

により、臨床研究に遅れが生じたこともあった。患者の家族や知人が患者の介護をするにあたり、情報の入手に制限を受けたこともあった。特定の要件を満たす場合には、患者の書面による同意がなくても情報の開示が可能であるが、医療機関によっては実施されていない。

医療機関や患者団体の調べでは、多くの国民が Privacy 規則について十分理解していないとされる。患者は自分の情報保護に関する権利について理解していないか、説明を受けても関心が乏しいケースが多々ある。

Privacy 規則施行後 1 年間に OCR が受取った苦情のうち 2700 件の内容を確認したところ、約 2/3 は、規則によって禁止されているわけではない行為に関する苦情であったり、規則の対象とならない機関に対する苦情であったり、施行前の行為に対する苦情であったりした。さらに残りの半分近くが、規則違反とはいえないと判断された。

この結果、会計監査院から、保健省長官に対して、HIPAA 法 Privacy 規則を「法令によって定められた場合には患者の個人情報公衆衛生担当部署に報告されることを『個人情報保護のお知らせ』に記載すること、及び、そのような公衆衛生上の医療情報は、情報公開ンにかかる責任から免除される」ように修

正することが推奨されている。

また、本 Privacy 規則で規定されている患者の権利に関して患者の認知度と理解を向上させるため、保健省に広報を行うことが推奨されている。

## 2) 会計監査院の評価に対する保健省の対応

このような会計監査院からの評価に対する保健省の対応は次の通り。

① Privacy 規則開始後 1 年間の施行状況が比較的円滑であったことは、保健省の調査によっても同様の意見がでており同意すること。

② 公衆衛生上の医療情報の取扱いを情報公開の責任から免除することについては、過去においても議論され、今後その必要性を引き続き検討していくこと。

③ 患者の権利に関するお知らせは長すぎることもあり、十分読まれていない場合があると考え、新たなリーフレット 2 種類を保健省のホームページに掲載するとともに、フリーダイヤルによる相談係を設置し、医療機関等に対して、患者の権利に関するお知らせを、より平易に書き、重要部分に印をつける等奨励することとした。

このような保健省による努力と大衆へ

の啓発を通じて、本規則のもとに設置された情報の保護を効率的に施行することが可能と考えられる。

### 3) 情報開示に伴う医療機関等の責任について

#### ① 開示後の情報追跡が困難なこと

情報開示後の経路を追跡する責任があるが、そのために相当の時間と資源が必要である。

たとえば、医療機関においては、電子化する必要のない患者の情報を院内の様々な部署において管理しているが、この情報の追跡をするために、システムを再構築したり、電子的なリンクを設置したり、手作業による経路追跡の手法を設置した。同様に保険者においては、患者の情報が、被保険者の加入、医療費請求、顧客サービス等の事項ごとに異なる部門やシステムにおいて管理されていることから、これらを統一して情報管理することが大変困難とされている。

#### ② 追跡が必要な開示情報が大量であること

法令で求められている情報開示、たとえば、疾病登録、人口動態情報、その他の保健医療データベースへの登録が頻繁で、様々な形で必要なため、その追跡作業が大量に発生し、大変な負担となっていることが指摘されている。

#### ③ 情報追跡が本当に患者のためになるのかどうか疑義があること

患者の情報開示後の追跡には大変な負担が伴うが、患者から医療情報開示の状況に関する確認の要望がほとんどだされていないため、本当に患者にとって有益な作業であるかどうかについて、医療機関等から疑義が生じている。

このため、医療機関等からは、法によって求められた場合には、公衆衛生関連機関や法を所管する団体に対し、患者の医療情報を提供することを、患者に対するお知らせ等においてあらかじめ断っておくよう Privacy 規則を修正するよう求める声が強い。この修正が実現すれば、法の定めるところによる情報の開示に関しては情報の追跡が不要となる。

#### 4) 委託業者との契約について

医療機関も保険者とともに、委託業者との契約に多大な資源を要したと報告されている。

この委託業者との契約が困難な理由として、どのような組織との間で委託契約が必要となるかについて混乱が生じたこと、また OCR による適切なガイドラインがないこと等があげられている。

Privacy 規則は、現行の契約に適応させて、規則にもとづく委託契約を段階的に実施することを規定しているが、この

ための対策が大変な負担と指摘されている。

医療機関等は、患者の個人情報の移動を伴う委託に関する数千に及ぶ契約の見直しが必要であり、特に、多種多様な委託先との契約内容について、法的側面を含めて個別に交渉、対応するために、多大な時間と経費を要したことを指摘している。

一方、医療施設認定合同審査会(JCAHO; Joint Commission on Accreditation of Healthcare Organizations)では、医療施設認定の申請書に追補版として委託契約の標準を加えることにより、このような負担や課題を削減させた実績もある。このような影響力をもたない医療機関は委託先と個別に交渉せざるを得ない。

多くの医療機関や保険者団体から、委託契約に関するより適切なガイドラインがOCRから発行されることが望まれており、現行のガイドラインは実用性がなればかりかより疑義を生じかねない内容となっていると指摘している。

## 5) その他の問題

会計監査院による報告書では、その他に次のような問題点が指摘されている。

①公衆衛生関連機関、研究者、患者の擁護人によるデータへのアクセスが制

限を受けてきている

②州政府及び連邦政府機関による公衆衛生業務を目的としたデータ収集に困難を生じていること

③研究グループによる保健医療データへのアクセスが遅延または困難となっていること

④患者の擁護人が、患者の代理として情報を収集するのに支障が生じていること

⑤患者は、患者の権利について熟知しておらず、Privacy 規則について誤解している可能性があること

⑥保健省 OCR に提出された苦情の多くが Privacy 規則に関する誤解に基づくものであること

## 2. 医療情報管理システム協会(HIMSS; Healthcare Information and Management Systems Society)による保健医療事業者のHIPAA 法準拠に関する調査

### 1)概要

医療情報管理システム協会(HIMSS)が、HIPAA 法 Privacy 規則が 2003 年 4 月に施行された 2 年後の 2005 年 1 月に、医療機関と保険者を対象に実施した調査(回答数;医療機関 320、保険者 80)によると、医療機関の 78%、保険者の 90%が HIPAA 法 Privacy 規則に準拠しており、その状況は

2004年6月の状況と大きな変化がないとされている。

また Privacy 規則準拠とされているなかにおいても、委託契約が規則準拠となっているか、また院内の個人情報の取扱いが規則準拠となっているか等において、温度差があることが分かっている。

過去6ヶ月間のうちに、医療機関の73%、保険者の56%が個人情報の取扱いに違反があったと回答している。

また、Privacy 規則施行後、医療機関の27%、保険者の31%が、連邦政府レベルまたは院内レベルで公式の苦情が申告されたと回答している。

## 2) 医療機関における規則準拠の状況

医療機関の規模別に Privacy 規則準拠の状況を見た場合、中規模の医療機関がもっとも高く95%、小規模の医療機関がもっとも低く67%であった。

また、HIPAA 法 Privacy 規則で準拠が困難であったのは、①院内における情報開示の責任体制の整備、②診察室等臨床現場で患者のプライバシーを確保することとの回答であった。

## 3) 保険者における規則準拠の状況

保険者の規模別に Privacy 規則準拠の状況を見た場合、被保険者数が50-150万人の保険者でもっとも高く100%であった。

また、HIPAA 法 Privacy 規則で準拠が困難であったのは、①第3者からの患者の個人情報の開示要求があったときの情報を必要最小限にあらためる手法、②委託業者との契約締結、③社内における情報開示の責任体制の整備 との回答であった。

## 4) Privacy 規則の分野ごとの規則準拠の状況

医療機関及び保険者の双方において、Privacy 規則準拠であっても、その分野ごとに準拠の度合いが異なり、その状況は下表のとおりである。

Privacy 規則の分野ごとの準拠の状況

Privacy 規則の分野	医療機関	保険者
患者の個人情報の利用と開示に必要な同意の取得	100%	100%
法令で保証された患者の権利の実現	100%	96%
Privacy 規則に関する掲示と配布	97%	98%
職員に対する Privacy 研修の実施	97%	96%
Privacy 規則の通知の受取、承知の取得	96%	n/a
院内における情報開示の責任体制整備	96%	98%
法令違反の内部報告に関する研修	96%	n/a
「必要最小限」の利用	89%	n/a
Privacy 規則準拠の組織的監視	88%	96%
Privacy 規則準拠の委託契約締結	88%	94%

## 5) 外部のコンサルタントの活用の状況

HIPAA 準拠のために外部コンサルタントを活用している医療機関や保険者は減少傾向にある。

2004年1月の調査で49%、2004年6月の調査で42%、今回2005年1月の調査で37%であり、多くはセキュリティ対策に関するコンサルタントであった。

医療機関と保険者別に外部コンサルタントの活用状況を見ると、医療機関34%に対し、保険者の46%が外部コンサルタントを活用していた。

またコンサルタントを活用している機関の内容を見たところ、55%がセキュリティの評価及び実施要領について、38%がセキュリティの啓蒙および教育について、33%がセキュリティの第三者評価や監査に活用していた。

#### 6) HIPAA 対応のための医療機関の予算

病床規模ごとに見た医療機関のHIPAA法(プライバシー、セキュリティ等を含む)対策のための平均的な予算は、100床以下の医療機関で年間50千ドル(約500万円)以下、100-400床の医療機関で年間250千ドル(約2500万円)程度、400床以上の大規模医療機関においては1百万ドル(約1億円)台で増加傾向にあった。

### 3. フロリダ州タンパにおける医療プライバシー

に関する弁護士からの聴取につい

ては以下のとおりであった。

・各病院におけるHIPAA法Privacyルールへの対応状況についてはどうか

→おおむね守られていると考えられるのではないか。

・HIPAA法Privacyルールへのコンプライアンスが極めて困難な医療機関がある場合、どのような背景に基づくと考えられるか(院長の意識の低さ、地域的な問題、医療制度上の問題、医療保険の問題、等???)

→多くの職種の多くの職員がいて、それらに対する研修が大変であることが一番問題だろう。HIPAA法遵守のための資金は政府から出るわけではなくすべて医療機関が自前で用意しなければならないことも重要である。やはり、コスト面での問題は多い。また、医療機関内のシステムが、マネージドケア、入院用、外来用等々すべて異なる上に、そのほとんどのシステムが患者情報へのアクセスをもっているためにHIPAA法の適用となるが、すべてにHIPAA準拠をさせるのは作業量や経済的負担が大きい。多くの医療機関が情報化に取り組んでいるが、プライバシーとセキュリティの確保が困難であること、医療機関職員が不慣れであることなどから、対応が追いつきにくい。

・医療機関におけるHIPAA法対応のため

の具体的な負担はどのような状況か？

→経済的負担については、最低でも、USD160/hr \* 10hr/day \* 5 day/wk \* 6wk が必要だろう。問題点の整理や研修に必要となる。Compliance Officer や Privacy Officer の雇用が必要。HIPAA 法対応のために全米で 400 億ドル(=4 兆円)必要と試算されている。プライバシー規則では、建物やインフラ整備、機器の整備は求められていないが、スタッフ(人事)面に関しての要求事項がある。このため、新たに雇う必要がある場合があり、一人当たり 4-5 万ドル/年の人件費が増加する。

○CPO(プライバシー責任者)の雇用について

・HIPAA 施行時は、プライバシー担当官を探すことが難しかった。内部の人材では教育等が困難であるので外部の人材を求めたが、安価でよい人材が得にくかった。結局、内部の人間を教育する方が多くなった。その投資が必要になったということもある。患者の個人情報への不正なアクセスについての法的闘争を行うことと、よいプライバシー担当官、危機管理担当官、コンプライアンス担当官等を雇用、配置することをくらべたら、後者の方が経済的といえる。一方、HIPAA 法によって、保険請求の統一化、請求コード等統一等により、医療事務負担の低減が図られている。

○ complaint の状況について

→DHHS の OCR には数千の告発があり、DOJ にも移管され、有罪の判決が出たこともある(ワシントン州シアトルの例)。病院職員が自分の情報への不正アクセスへの不安があるのは事実で、実際に内部告発も存在する。

○ 監査について

・内部における監査は実際行われていると思われるか、適切であると思われるか？

→比較的適切に行われていると思われる。記録が必要で、監査の可能性もあるので、今のところ、しっかりした情報はないが、悪い噂は聞かない。

○ HIPAA 法 Privacy 施行後における社会状況の変化と今後の見通し

→2002 年には、AMA、全米病院協会等が法案へのコメントや修正要求を出した。現在も、account の期間に関する変更を求めている。今後は、より協力的になっていくのではないかと考えられる。

・HIPAA を口実に患者への情報開示を断る事例が発生しているということを聞いたがどういうことか。

→あまりありえないと思われる。

・一般市民や患者の、HIPAA 法の存在や

目的、規定についての、理解度や浸透度はどの程度か。

→HIPAA 法の求めるところにより、国民は、医療機関受診の際に自らの権利について知らされることになっているから、十分認知されていることと思われる。

#### ○ 診療録の法的根拠について

・医師法、医療法、社会保障法等における医師の診療録記載の義務および保存義務はどのように整理されているのか。

→支払請求の証拠書類としてカルテの文書化と保存が必要である。文書化は求められているが、その内容、項目等については規定されていない。新しくメディケア用に連邦法ができていて保存期間は州と文書の書類によって異なり、7、10、20年程度である。

・診療録の電子保存に関する法的体系はどのように整理されているのか

→紙でも電子媒体でも、規定年数保存することになっている。真正性は、医療機関は、医療記録に関する監査を受けることになっていることで対応。

・電子カルテに関する法的規制や法的要件は具体的に制定されているか、

→連邦レベルでの電子カルテは存在しない。国や政府レベルでの「電子カルテの要件」に関する法律、通知等はない。セキュリティについては HIPAA のセキュリティ法の

み存在している。

#### D. 考察

米国会計監査院の報告による米国での医療分野における個人情報保護である HIPAA 法 Privacy 規則施行後の状況は、初年度は概ね良好にスタートし、医療機関や保険者の職員は個人情報の取扱いやその手順に敏感になってきたこと、Privacy 規則への遵守への要領について理解が得られてきている。一方で、運営面での課題や誤解による障害も見られ、その代表的なものとして、公衆衛生を目的として法で定められている患者情報の報告等にかかる情報の追跡に関する負担、及び委託先との契約の見直しがあげられていた。また、Privacy 規則について十分理解を深めていない医療機関や保険者においては、個人情報の取扱いに法の求める以上に過敏になっており、それが、研究や公衆衛生面での業務実施に影響を与えていることが指摘されている。

また HIMSS の報告においても、会計監査院の報告はある程度裏づけされると考えられた。

特に、医療機関において、①院内における情報開示の責任体制の整備、②診察室等臨床現場で患者のプライバシーを確保すること、が困難であったこと、また、保険者において、①第三者からの患者の個人情報の開示要求があったときの情報を必要最小限に絞る手法、②委託業者との契約締結、が困難であったこ

とは、我が国の医療機関においても同様の状況が想定される。

我国はこれらの先例に基づき、厚生労働省をはじめとした業界団体等によるガイドラインの整備に力をいれ、とくに委託先との契約内容、苦情の際に対応すべき事項等について、ある程度明らかにしておくことが望ましいと考えられる。

における物理的な患者のプライバシー保護、法的側面を含む委託契約の内容、等については、一医療機関における考察や対応では困難を伴うことが予想され、国レベルまたは医師会や病院会等の団体による実践的なガイドラインを提供することが望まれていると考えられる。

さらに、HIPAA 法は Privacy 規則以外にも、Security 規則、Transaction, Code set 規則等も含んでいるが、これらに対応するための医療機関における年間予算が、100 床以下で 500 万円、100-400 床で 2500 万円、400 床以上で 1 億円程度必要との統計が出ていることは、医療機関にとっての負担が非常に大きなことが予想される。我が国においても、今後、個人情報保護法の摘要後、e-Japan 推進計画に基づいて電子カルテの普及、オンラインレセプト等が推進された場合、医療機関の負担は同様なものとなると考えられ、これに先駆け、そのためのインセンティブや予算措置等を検討する必要があると考えられる。

## E. 結論

個人情報保護法は、米国の先行事例を見る限り、施行後 1 年で多くの医療機関が適正に準拠する傾向にあり、当初の混乱も解消しつつある。一方、院内の体制整備、診察室等



研究成果の刊行に関する一覧表

雑誌

発表者氏名	論文タイトル名	発表誌名	巻号	ページ	出版年
山本隆一	電子カルテの進展と医療情報保護	診療録管理	Vol. 16、 No. 1	Pp8-17	2004
山本隆一	医療情報のセキュリティ	クリニカルプラクティス	Vol. 23、 No. 11	Pp98 -101	2004

# 電子カルテの進展と医療情報保護

## *Security and Privacy on Electronic Health Record*

山本 隆一

### 1. はじめに

電子カルテという言葉はあいまいな言葉で、すでにいわゆる電子カルテを導入している医療機関も少なからず存在するが、それぞれ扱う情報の範囲や運用は異なり、導入した施設の数だけの種類の電子カルテがあると言っても過言ではない。2003年に日本医療情報学会が電子カルテの定義に関する見解(1)をまとめたが、かなり幅の広い定義になっている。またやや古い1996年に日本保健医療福祉工業会がまとめた電子カルテのレベル定義でも幅広く電子カルテをとらえている。

本稿で定義云々を長々と議論することは診療録管理の立場から診療情報の安全管理や個人情報保護を考えるという本来の目的から外れるが、言葉を使う以上は一定の定義が必要である。そこで、本稿では電子カルテを「診療録の一部または全部を情報の発生から保存にいたる全過程を実質的に電子的に行うもの」と定義して用いることにした。「実質的に」とわざわざ書いているのは、電子保存への対策が未整備で、形式的に紙に印刷して保存のためだけに用いている医療機関が存在するからである。そのような施設でも安全管理上や個人情報保護上の要件は変わらない。

以上のような定義で電子カルテをとらえると、診療録管理上2つの場合にわけて考える必要がある。ひとつはいわゆるペーパーレス運用をする場合で、電子化情報だけに注目すればよい。もうひとつは電子化情報と紙などの物理媒体上の情報が混在する場合で、この2つは安全管理上や個人情報

保護上の扱いに多少の違いが生じる。

さて電子カルテに関する概念の一応の整理ができたので、本論に入りたい。最初に医療の電子化と電子カルテの意義を考え、電子カルテの安全管理について触れ、つぎに診療情報とプライバシーについて概観する。さらにプライバシーに関連する事項も含めた診療情報の安全管理について述べ、具体的対策の一つである JIS Q15001を紹介する。

### 2. 医療の電子化と電子カルテ進展の意義

医療は本来、患者さんと、医師を中心とする医療担当者の極めて個別性の高い関係の中で成立するもので、いわば人間同士のつきあいを基本とする。端的に言えばその中に情報機器が主役を演じる余地は少ない。うかつに情報化を導入すれば、医療の基礎である人間関係が希薄になる可能性さえある。現在の医療に何か問題があって、それを解決するのに情報技術が役立ち、さらに副作用が十分小さいことを確かめて、はじめて導入すべきものだと考えるべきであろう。新薬や新しい医療機器を使うのと同様である。それにもかかわらず医療の情報化は確実かつ急速に進行しつつある。

では、現在の医療にどのような問題があるのだろうか。大小様々な問題が指摘されているが、ここでは4つの問題にしばって論じたい。最初に「情報の共有」に関する問題を考える。かつて医療の大部分は一对一で行われてきた。つまり一人の医師と一人の患者だけが関係して、その患者の一生にわたってそれだけで終わることが多かった。このような場合、情報の共有は問題にならない。しかし現在の高度に発達した医療では、一人の医療従事者で一人の患者の問題すべてに対応す

Ryuichi Yamamoto

東京大学大学院情報学環 助教授

〒113-8655 東京都文京区本郷7-3-1

ることは不可能である。分業が進み、院内分業もあれば、診療所と特定機能病院のように地域における分業もある。また慢性の疾患が問題になるにつれて、断続的な診療がお互いに関連する、いわば時間的な分業も一般的である。分業には情報共有は欠かせない。まさにこのことが診療録管理の重要性の根拠のひとつである。紙やフィルムの物理媒体に記録された診療記録の場合、直接診療記録をすべて渡すか、あらためて要約を作成し、紹介状（診療情報提供書）や依頼状を作成することになる。すべて渡せばもとの部署は一切アクセスできなくなるし渡すボリュームも最近では相当なものである。紹介状や依頼状は転記や要約に時間と労力が必要で、転記によるミスや、必要事項の欠落も起こりえる。これは物理媒体に記録された情報の再利用が難しいことに由来しており、必要な情報が電子化されていれば飛躍的に効率的な情報共有が可能になる。

2番目は医療の品質管理の問題である。電子カルテであろうとなかろうと医療の品質管理が重要なことに異論はないと思われるが、本当の意味で品質管理を行おうとすると、客観的な評価が欠かせない。そのためには広い範囲で詳細な比較が必要で、たとえばA病棟とB病棟の品質比較を紙の診療記録で行おうとすると、時系列の対照表や処置の平均時間の計算など、膨大な手作業が生じ、忙しい医療現場ではすくなくとも継続的には不可能である。施設をまたがっての比較となると、サンプリングするしかなく、やったとしても限定的な意味しか持ちえない。これらは適切に電子化された診療記録でははるかに簡単にできる可能性がある。もっとも後で述べるように適切に電子化することが重要で、不適切な電子化では利点は少ない。

3番目は本論の主題の一部である情報主権の問題で、プライバシーの問題と言いかえても良い。わずか100年前はほとんどの疾病は隠しようもない事実であった。例えば脳卒中にかかれば、生きながらえたとしても様々な程度の麻痺が残り、誰がみても病気であることがわかった。しかし現在では脳卒中の危険因子である高血圧や動脈硬化を疾病ととらえて積極的に管理している。これに

よって脳卒中は減少し、医学の進歩と言える。しかし高血圧や動脈硬化はそれ自体では生活に目立った制限を加えない。つまり外観からでは容易に疾患の有無を判別できない。最近ではもっと軽微な変化さえも健康管理の指標として重要視されつつあり、遺伝子パターンなどもその例としてあげることができる。このような疾病または健康に関する情報が、もし社会に知れ渡ればその人の生活に大きな影響を与える可能性がある。脳卒中は極端な例であるが、あらゆる健康情報は不用意に公表すべきものではない。近代的な個人情報保護の考え方はあとで詳述するが、個人の健康情報は原則として当該情報の主権者、すなわち本人のコントロールにゆだねることになる。例えば「血液型とインシュリンを打っているという事実はすべての人に公開しても良いが、高脂血症があることは病院の人と家族だけ、父親が血友病で亡くなったことは主治医だけしか知られたくありません。」というような要望がありうる。あった場合に紙の診療記録では対処が非常に難しく、実質的には不可能であろう。もちろん現時点ではこのような要求にはこたえられないということで済んでしまう可能性が高いが、医療機関によって対応可能、対応不可能の差が明確になってきた場合は患者の医療機関選択の根拠にならないともいえない。患者のプライバシーに関しては、ただ秘密を守るという医療従事者の義務であった時期が長く続いてきた。守秘義務だけでよければ物理媒体に記録された情報も、電子化情報もおおきな違いはない。しかし、近代的なプライバシーは自己の情報をコントロールする権利である、という考え方に対応するためには、さまざまな情報の単位でアクセスを制御する必要があり、適切な電子化は避けられない。

4番目はスペースと利用性の問題である。紙の診療記録やフィルムが保管に膨大なスペースを必要とすることは一度でも保管庫を見れば容易に理解できる。電子化された情報はハードディスク、CDやDVDに記録すれば保管に必要なスペースは著しく小さくなることは間違いない。日本は土地代が高価でスペースは確かに重要な要素であろう。しかし、さらに大きな問題は利用性である。

ものを整理して保管する場合、何らかの順番付けを行う。診療記録の場合、患者 ID や氏名で並べることが考えられるが、仮に患者 ID 順に整理した場合、棚には ID 番号順に整然と診療記録が並ぶことになる。ID 番号がわからない診療記録を探す場合は、氏名がわかっているならば、氏名からまず ID 番号を調べ、その ID 番号で探すことになる。そのためには氏名と ID 番号の対応台帳をあらかじめ作る必要がある。また氏名もわからないが、診断名と最後の受診日がわかっている場合はどうすればよいか。その日付に受診した人の ID 番号を調べ、その ID 番号の診療記録を順番に調べて診断名が一致するものを選び出すことになる。もちろん台帳をコンピュータ化し、考え付く属性を入力しておけば、かなり効率があがるが、入力されていない属性をキーにする場合は膨大な手間がかかる。学会発表に使うような貴重な症例はこんな手間はかけられないので、一度苦労して診療記録を借り出したら、返さずに別に保存するという事態も起こりかねない。極端な場合、保管庫には使われない診療記録だけが並び、貴重な症例は探しても見つからない、といったことになる可能性もある。必要な時に使用できないのではそもそも保管の意味が問われることになる。これに対して適切に電子化した情報をデータベースに保存すれば、余程まずい設計をしない限り上記のような検索は自在に、そしてすばやく行うことができる。

これ以外にも現在の医療で多少とも問題となっている部分が電子カルテの導入で改善されることは数多くあると思われるが、ここにあげた4つの理由だけでも導入を進めるには十分な動機になると考えられる。

### 3. 電子カルテの問題点—セキュリティとプライバシー保護

利点は明らかだが電子カルテの導入はそれほど急速に進んでいるわけではない。それは短所が存在するからで、切れの良い新薬にしばしば重大な副作用があることと似ている。短所ですぐに思いつくのは入力のコストである。しかしこれは使う側の IT リテラシーや診療状況にも依存するし、

また、技術的にも工夫の余地がある。現状でもかなり多くの診療所でいわゆる電子カルテが使われているし、大規模で高度な先進医療を行う病院で使用しているところも増えてきている。問題はあがるが、徐々に改善されつつあると言ってよいだろう。

利用者からは見えにくいですが、重要で解決しなければならない問題点は安全性（セキュリティ）とプライバシー保護であろう。プライバシー保護は電子カルテに限った問題ではないので、項をあらためて論ずることにし、ここでは安全性を主に扱う。安全性は機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）の3つが確保されることで達成されると言われている。この3つの要素を英文の頭文字をとって CIA と呼ぶこともある。機密性は、知る必要がない、または知ることが許されていない人や機器が情報にアクセスできないことを指す。完全性は一旦作成された情報が、情報作成の責任者が明確で、不正に書き換えたりされないように情報を保護するを指す。可用性は情報が必要な時に適切に利用できることを保障することを指す。

安全性の確保は重要で、例えばある患者が継続して受診しているのに、これまでの診療記録が利用できなくなることは許されないし、入院患者に対して主治医が行った処方が第三者に書き換えられてもいけない。また入院患者の病名がインターネットから誰でも見ることができてはいけない。紙の診療記録では筆跡や紙やインクの劣化の程度などで、不正な書き換えが検出できるとされているし、そもそも紙の診療記録は丈夫なもので、停電でも蠟燭の灯りがあれば利用可能である。また不用意に廃棄したり大量のコピーでもしない限り不特定多数の人が見ることもありえない。これに対して電子化された情報は誰が入力しても同じものができるし、大量のコピーもきわめて簡単に短時間にできる。またネットワークに接続されていれば、適切な対策をしない限りネットワーク上から容易にアクセスできる。

こう書くと電子カルテは大変危険なシステムに見えるが、実際には安全上の問題のかなりの部分はすでに解決されている。技術的に詳しく解説す

ることは本稿の目的ではないが、電子署名と呼ばれる技術などを用いれば、筆跡や紙・インクの劣化よりはるかに嚴重に作成者の限定や不正な書き換えの防止することができる。またファイアウォールと呼ばれるネットワーク上の検問所は適切に設置していれば、病棟の詰め所に忍び込んで、カルテを盗み見するよりはるかに安全に運用することが可能である。つまり機密性や完全性はかなりのレベルで達成可能となっている。可用性は、さすがに蝋燭の灯りだけではコンピュータは動かないが、無停電電源装置 (UPS) も安価になり、また電池駆動のノート PC も高機能になっている。通常の短時間の停電なら対処は不可能ではない。ではすべて解決したのかということそうではない。技術的、理論的には道具はそろっているが、電子カルテをはじめとする診療情報システムはシステムだけで完結した機能を持つものではなく、むしろ非常に多くの場面で、利用者である人とのインターフェイスを持つ。この、人とシステムのかかわり方が問題として残っている。電子署名のプログラムを書くことはそれほど難しいことでも高くつくことでもない。しかし電子署名をするためには電子の印鑑に相当する秘密鍵を用意する必要がある。秘密鍵はその名のおり秘密情報で、その鍵の所有者だけが使えるから意味がある。これを例えば他人に貸したりすれば、まったく意味がない。パスワードを人に教えたり、IC カード (スマートカード) を人に貸したりすることは問題外であるが、容易に推測できるパスワードを使ったり、IC カードを置き忘れることも情報の安全管理上の大きな問題になる。また診療情報はどんなにすぐれた電子カルテシステムを作ってもシステムの中だけに留まることはない。入力前に口頭でやりとりすることもあるし、結果を患者にメモにして渡したり、口頭で説明したりする。このようなシステムから離れた部分の情報の扱いにも十分な注意を払う必要がある。

いかに安全な電子カルテシステムを作っても、使う人も含めて対応しなければ安全性は確保できない。忙しい医療の現場では人の対応には限界があり、安全のために利用者の使い方に多大な制限を課すシステムは結果的に安全性を確保できない

ことになる。一方で、利用者の安全への意識が高く、しっかりした運用をすれば、システムの安全機能はある程度軽く作ることができる。一般にシステムの安全性と利用のしやすさは相反関係にあり、システムで安全性を確保しようとするほど、利用性は低下し、価格も高騰する。安全性の確保は運用とシステムのバランスが重要である。

#### 4. 電子カルテと法規制

プライバシーを論じる前に電子カルテと法律規則の関係に触れる。診療記録の大部分は法律や規則で作成することが義務付けられているもので、その意味では電子カルテも法律や規則で規制されている。しかしそれらの多くは電子化の有無にかかわらず、診療記録自体に対する規制である。電子化された診療記録にだけ関する規制は保存にだけ関するものである。平成11年に厚生省 (当時) が「診療録等の電子媒体への保存について」という通知を出し電子媒体への保存の条件を示した。平成14年には厚生労働省が「診療録等の保存を行う場所について」という通知を出し、医療機関外への保存の条件を示している。いずれも電子化された診療記録に関してはほぼ同様の内容で、真正性の確保、見読性の確保、保存性の確保を条件とし、プライバシー保護への留意とシステム機能と運用の組み合わせで実現することを求めている。

ここでいう真正性とは、先に述べた完全性とほぼ同じ意味である。見読性は可用性とほぼ同じであるが、より具体的に人間が読むことができる状態にできることを指している。保存性は真正性と見読性が法律や規則に定められた保存期間、保たれることを指している。つまり安全性の3つの要素のうち機密性には触れられていない。留意事項にプライバシーの保護があるので、機密性が確保されなければならないことは当然であるが、それは完全性や可用性にも同じことが言える。機密性に特段の言及がない理由は、すでに刑法や各種医療専門職の規定法で守秘義務が明確に規定されているため、紙であろうと電子化情報であろうと機密性は当然であるからである。

つまり法的に有効な電子カルテを運用するにあ

たつては後で述べるプライバシー保護とこれまで述べた安全性の確保を正しく理解すれば問題はない。あえて言えば法的な保存期間を考慮する必要があるが、法的な保存期間というのは紙やフィルムの物理的な容積を考慮した最低限のルールであり、容積の問題の少ない電子化をする以上はこの最低限の保存期間に拘泥することなく、さらに長期の保存を目指すべきである。

## 5. 診療情報とプライバシー保護

### 5.1 プライバシーの概念

診療情報とプライバシー保護を扱う前にプライバシーの概念を整理しておきたい。プライバシーには適切な日本語訳がない。英語の Privacy という言葉も19世紀末にはじめて使われた新しい言葉である。1890年に Wallen と Brandeise が法学の論文に用いたのが最初で、「そっとしておいてもらう権利 (Right to be let alone)」として定義されていた。Privacy は Private という一般的な語から作られたものだが、Private の語源はラテン後の Privo で、これは「奪い取る」とか「切り出す」という意味である。つまり社会的な存在である人間が社会から私的な部分を「奪い取る」または「切り出す」ことを指している (図1)。しかし考えてみれば私的な部分をいうのもあいまいなもので、たとえば勤務先やマスコミなどに対して家庭は私的な部分と考える人が多いが、家庭内でも個人の私的な部分が存在すると考える人も多い。つまり私的な部分は状況によって変化する可能性があるもので、これを合理的に定義することは難しい (図2)。人類は太古から社会的生活を営んでおり、

一定の私的部分は存在したが、それ自体があいまいであり、さまざまな社会的な制度の大きな変化のなかで他の人権が優先された結果、19世紀末まで Private な領域を守る権利自体を明確に示す言葉が存在しなかったのであろう。

ではなぜ19世紀末にあらためてクローズアップされたのであろうか。それはコミュニケーションの飛躍的な発展が大きく関係している。当時印刷技術は急速に普及し、新聞が大量に発行されるようになった。新聞は売り上げを伸ばすために世俗的な関心を呼ぶことを売り物にし、いわゆるゴシップ記事が世の中に大量にあふれることになった。つまり Private な部分を公にすることが商品価値を生むようになったといえる。このような状況ではじめて Private な部分を守ることが人権としてクローズアップされるようになったと考えてよい。したがってこの時点での Privacy は当然「私的な事項を隠す」権利であった。この考え方がほぼ100年続いたが、20世紀末に Privacy の概念は大きく変化する。

いくつかの判例や事件があったが、象徴的なことは1970年に米国で Privacy act (プライバシー法) が成立したことであろう。法律の名前は単純かつ直裁的であるが、名前の印象と法律の中身はかなり違う。この法律は連邦政府の職員だけを対象としたもので、一般の人は対象ではない。このころ、米国連邦政府は行政業務にコンピュータを積極的に導入しはじめた。つまり国民の情報管理にコンピュータを用いはじめたのである。当然ながら大きな議論が起こり、その結果この法律ができたと考えてよい。

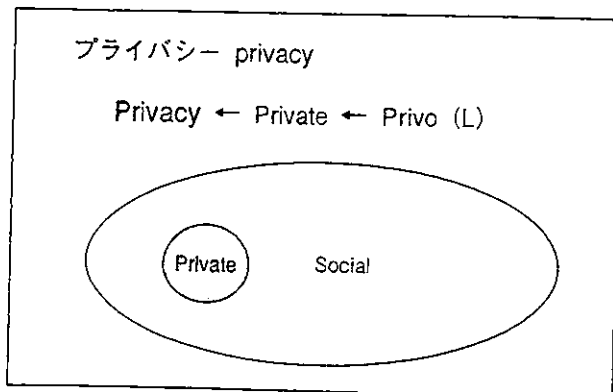


図1 プライバシーとは社会から私的な部分を奪い取るまたは切り出すことであった。

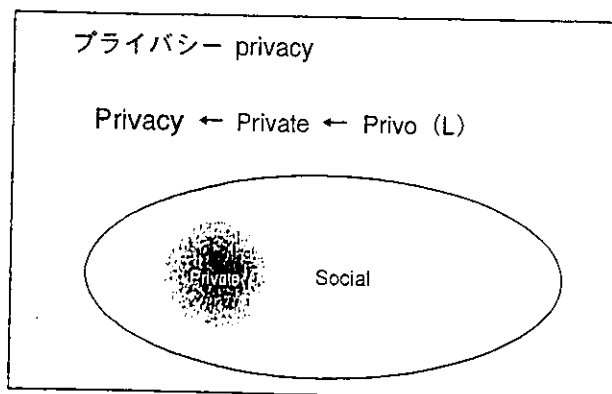


図2 社会と私的な領域の境界はかならずしも明瞭ではない。

ここで重要なことは、連邦政府が個人の情報を、コンピュータを用いて管理する主目的は行政サービスの向上であり、振り返って見ても国民の個人情報を情報技術を用いて効率的に扱うことは米国民にとって利益があったことは疑いがない。一方で日々発展する情報技術は予想外の情報活用方法を生み出し、使い方をあやまれば、国民の個人生活に大きな負の影響を及ぼすことになる。つまり個人情報を適切に利用することは本人に利益をもたらすが、無制限な利用は許されないということになる。では適切な利用とは何か。人間が社会的な存在である以上、所属するコミュニティの公共の福祉は配慮されなければならないのは当然であろう。それ以外の社会の中での利益背反事象ではどのような基準で適切と判断すればよいのであろうか。本稿の最初で述べたようにそもそも範囲があいまいな私的部分の扱いを具体的に定義することがかなり難しい。そこで、個人情報に対して主権という概念を導入し、個人情報は主権者がコントロールする権利を持つ、という考え方が導入された。つまり公共の福祉に反しない限り、個人に関する情報は当該個人がコントロールする権利をプライバシーと再定義したわけである。社会の情報化によってプライバシーの概念が変化したといえる。

その後、このプライバシーの考え方は急速に普及し、1980年には OECD（経済協力開発機構：Organisation for Economic Co-operation and Development）が Privacy 保護の指針（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data）を発表し、加盟国は制度整備をすることを求めた。1995年にはヨーロッパ連合（EU）が加盟国に OECD の指針に基づいた法整備をすることを求める指令を出し、同時に、EU と個人情報を交換するすべての国にも法整備を求め、2003年にはわが国で個人情報保護法が成立した。

あらためて強調しておきたいが、プライバシーの概念の変化は社会の情報化に対応する形で起こった。情報技術の進歩により個人情報の扱いが大きく変化し、行政も企業も保健医療福祉分野でも個人情報を活用することによって効率的なサー

ビスを行うことができるようになった。一方で、個人の意に反した個人情報の利用も容易に可能となったために、明確な人権としてのプライバシーが重要な意味を持つようになったと言える。個人の立場から見れば、適切に個人情報を活用しなければ情報化社会では十分な利益を享受できないが、無制限な個人情報の利用は法律や規則を利用して防がなければならないということになる。

## 5.2 OECD のプライバシーガイドライン

では、個人の情報を本人がコントロールすることができるという人権を守るとは具体的にどういうことであろうか。前節で述べたように1980年以降、各国で法律や基準が作られているが、その多くは OECD のプライバシーガイドラインを基礎としている。そこでこのガイドラインを少し詳細に検討したい。図3は OECD のプライバシーガイドラインの8原則を示している。わが国の個人情報保護法も細かな差はあるが、基本的にはこの原則を踏襲している。端的に述べれば個人情報は合法的に、目的を明示して収集し、明示した目的以外には使用せず、収集した情報は正確、かつ安全に管理し、本人の求めに応じて開示や訂正に対応しなければならない。また個人情報の取り扱い方法を公表し、以上の原則を収集主体の責任のもとに実施する、ということになる。

### OECD Guidelines for privacy

- > 1. Collection limitation principle（収集制限）
- > 2. Data quality principle（データ内容）
- > 3. Purpose specification principle（目的明確化）
- > 4. Use limitation principle（利用制限）
- > 5. Security safeguards principle（安全保護）
- > 6. Openness principle（公開）
- > 7. Individual participation principle（個人参加）
- > 8. Accountability principle（責任）

図3 OECD のプライバシー保護指針

個人から見れば自らの情報を誰が何の目的で収集しているか明確で、自分の情報の状態をいつでも確認することができ、意に反している場合は利用の停止や訂正を求めることができる、ということになる。

ここで重要なことは、合法的収集で、目的が明

示されていて、本人の関与を保障すれば個人情報  
を収集し活用することが可能な点である。収集前  
に本人の同意を得ることは明確には求めていな  
い。しかし収集された情報の状態や取り扱い方  
に対して本人の関与を認めている点から、実質  
的には何らかの同意のもとに個人情報の収集や  
利活用を行う必要がある。

### 5.3 わが国の個人情報保護法

2003年5月にわが国でも個人情報保護に関  
する法律が成立した。5つの法律からなり、基  
本法と民間事業者への規制を含む個人情報保  
護法と、行政機関、独立行政法人をそれぞれ  
対象とする法律の3つが主体で、他の2つは  
法律実施のための整備法である。3つの主  
な法律のうち、基本法の部分は成立後即日  
実施されたが、具体的な規制を含む残りの  
部分は2005年4月に実施される。3つの  
法律の内容はほぼ同じで、行政機関を対象と  
したものおよび、独立行政法人を対象とし  
たものは民間事業者を対象としたものに  
比べてやや厳しい。

法律の内容はほぼOECDの指針を踏襲した  
ものであるが、本人が利用の停止を求め  
ることができる条件でやや制約が強く、結  
果としてOECDの指針より少し後退した  
ものとなっている。具体的には第16～18  
条で、個人情報を収集する場合、あらか  
じめ利用目的を公表するか、取得後ただ  
ちに本人に取得の事実と目的を通知する  
こととなっている。そして第27条で、こ  
れらに違反しているという理由で利用を  
停止することができるとなっている。つ  
まりあらかじめ公表した利用目的で、  
合法的に取得している個人情報を、その  
利用目的の範囲内で利用している場合、  
本人は利用停止を要求できないことにな  
る。また報道目的、学術目的、宗教活動、  
政治活動などが法律の対象外とされてい  
る。

またOECDガイドラインでは直接は触れ  
られていない第三者提供や委託先の監督  
義務など、具体的な項目も盛り込まれて  
いる。これは1980年以降、情報のネッ  
トワーク化や社会の分業化の進展を反映  
したものであろう。

それ以外の特徴としては、罰則を伴う法  
律ではあるが、罰則の適応はかなり慎重  
で、違反があっても直接罰則とはならず、  
一度警告を行い、さら

に違反が続く場合に初めて罰則の適応と  
なる。

一部具体的な記述があるものの全体とし  
ては抽象的な内容で、個々の事業分野に  
おける実際的な個人情報保護手順は法律  
自体には記載がなく理解しづらい。その  
代わりに、認定保護団体を定義し、認定  
保護団体が具体的な指針作りや苦情処理  
を行うことを認めている。

### 5.4 診療情報のプライバシー

これまでプライバシーとその法制度の  
一般論を述べてきたが、具体的に診療情  
報のプライバシーについて考えたい。プ  
ライバシーという概念の対象はあくまで  
個人が識別できる情報であるが、個人が  
識別できる情報といっても現実にはさま  
ざまな情報が含まれる。病院に入るとス  
タッフはネームカードをつけているが、  
ネームカードに書かれた氏名も個人識  
別情報であるし、ある人が進行がんを患  
っているというのも個人識別情報である。  
この2つには一般に明らかに差があり、  
一方は個人識別情報ではあるが、プ  
ライバシーの問題として取り上げられ  
ることはほとんどない(注1)。一方、  
ある特定の人がかつて重篤な病気である  
ことはほぼ常に深刻なプライバシーの  
情報として考えられる。後で触れるが  
日本工業規格のJIS Q15001は組織が  
プライバシー保護を行う計画書(コン  
プライアンス・プログラム)の規格であ  
るが、その中にはプライバシーに機微  
な情報として思想や信条などと共に医  
療に関する情報をあげてきわめて慎重  
に取り扱うことを求めている。つまり  
我々が扱う診療情報はきわめて慎重に  
扱う個人情報ということになる。

これまでに述べたプライバシーの一般  
論を厳しく適応しなければならないとい  
うことになるが、「厳しく」には二通り  
の意味がある。ひとつは極めてプライバ  
シーに機微な情報をあずかる医療機  
関として十分な配慮が要求されること  
で、当然であろう。もうひとつは患者  
の立場にたった厳しさである。一般論  
として論じてきたように現代のプ  
ライバシーの考え方は本人のコント  
ロール権すなわち関与権を基本にして  
いる。これは言い換えれば原則として  
本人の同意のもとに取り扱われること  
になる。問題は同意で、少なくとも最  
低限の利用目的に関しては同意しな  
ければ診療を受けるこ



とができない。同意した以上は同意した側にも責任が生じる。旧来の医療従事者の守秘義務はあくまでも医療従事者の義務で、患者側には何が起ころうと責任はない。そのことに比べると、現代のプライバシーの考え方は本人の自己責任に一定の比重がかけられることになり、その意味で患者にきびしい概念といえる。

インフォームドコンセントにまつわる多くの議論で明らかのように、患者と医療従事者には決定的な知識格差があり、医療従事者が説明し、患者が同意をするという過程は決して安易なものではない。医療機関はこのことに配慮することが必要で、そのために利用目的の説明にあたっては十分な理解を得るように勤めなければならない。これが2つ目の「厳しさ」である。クレジットカードの契約書を例にあげると、細かな、しかもなぜか薄い色の印刷でびっしり埋められた契約書には個人情報取り扱いについても詳細に書かれている。読めば理解はできるが、詳細に読むことを前提に書かれているとは思えない。金融に関してはこの程度の同意方法でも問題になることはないが、医療の場合はこれでは不信感を増すだけであろう。

### 5.5 プライバシー保護の実際

さて2005年4月から個人情報保護法が完全実施されるのであるが、ではどうすれば医療現場でプライバシー保護が達成されるのであろうか。先に述べたように個人情報保護法は抽象的で原則的であり、実際の医療現場での対応を導き出すことは難しい。また個人情報保護法を守ればプライバシーが守れるのか、という疑問もある。概して日本の法律は諸外国に比べると抽象的で、さらに規制の範囲も小さいことが多い。これは日本では法律の改正に大変な手間がかかることにも関係があり、法として決めることは最低限にしておき、あとは現場の変化に対応しやすい、行政的な通知・指導、または自主規制的な指針が大きな役割を占めるためである。個人情報保護法も法自体は最低限の規制であり、指針等で具体的な対策を行うことを求めている。しかしながら現時点では保健医療福祉分野の指針は存在しない。

ではどこかが何らかの指針を作成するのを待て

ば良いのかというと、そうではない。すでに法律の実施は決まっているし、この法律自体が世界的に共通である情報の流通の高度な進展を背景に、あらたな基本的人権への配慮として生まれたものである以上は、もっともプライバシーに機微な情報を扱う保健医療福祉機関としては自主的かつ先進的な取り組みを行う必要がある。法律が実施されれば、最低限それに従えばよいという考えではスムーズな医療はなしえなくなる可能性もある。

しかし一方で、我々医療従事者はヒポクラテスの誓いからすでに書かれている「守秘義務」には慣れ親しんではいるが、20世紀後半に変貌したプライバシーの概念には十分対応できていないのも事実で、何らかの指針は必要である。そこで現時点で指針にかわりうる2つの文書について次項以下で紹介し、考察したい。

### 5.6 米国 HIPAA Privacy Standards

1996年に米国では「Health Insurance Portability and Accountability Act: HIPAA」という法律が成立した。これは端的に言えば診療報酬請求にかかわる手続きを強制的に電子化する法律で、2004年から実施される。ネットワークを介して診療報酬請求書やそれにかかわる情報の交換を行うために、セキュリティやプライバシー保護に関して規則を作ることが求められ、2002年にその一環として Privacy Standards が定められた。日本の省令に相当する規則で米国厚生省が作成した。ちなみに米国では日本の個人情報保護法に相当する包括的な Privacy 保護法は存在しない。医療分野が先行した形になっている。この Privacy Standards は医療に特化しているだけに、極めて詳細かつ具体的である。たとえば取得目的の明示と同意に関して言えば、本人の加療 (Treatment)、診療報酬請求 (Payment)、および医療機関の運営に必須の目的 (Operation) に関しては同意を得る必要がないが、それ以外の目的は原則として署名による同意が必要とされている。また医学研究のための利用は退院後や死亡後など本人の同意を得ることが難しいことがあるが、このような場合の倫理委員会の役割なども明快に規定している。また罰則も規程されており、かなり厳しい。詳細かつ具体的であるために、細部ではわが国に受けいれ

難しい部分もあるが、大いに参考にはなる。参考文献に挙げた「医療の個人情報保護とセキュリティ」(2)にはこの Privacy Standards の日本語訳が含まれている。

### 5.7 JIS Q15001 (個人情報保護に関するコンプライアンス・プログラムの要求事項) とプライバシーマーク制度

JIS Q15001は1980年の OECD の指針が発表され、加盟国に制度整備をすることが求められたのに対応して作成された規格で、その後何度か改定されている。またプライバシーマーク制度は、ある事業者がこの規格にそってプライバシー保護に努めていることを認定する制度である。JIS Q15001自体はプライバシー保護を漸進的に達成するための計画について規定したもので、確実にプライバシーが保護されることを保障するものではない。むしろ情報化社会の急速な発展をにらみ、予想外な事態が起こっても速やかに対処できる体制作り重点が置かれている。

具体的にはポリシーと呼ばれる基本方針を作成し、プライバシー保護に関する責任者と監査者を含む体制を定め、扱う個人情報を洗い出し、具体的な手順を定め、実施し、評価および監査を行い、

問題あれば最初にもどって計画を修正する、というサイクルを繰り返すことを基本にしている。この仕組みは PDCA サイクル (Plan Do Check Act Cycle) と呼ばれていて、たとえば ISO9000 シリーズの品質管理や14000シリーズの環境保護にも適応されている考え方である (図4)。そしてこのような手法をとるもっとも大きな理由は、組織の努力という、あいまいに見えることが多い行為を説明可能な明確なものにすることである。

もちろん JIS Q15001にはプライバシー保護のかなり具体的な手順にも言及されており、さらに医療機関向けの指針も存在する(3)。プライバシーマークを取得するかどうかは別にして、保健医療福祉機関がプライバシー保護対策を考える上で大いに参考になる。個人情報保護法との関係は JIS Q15001のほうが法自体よりはるかに具体的で、かつ厳しい。しかし当然ながら JIS Q15001自体に罰則は規程されていないし、また JIS Q15001がプライバシー保護の達成を保障するものではない。プライバシー保護の努力を保障するものである。

したがって、あくまでも公的な規則であり、従わなければ罰則がある米国の Privacy Standards

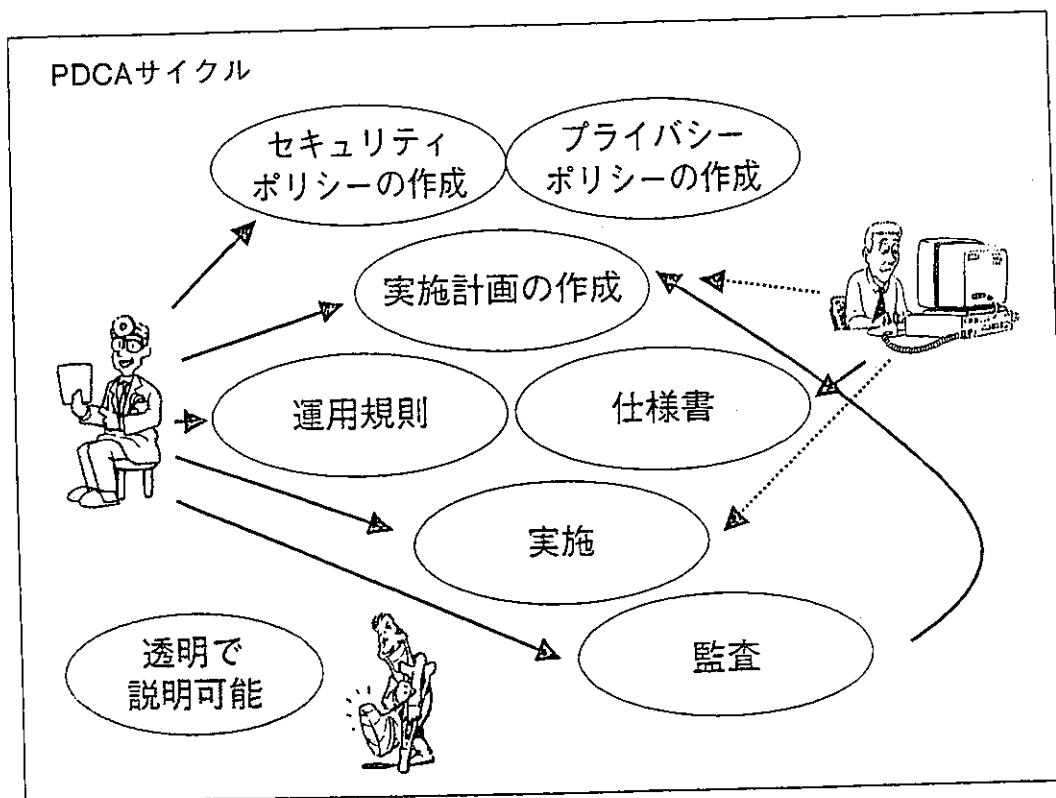


図4 プライバシー保護のPDCA サイクル

とは根本的に考え方が異なる。Privacy は本稿の最初で述べたように、本質的にあいまいなもので、しかも医療においては患者と医療従事者の知識格差を十分配慮した対応が求められるが、そのような定式化が難しい対策においてはある程度の法的な規制は必要なものの、JIS Q15001のような継続的努力を評価する方法もきわめて有効である。

## 6. おわりに

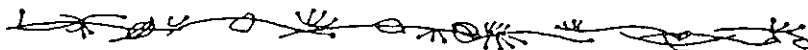
医療の電子化とプライバシーについて論じてきた。残念ながら紙数の関係と現時点で社会的な合意が十分にできていないために、医療現場におけるプライバシー保護の実際の対策の詳細には触れることができなかった。しかしプライバシー保護の基本はプライバシーの本質をまず理解することが必要で、個人情報保護法の具体的な指針が作られる前でも、その本質を理解することは意義深い

と考えられる。また最後に触れた JIS Q15001 およびその医療機関向け指針、さらに米国 HIPAA Privacy Standards は大いに参考になると思われるので、ぜひ一読することを薦めたい。

注1 事業所における名札装着を義務付けることがプライバシーの侵害であるという訴訟は存在した。しかし判決で否定されている。

## 参 考 文 献

- 1) 日本医療情報学会, 「電子カルテの定義に関する日本医療情報学会の見解」, 2003, <http://jami.umin.ac.jp/publication/denshikarute.pdf>
- 2) 開原成允, 樋口範雄編, 「医療の個人情報保護とセキュリティ」, 有斐閣, 東京, 2003
- 3) 財団法人日本情報処理開発協会, 「個人情報保護に関するコンプライアンス・プログラム (JIS Q15001) 医療機関の認定指針 V1.0」, 2002, <http://privacy.medis.jp>



## 医療情報とセキュリティー

### ——概要と今後の動向

山本 隆一

診療情報の電子化に重要なのは「標準化」「安全性」「プライバシー保護」である。情報の安全性は可用性・機密性・真正性を確保することで達成されるが、これにはいずれも単純な技術対策のみでは困難であり、適切なシステムの運用があって初めて安全性が確保される。しかし、システムの運用状況は各医療機関によって異なるため、診療情報の運用状況を念頭に基本方針を定め、それに沿って計画・実施・チェック・評価を繰り返し、確実な実現を図る必要がある。現在わが国には米国のHIPAA Security Standardsのような保健・医療分野の安全基準が整備されておらず、医療機関向けのガイドライン作成が望まれる。

### キーワード

診療情報  
 セキュリティー  
 PDCA サイクル

### ウェブサイト

東京大学大学院情報学環・学際情報学府ホームページ

<http://www.iii.u-tokyo.ac.jp/>

東京大学大学院医学系研究科医療情報経済学/保健医療情報学ホームページ

<http://www.m.u-tokyo.ac.jp/medinfo/>

やまもと りゅういち

東京大学大学院情報学環 助教授

#### 【連絡先】

〒113-0033 東京都文京区本郷7-3-1

東京大学病院管理研究棟4F 企画情報運営部内

東京大学大学院情報学環



### はじめに

診療情報を電子化する利点はほかの論文でも触れられており、あらためて詳細に論じることは避けるが、情報の流通と再利用が行われなければ、その利点は小さい。言い換えれば、流通と再利用ができるように電子化することが必須と言える。そのためにはいくつかの留意すべき点があるが、なかでも重要なのは「標準化」と「安全性」および「プライバシー保護」である。本稿ではそのなかで安全性について述べる。



### 安全性とは

それでは、安全性とは何であろうか。何かが安全であるかどうかは、一般に対象と状況によって異なり、なかなか一概に論じることはできない。診療情報が安全であるということは、医療従事者と患者のいずれから見ても、安心できる状態にあることと考えることができるが、「安心」も人によって異なるであろう。

微妙な問題はケース・バイ・ケースで対応せざるを得ない。しかも、ケース・バイ・ケースと言っても、同じ状況では同じ結果になる必要がある。このような性質の問題に対応するための一般的な対策を以降で論じたい。