に保存するだ

けといった、きわめて限られたユースケースでは成立するが、診療情報の利活用における個人情報保護といった、システムを離れた部分にも十分な考慮が必要な範囲では対応できない。後者の診療録等の電子保存に関する指針では、技術的対策と運用的対策の組み合わせで安全管理を実現することを求めており、また基準にも留意事項ではあるが、プライバシー保護が取り上げられていて、その意味では本研究で作成を目指す指針の土台として検討に値する。しかし、電子媒体への保存のみを想定した指針であり、また技術的中立を強く打ち出しているために、必然的に技術要素に具体性がなく、そのために技術的対策に呼応して講じられるべき運用的対策も限定することが非常に難しい。電子保存という、いわば特殊な作業をあえて行う医療機関であれば、それなりに情報技術の素養が求められ、そのようなスキルを前提にすればこのような指針でもよいが、本研究で作成する指針はすべての医療情報システムが対象で、小さな診療書のレセコンまで含まれる。そのため、特別なスキルがなくても可能な限り容易に具体的対策が立てられることが必要で、その意味では技術的中立は不適であろう。

したがってこの平成11年の指針をベー

スにしながらも、個人情報保護法に関連する厚労省指針や経産省指針の要件を満たし、利用可能な技術的対策をできるだけ具体的に取り入れ、それぞれに応じた運用的対策を明確にし、指針を作成した。結果的に、具体的で、電子保存に関する指針よりは容易に理解できるものにはなった。

しかし問題もある。一つは技術的対策を網羅することの困難さで、情報セキュリティの分野での技術開発は日進月歩で、網羅することは難しい。また、コストも問題で、大雑把に言って技術的対策にコストをかければかけるほど、運用的対策は利用者に負担の少ないものとなる。その典型例が利用者認証における生体計測認証であろう。この分野の技術的進歩はめざましく、高精度の識別が可能な装置もすでに存在する。しかしかなり高価であり、特別な部屋の入退室管理程度なら大規模な医療機関であれば利用できるかも知れないが、個々の病院情報システムのクライアントで導入することは不可能である。したがって純粋に技術的な観点からは生体計測認証だけで、利用者を識別することは可能であるが、現実的には、すなわち実現可能な程度のコストでは他の方法と組み合わせることが必要になる。

また、技術の進歩が早いことは、具体的

な技術的対策を積極的に取り入れたこの指針が陳腐化するのも早いことを意味している。技術的に中立に記載すれば、いわばセキュリティの基本方針が変わらない限り有効な指針となるが、現実の技術的対策を具体的に記述すれば、技術の進歩に応じて改定する必要がある。技術開発の速度を予測することは難しいが、1～2年のスパンで見直しは必須と考えられる。

なお、本研究で作成した安全管理指針は、17年3月31日に厚生労働省から公表された「医療情報システムの安全管理に関するガイドライン」に反映されている。この指針は個人情報保護法の要請だけに対応するものではなく、いわゆる電子署名法、やe-文書法に対応するための指針で、電子保存や外部保存の指針のリライトも含まれており、大部なものとなっている。

E. 結論

前研究班の成果とあわせ刊行した個人情報保護とセキュリティに関する書籍を改定した。また昨年が続いて米国 HIPAA 法 Privacy Standards の実施状況と医療機関の対応状況を調査し、次第に定着していることを明らかにした。さらに誇示情報保護法全面実施直前のわが国の医療機関の状況