は明らかに「個人情報取扱事業者」になります．また，診療録（カルテ）などは，「個人情報データベース」ということになって，やはりこの法律の対象になります．したがって，医療機関もいろいろ守るべきことが出てくるわけですが，その点，先生はどうお考えになりますか．

◆平成17年4月までに医療機関は個人情報保護体制の構築が必要

喜多　最も重要な点としては，患者さんから収集する診療情報の利用目的を事前に明確にして，何に使われるのかを患者さんに知らせ，同意を得るということだと思います．特に，診療情報を病院の外に出すときには注意が必要になると思います．

開原　そうですね．しかし，診療情報を何に使っているかということは，意外に難しい問題ですね．医療機関は，診療情報をこれまでいろいろなことに使ってきました．例をあげてみれば，「診療」に使うことはもちろんですが，「診療報酬請求」，「経営管理」，保健所に報告をするというような「医療行政」，「医療監査や医療評価」，「裁判などの司法関係」，「各種の診断書の発行」それに，「医学教育」や「医学研究」があります．こうした利用法のなかで患者さんが直接かかわったものは，患者さんから暗黙の同意を得たものと見なすことができますが，これまでは患者さんが知らないうちに診療情報を医療機関が使っている場合もあったと思います．もちろん必要があったから使っていたわけですが，個人情報保護法の観点からは許されなくなります．これからは利用目的を明確にして，患者さんからの同意を取り，その利用目的の範囲内で使うことが必要となりますね．

喜多　しかし，同意を得ないで使ってもいい例外規定はありますね．

開原　ええ，同意を得ないで使ってもいい場合も個人情報保護法には書いてあって，その主なものは，その利用が個人情報保護法以外の法律で決まっているものです．たとえば，感染症の届け出などは，感染症法で決まっていますから患者さんの同意を得ないで届け出てもいいわけです．

それにしても，これを厳格に守るのは大変なことで，医療の場合には，すでに死亡した患者さんの情報など，同意を取りたくても取れない場合もあります．また，どうすれば同意を得たことになるかも個人情報保護法には書いてありません．

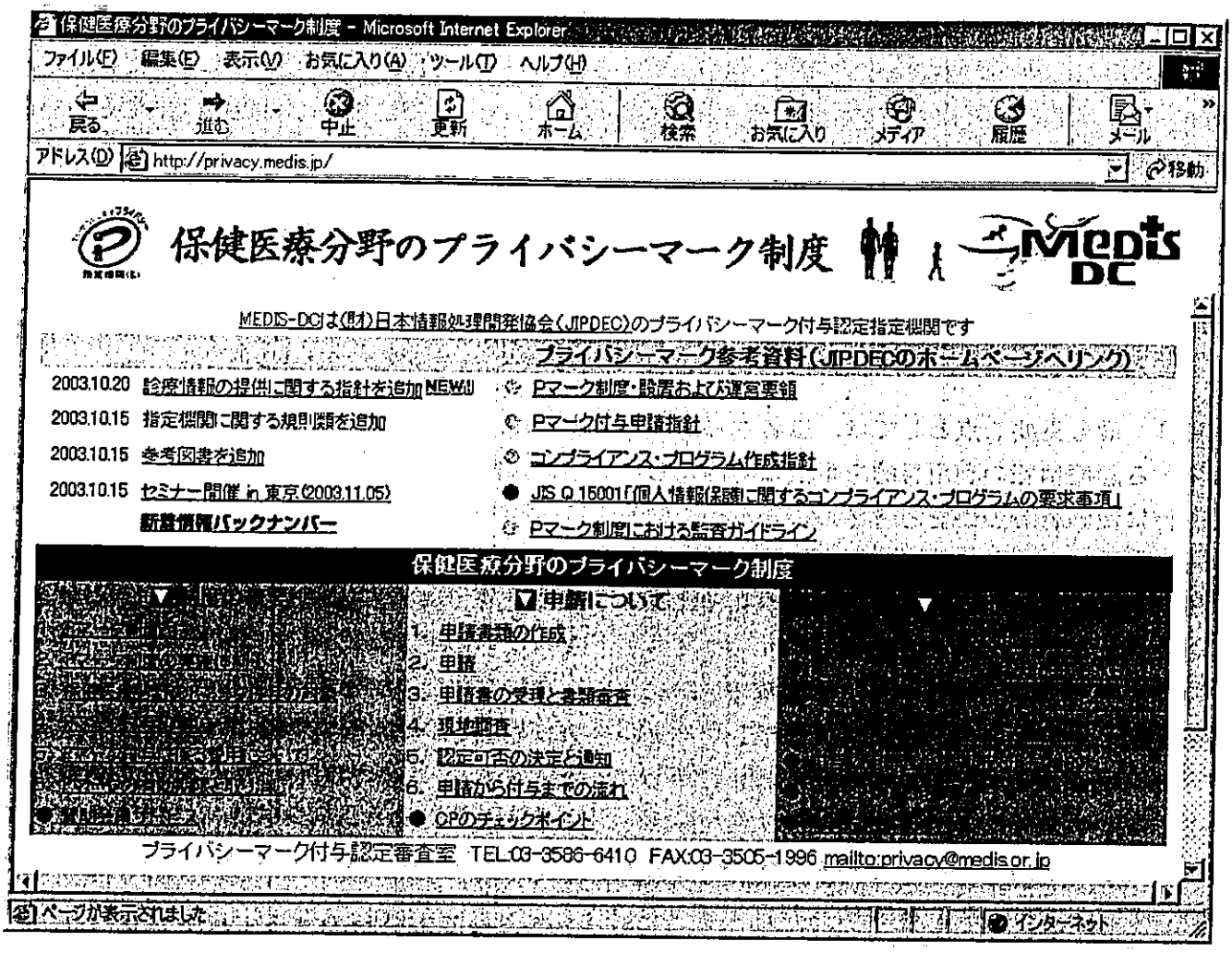
個人情報保護法が完全に施行されるのは平成17年4月1日と決まりました．それまでにこうした具体的な診療情報の取り扱い方法を医療関係者自身で決めて体制を整備していかなければならないのです．

現段階では，いわば手探りでやっていかなければならないのですが，そのための道筋を示したものの1つにプライバシーマーク制度がありますね．そのプライバシーマーク制度について解説していただけませんか．

◆保健医療分野のプライバシーマーク制度とは

喜多　もともと，先ほど話しの出たOECDの8原則を日本でも守るようにするために，1999年に国が日本工業規格で「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（JIS Q 15001）」を制定しました．そしてこのJIS Q 15001を基に，個人情報を扱う企業に対して個人情報保護を徹底させようという趣旨で，（財）日本情報処理開発協会（以下，「JIPDEC」という）が進めてきたのがプライバシーマーク制度です．したがって，プライバシーマーク制度は，企業がJIS Q 15001に準拠した個人情報保護体制を構築していることを間接的に認証する第三者認証制度です．

このような成り立ちから，プライバシーマーク制度は，個人情報保護法の精神を先取りしたものとなっており，ミニマムスタンダードであ



図❷ 医療情報システム開発センターのホームページ

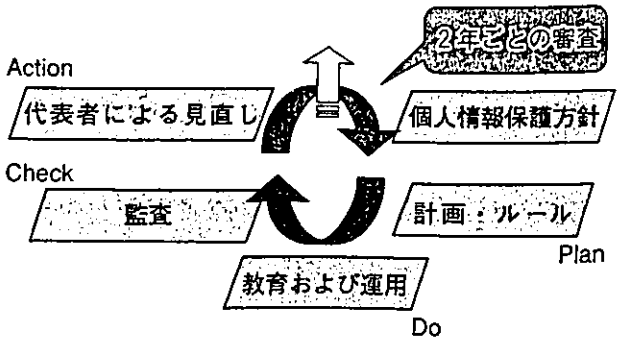
る個人情報保護法より高い保護水準を要求しています.

開原 一般企業向けに作られた制度だと，医療機関に適用するのに困難な面はないのでしょうか.

喜多 プライバシーマークの認定には,「コンプライアンスプログラムの要求事項（JIS Q 15001)」というものが公表されており，この指針に従うことが必要なのですが，このJIS規格は一般企業向けに作られたものなので医療機関に適用するには難しい面がありました．そこでJIPDECは「医療機関の認定指針」を別途作成し公表しており，医療機関の場合にはJIS Q 15001をどのように解釈すべきかを示しています．また，審査機関としても，医療機関の特殊性を考えて,（財）医療情報システム開発センター（以下,「MEDIS-DC」という）を医療機関を審査する団体と定め，プライバシーマーク付与の審査を任せているわけです．特に医療機関に対するプライバシーマーク付与認定制度を「保健医療分野のプライバシーマーク制度」といい，一般企業向けのプライバシーマーク制度と区別して呼んでいます.

この制度の詳細や医療機関の認定指針については，MEDIS-DCのホームページに掲載されているので関心のある方は参照してください（図❷，http://privacy.medis.jp)

開原 医療機関に対する認定指針があるということなのですが，そこではどのようなことまで具体的に書いてあるのですか.



図❸　コンプライアンスプログラムの考え方

喜多　「医療機関の認定指針」はJIS Q 15001の条文ごとに,「医療機関としての解釈」,「最低限のガイドライン」,「推奨されるガイドライン」に分けて，レベルに応じた具体的な方法を明記しています．要求事項をレベル分けしているのは，個人情報保護の具体的なやり方は，各施設の特殊性があり一律に決められるものではないからです．たとえば電子カルテの導入の有無でカルテの管理方法が異なるでしょう．もっと身近な例では，お見舞い客が受付に来たときに，ある名前の入院患者がいるかどうかを，どういう場合に教えて，どういう場合に教えないかという問題などは意外に複雑で，病院によって事情が違うと思います．こうした問題に対しては，病院がきちんとした方針を持っていることが重要なのです．

その意味で，プライバシーマークでは，コンプライアンスプログラムとして，企画（plan），実行（do），監査（check），修正（action）というサイクルを重視しており，これを「PDCAサイクル」などと言います（図❸）．要するに，方針を立て実行してみて，問題があれば修正するということを絶えず行っているということが重要なのであって，人から言われたことをいやいやながらやっているというのでは，決して良くはならないということなのです．

開原　なるほど，しかし医療機関としては，たとえば患者の同意の取り方一つとっても，患者の見えるところに掲示しておけばいいのか，口答で同意を取ればいいのか，それをどこかに記載しなければならないのか，患者にサインをしてもらわなければならないのか，非常に迷うところですね．特に，研究に用いる場合や，研修医に対してカルテを使って研修を行うときなど，すぐ具体的な問題として医療機関は悩むことになりそうですが，その辺りの具体的なことは書いてあるのですか．

喜多　現在の「医療機関の認定指針」には，最低のガイドラインは書いてあります．この例では,「文書を手渡すか，見やすいところに掲示し，内容を理解し，同意したことを確認すること，例えば，初診申し込み用紙などに同意した趣旨を確認できる記載を行う」というようには書いてあります．これ以上の具体的問題は，これから医療関係者が協力してコンセンサスを作っていかなければならないのだと思います．できれば，それが厚生労働省も関与して公式のガイドラインになることが望ましいわけで，たとえば疫学研究の個人情報保護に対してはガイドラインがすでに出ていることはご存じのとおりだと思います．

しかし，一方で，あまり細かいところまで国が関与して決めてしまうのも良くないと思っており，その点，先ほどのPDCAサイクルの考え方はガイドラインが整備されてきた後も重要な考え方として残ると思います．

開原　最近，コンピュータウイルスやハッカーなどが問題になっていますが，今の認定指針では，その点はどうなっているのですか．

喜多　その点も認定指針は当然触れており，こういう点に注意しなさいという項目は示してありますが，具体的にどういうファイアウォールを作るべきであるとか，どういうウイルス対策をするべきであるとか，というところまでは書いてありません．それは病院自身で考えなければなりません．

◆個人情報保護法に対応するには プライバシーマーク取得が早道

開原　最近では，医療機関でもそういうプライバシーマークを取っているところがありますか．

喜多　東京では，河北総合病院，大阪では城東中央病院が取っており，個人情報をしっかり管理しておられます．それを取ることによって，病院の職員の個人情報に対する関心が高まり，また病院自身もいろいろな意味で活性化するなど，副次的な効果を得られたと伺っています．

開原　それは素晴らしいことですね．しかし，医療には周辺にも個人情報を扱う企業などがありますね．たとえば，検査センターや診療事務の請負業者，また少し違いますが健康保険組合も個人情報を持っていることになりますね．こうしたところもプライバシーマークに関心は出てきているのでしょうか．

喜多　はい．むしろ，そうした周辺の企業のほうがより高い関心をもっているとも言えます．また，臨床試験を請負う業者，たとえば一般にCRO（contract research organization）と呼ばれる企業など，すでにプライバシーマークを取っているところもあります．

開原　そうすると，やはり現在のところ医療機関が個人情報保護法に対応するには，保健医療分野のプライバシーマークを取得することがいちばんの早道といえそうですね．

喜多　はい，特に医療機関のような診療情報という非常にデリケートな情報を取り扱う分野では，単に個人情報保護法を満足するのでは十分ではなく，より高いレベルの保護体制を構築する必要があると思います．それには，保健医療分野のプライバシーマーク制度を導入することが最適と思います．

◆プライバシーマークの表示

開原　プライバシーマークを取っている機関は外から分かるのですか？

喜多　たとえば，玄関にプライバシーマークを表示するとか，病院案内やホームページにプライバシーマークを掲げることもできます．また，職員の名刺にこのマークを印刷しておられるところもありますね．

開原　これを認定する側でも，どこがプライバシーマークを取ったかを公表しているのですか．

喜多　JIPDECおよびMEDIS-DCなどのホームページで公開されています．

開原　せっかくそういう制度があるのですから，これからの医療機関はその取得を目指すといいと思うのですが，取得するにはお金がかかるのでしょうか．

喜多　はい．認定料と審査料が必要になります．規模によって価格に違いがありますが，大きな病院で60万円程度です．

開原　取得するのはかなり大変ですか．

喜多　職員の個人情報保護に対する意識を変えることがいちばん大変ですが，それができればあとは文書を整備し実施していくことになります．最近では，医療コンサルタントの方々もこの問題には関心をもっておられますので，医療コンサルタントの方々に相談に乗ってもらう方法もあります．

開原　そうですか．いずれにしても個人情報保護の問題は今後ますます重要になると思いますので，本日のお話は大変参考になりました．どうもありがとうございました．

（ラジオたんぱ；平成15年10月19日放送）

JSRT, Medical Informatics

日本放射線技術学会
医療情報分科会雑誌

No.3 Oct. 2004

特集　個人情報保護法施行を迎えて
・・・セキュリティへの取組み

JAPANESE
SOCIETY
OF
RADIOLOGICAL
TECHNOLOGY

（社）日本放射線技術学会
医療情報分科会
JSRT, Medical Informatics

巻頭言

電子政府の構築と医療の情報化

東京工業大学 フロンティア創造共同研究センター
大山永昭

電子政府の構築と医療の情報化には、いくつもの共通点があるように見える。例えば、電子政府の実現では、はじめに行政機関内の情報化が、次に行政機関間のネットワーク化が、そして最後にインターネット等を介した外部との接続が行われる。この順番は医療の情報化にもそのまま当てはまる。すなわち、はじめは電子カルテなどを用いた医療機関内の情報化が、次は、まもなく公表される「医療情報ネットワーク基盤検討会」の報告書に記された医療機関間のネットワーク化が対応している。そして最後のステップは、次の課題である。

電子政府の構築は、我が国の情報化を推進するために設立された高度情報通信社会推進本部の基本方針に明記された 1995 年から開始され、すでにKWAN(霞ヶ関WANの略で全府省を結ぶネットワーク)やLGWAN(Local Government WANの略で地方自治体間を結ぶネットワーク)、さらには GPKI (Government PKI の略で、大臣等の役職印の電子署名版)やLGPKI(Local GPKI)の整備による第2ステップを終了し、今は最終のインターネットを介した各種の申請・申告のオンライン化などを可能とする第 3 ステップに入っている。そして現在は、2005 年度末までに世界最先端の電子政府を構築するための努力が行われている。一方、医療分野では、電子カルテの普及にさまざまな支援が行われている状況で、医療機関間のネットワーク化はこれから始まると予想される。

電子政府の構築には、電子自治体を含めると、年間 2 兆円以上もの費用を投じている。にもかかわらず、電子政府に関連する IT システム産業、とりわけソフトウエアは輸出になっていない。その原因は、買い手である政府側に IT に関する知識が不足していること、公平な競争環境ができていないことなどが指摘され、すでにITに関する十分な専門知識を有する民間人の全府省への配置や調達制度の改正などに着手している。そして従来型のレガシーシステムのオープン化を目指して、EA (Enterprise Architecture の略で業務・システム最適化と訳している)の導入を図っている。これらの動きは、まさしく戦略的な政府調達を通して、IT 化の本来の目的である国民の生活レベルの向上や国の発展を期すための努力である。医療においても、IHE-J の活動に見られるように、その最終目標は EA 手法の医療情報システムへの適応であろう。この目標が達成され、電子カルテなどの医療情報システムが、電子政府関連の情報システムと同じように輸出につながることが強く望まれる。

一方で、社会の電子化が進むにともなって、個人情報保護の必要性が強く指摘された。そして、このような社会的な要求に応えるために、個人情報保護法が制定され、平成17年4月1日から施行される予定である。ところが最近は、新聞等の報道によると、民間企業などから個人情報の流出事件が起きている。個人情報保護法の施行は、一定レベルの抑止力になると期待されるが、報道されている事件の中には怨恨などによる内部犯行が見受けられる。従来の情報システムの多くは、行政、医療のどちらの分野でも、内部犯行に対して脆弱であると言わざるを得ない。安全で安心そして便利な情報システムを作るためには、そろそろ技術的な仕掛けを組み込むことも必要

特集

個人情報保護法施行を迎えて・・・セキュリティへの取組み
プライバシーマーク制度について

東京工業大学 像情報工学研究施設 特任教授　喜多 紘一

1. はじめに

個人情報保護法が来年の4月に施行されるが、これに対する医療機関側の対応は必ずしも進んでいるとはいえない。個人情報保護法の遵守事項は医療機関が個人情報取扱業者として患者に個人情報のコントロール権を保護することを求めている。

これは、図1に示すように、従来、医療機関側が守秘義務としてコントロール権を持っているとしていたものを患者のコントロール権があるとするものである。従って従来の守秘義務遵守の規程だけでは法を遵守していることにはならない。また、法を犯すことを恐れるあまり利用が制限され、診療に差し支えることがあっては、法律の趣旨に反する。個人情報保護法は従来、各機関によって様々に取り扱われてきた保護レベルを統一した規定に従って個人情報を保護しつつ活用しようというものである。しかし、法律は要求事項しか規定せず、具体的手法が示されていないので、医療機関ではどうしてよいかとまどっているのが現状と思われる。JIS Q 15001は法律が要求するレベルより少し高いレベルで、どのように実現していくか、そのステップに沿って要求事項を規定している。この要求事項を満たして管理できているかを第三者機関が認定するのがプライバシーマーク制度である。

ここでは、その制度の理解を深めるために「プライバシーマーク制度の概要」、「コンプライアンス・プログラム構築の手順」、「プライバシーマーク取得のポイント」および「医療機関としての注意事項」を述べる。

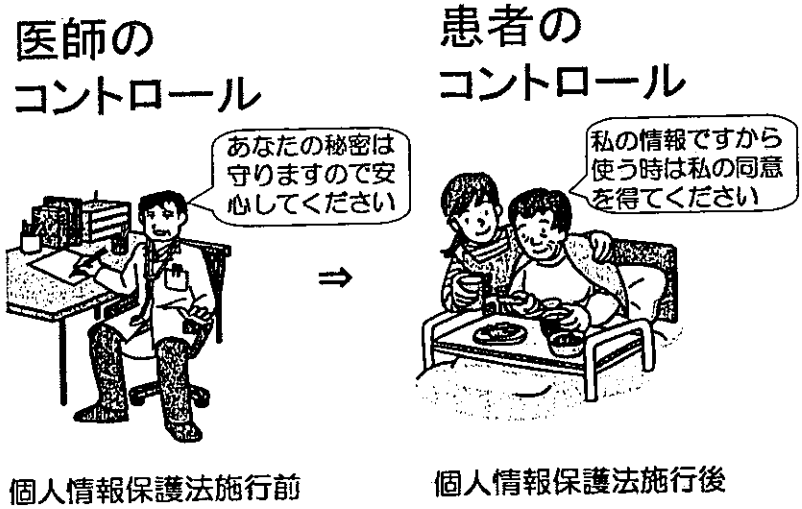


図1 個人情報保護法の概念

比較項目	プライバシーマーク制度	個人情報保護法
		事業者の義務
個人情報保護方針	◎	
計画	◎	
体制及び責任	◎	
個人情報の収集に関する措置収集の原則	○	○
個人情報の利用及び提供に関する措置	○	○
個人情報の適正管理義務	○	○
個人情報に関する情報主体の権利	○	○
教育	◎	
苦情及び相談	○	○
監査	◎	
事業者の代表者による見直し	◎	

図2 プライバシーマーク制度と個人情報保護法の関係

2. プライバシーマークとは

プライバシーマーク制度は、個人情報について適切な保護措置を講ずる体制を整備している事業者であるかを第三者機関である(財)日本情報処理開発協会(JIPDEC)及びその指定機関が評価・認定する制度である。また、その証としてプライバシーマークと称するロゴの使用を許諾している。その認定根拠は、日本工業規格で定めるJIS Q 15001「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」を基本にしている。保健医療分野に関しては(財)医療情報システム開発センターが指定機関になっている。

個人情報保護法は2005年4月1日より施行され、医療機関も個人情報取扱事業者となるので、法律が適用され、個人情報保護法遵守は病院経営者の義務となり、さけて通ることができなくなる。個人情報保護法に対応するための要求事項は守秘義務だけではなく、患者の情報に対する患者のコントロール権を保証することや、情報の適正な管理方針を明確にすることもふくまれるので2005年4月1日に医療機関は何も対応しないですますことはできない。何らかの対策が必要である。いたずらに、守秘義務を守ることに終始し、情報を十分活用できなければ、情報化の意味が半減してしまう。

プライバシーマーク制度はこの場合、病院経営者の個人情報保護推進のよりどころとなる制度である。特に電子カルテ等の情報システムを導入した医療機関ではその便利さの享受と個人情報保護は車の両輪である。電子カルテを有効に運用するためには、個人情報保護を積極的に進める必要がある。何か問題になり訴訟になった場合、善管注意義務を果たしていないと、相手に責任があっても訴訟に耐えられなくなり、賠償も相殺になって損失を回収出来なくなってしまう。

JIS Q 15001「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」と個人情報保護法の関係は図2の様である。個人情報保護法は個人情報取扱業者の義務としての要求事項を定めているがどのように義務を果たすかは規定されていない。JIS Q 15001は何をすべきかを含め、マネージメントとして実現・維持するための守るべき手段も規定している。すなわち、「個人情報保護方針の作成」、「計画」、「体制及び責任」、「教育」、「監査」および「事業の代表者による見直し」を追加することにより個人情報保護のコンプライアンス・プログラムを実現させている。図3にJIS Q 15001の要求事項の一覧を示す。

1. 適用範囲
2. 引用規格
3. 定義
4. コンプライアンス・プログラムの要求事項
  4.1 一般要求事項
  4.2 個人情報保護方針
  4.3 計画
  4.4 実施及び運用
    4.4.1 体制及び責任
    4.4.2 個人情報の収集に関する措置
      4.4.2.1 収集の原則
      4.4.2.2 収集方法の制限
      4.4.2.3 特定の機微な個人情報の収集の禁止
      4.4.2.4 情報主体から直接収集する場合の措置
      4.4.2.5 情報主体から間接的に収集する場合の措置
    4.4.3 個人情報の利用及び提供に関する措置
    4.4.4 個人情報の適正管理義務
    4.4.5 個人情報に関する情報主体の権利
    4.4.6 教育
    4.4.7 苦情及び相談
    4.4.8 コンプライアンス・プログラム文書
    4.4.9 文書管理
  4.5 監査
  4.6 事業者の代表者による見直し

図 3 JIS Q 15001 の要求事項一覧

ステップ 1:個人情報保護方針を定め文書化する
ステップ 2:CP策定のための組織を作る
ステップ 3:CP策定の作業計画をたてる
ステップ 4:個人情報保護方針を組織内に周知する
ステップ 5:個人情報を特定する
ステップ 6:既存の個人情報取扱いシステムを評価する
ステップ 7:CPの構成を検討する
ステップ 8:CPの基本となる規程を策定する
ステップ 9:CPの詳細規程を策定する
ステップ 10:CPを文書化する
ステップ 11:CPに準じた体制の整備を行う
ステップ 12:CPを周知するための研修を実施する
ステップ 13:CPの運用状況を監査する
ステップ 14:CPの改善を実施する
(JIPDEC 資料より抜粋)

図 4 コンプライアンス・プログラム手順

3. コンプライアンス・プログラム構築の手順

コンプライアンス・プログラムとは JIS Q 15001 では「事業者が自ら保有する個人情報を保護するための方針、組織、計画、実施、監査および見直しを含むマネージメントシステム」と定義している。単に規程を指すわけではない。その実現手順は図 4 に示すようなステップが推奨されている。そのステップの中の主なものを以下に解説する。

3.1 個人情報保護方針作成および周知

個人情報保護方針は以下の内容の項目を各施設の状況に合わせて盛り込んだ宣言文を作成し、役員及び従業員に周知、一般の人が入手可能な措置をとることが求められている。

a) 事業の内容及び規模を考慮した適切な個人情報の収集、利用及び提供に関すること。
b) 個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなどの予防並びに是正に関すること。
c) 個人情報に関する法令及びその他の規範を遵守すること。
d) コンプライアンス・プログラムの継続的改善に関すること

3.2 コンプライアンス・プログラム作成のための組織

コンプライアンス・プログラム(以下 CP という)作成のための組織は作成後の CP 推進活動を配慮し、一例として図 5 のような形態が推奨される。医療機関の代表である院長あるいは理事長をトップの下に個人情報保護管理者をおき、個人情報保護の推進をさせる。普通この下にプライバシーマーク推進事務局をおき、この下に各部門からのコンプライアンス・プログラム作成責任者を兼務させる形が推奨される。医療機関の代表者はこうした業務に資源配分を行う責任がある。

コンプライアンス・プログラムを構築するには医療

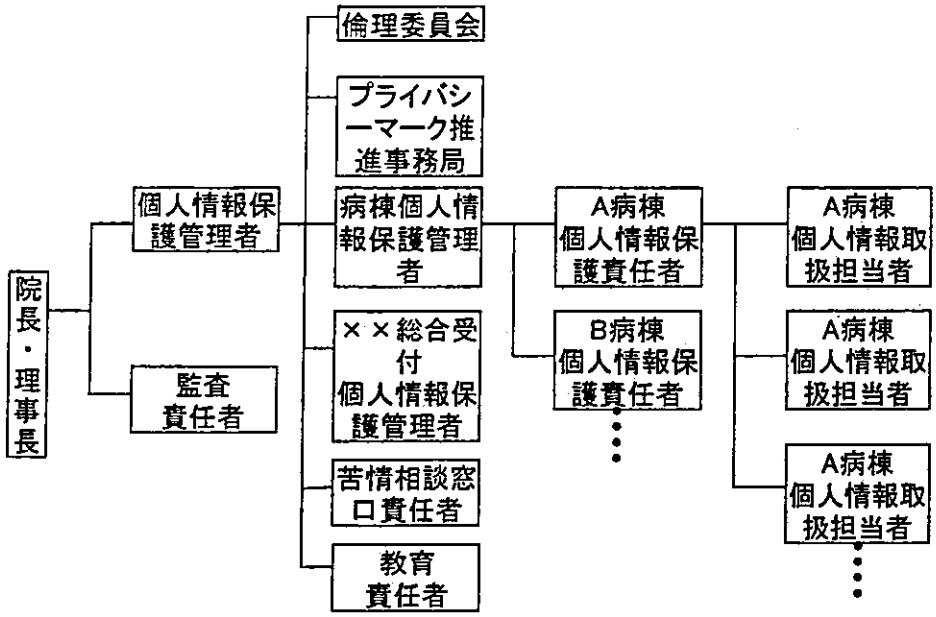


図5 CP策定のための組織作りとCP運用の体制

機関の業務を文章化する必要があり、今まで経験により進められてきてうまくいっていると思われている「業務を分析して文章化する」という頭の切り替えが必要になる。また、医療機関の場合は医師、看護師、技師、事務員等の異なる職種の職員がアウトソースを含めた指揮系統の異なる組織体となっているので責任者の選出に当たっては医療機関ごとの事情に合わせた組織化を配慮すべきである。

3.3 個人情報保護法の特定

個人情報を保護するためには、医療機関内で取扱われている保護されるべき個人情報を特定する必要がある。個人情報は「個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述、又は個人別に付けられた番号、記号その他の符号、画像若しくは音声によって当該個人を識別できるもの(当該情報だけでは識別できないが、他の情報と容易に照合することができ、それによって当該個人を識別できるものを含む)」と定義されている。

図6に医療機関における個人情報を含む書類の例を示す。各部門で使用される伝票、用紙あるいはコンピュータの画面単位で特定するのがわかりやすい。部門あるいは業務フローごとに特定した個人情報ごとに他部門から自部門への入力としての情報収集、提供、預託先と他部門への出力としての提供、委託、返却、開示先を明確にする。また、部門内部で発生する収集または作成された情報あるいは破棄される情報であればそれも明確にし、且つ部門内での情報の取扱い方法および利用目的も明確にする。図7に個人情報の特定と次に述べるリスク分析における脅威の例をあげた。

3.4 リスク分析と対策

特定された個人情報に対してリスクを引き起こす可能性のある脅威を想定する。脅威は情報の外部との授受および部門内での情報処理の際に発生する。それらの場面に対する脅威と現状の対策を評価し、その機関として許容されるリスク以下に抑えられない場合は脆弱な箇所に対して対策を追加する。医療機関では想定しにくいと思われるが、これらの対策には内部要員の出来心からくる脅威を抑制できる仕組みを含めて配慮する必要がある。これは、逆に職員を犯罪の誘惑や危機から救うことにもなり、経営者の責任である。

こうしたリスク分析はまだその医療機関では起こっていないことを仮定することになるので多少被害妄

診察申込書	検査依頼伝票	請求書／領収書
保険証	検査結果報告書	薬歴情報
紹介状	一生化学検査	退院証明書
診察券	一生理検査	院療養計画書
予約票	一超音波検査	手術管理情報
入院申込書	一内視鏡検査	給食管理情報
入院療養計画書	一放射線検査	行政官庁への報告
診療録	看護記録	のための各種届出書等
処方せん	レセプト	

図 6 医療機関における個人情報を含む書類の例

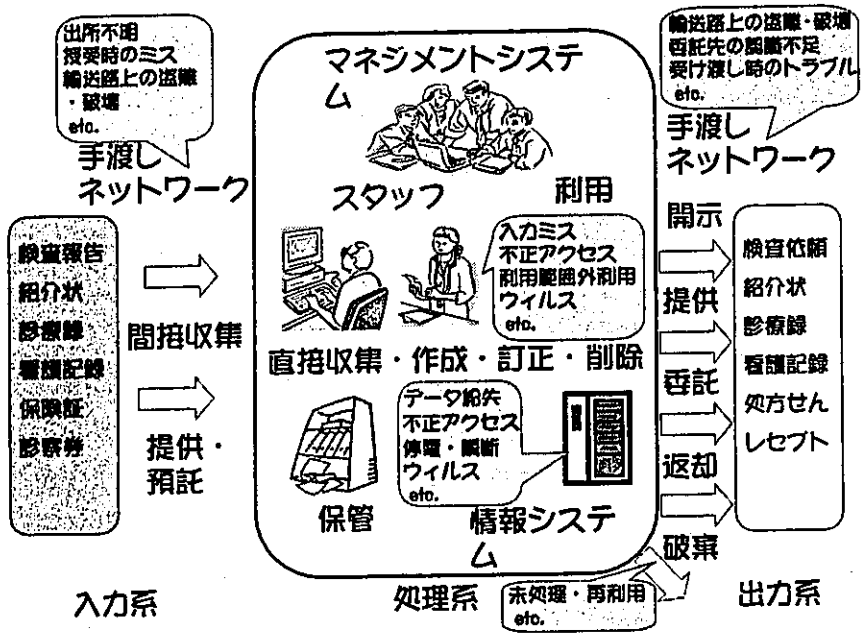


図 7 医療機関における個人情報の特定とリスク分析における脅威例

■ 提供・預託
- ■ 出所確認
- ■ 受け渡しエリアの確保
- ■ 輸送路上の注意
- ■ 授受記録

■保管
- ■ アクセス制限
- ■ ユーザ認証
- ■ 鍵管理
- ■ 記録, ログ
- ■ バックアップ/リカバリ
- ■ 電子保存の基準遵守
- ■ 災害管理

■ 処理・利用
- ■ 正確性の確認
- ■ 利用範囲の確認
- ■ ユーザ認証
- ■ アクセス制限

■ 委託・返却
- ■ 輸送路上の注意
- ■ 授受記録

■ 破棄
- ■ 破棄確認
- ■再利用時の確認

図 8 脆弱性に対する対策例

想的な想像力を要求され、ある程度の訓練を必要とする。この訓練が脅威とその対策に対する職員の感度を挙げることにもつながるので、コンサルタント任せというのは推奨できず、職員も参加して行うべきである。

情報安全は目に見えにくいので想像しにくいが、現在医療事故を未然に防ぐ手法として、患者安全に関した「ヒヤリ・ハット」事例による危険予知訓練や原因分析活動等が盛んに行われており、これらの手法に習うのも一案である。自機関の「ヒヤリ・ハット」レポートによる対策手法はインシデントが起ってから分析を行い、対策を立て、未然に致命的災害を防ぐ手法である。しかし、プライバシーマークでは計画段階で個人情報の特定後、リスクを推定し対策をたてることが要求される。他機関の「ヒヤリ・ハット」事例を自機関に当てはめ、似た事例としてインシデントに至る前に未然に対策を検討する方式がこれに近い。そのための対策例を図8に示す。図7も参考にし、リスク分析の目を養っていただきたい。

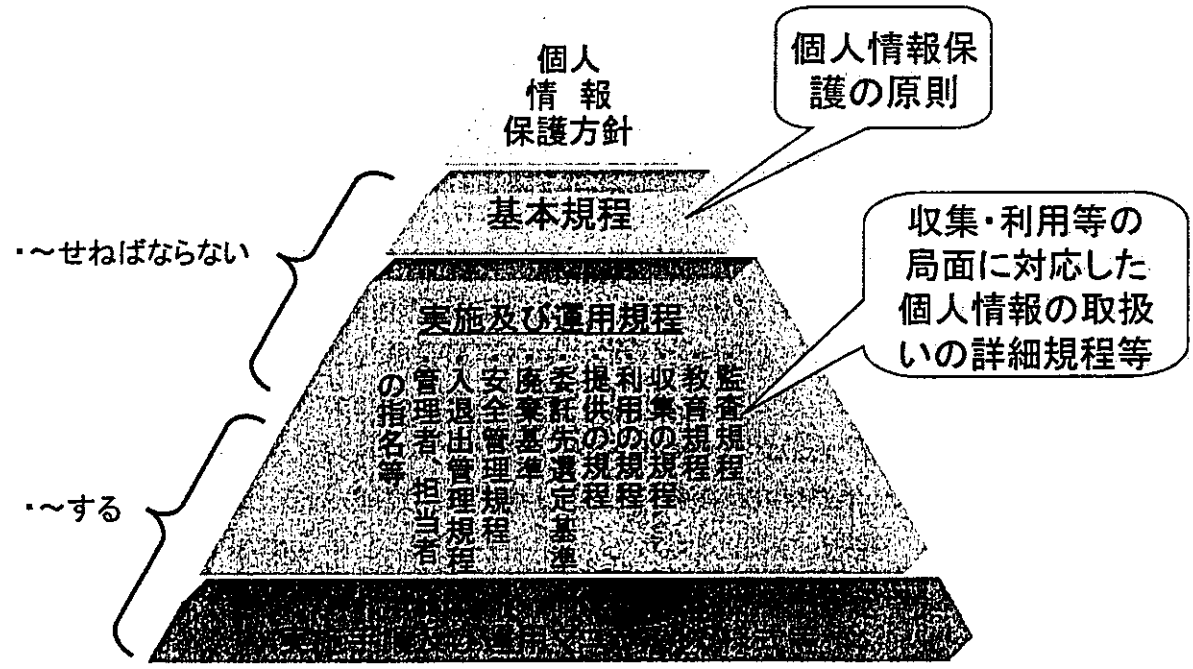
脅威の発生としては以下の様な「脅威を受ける場面」や「脅威を与える動機やきっかけ」が考えられる。

「脅威を受ける場面」としては

a) 情報の処理・授受・運送(うっかり、攻撃)・自宅への仕事の持ち帰り
b) 情報の破棄
c) 保守・研究・緊急時
d) コピーの作成・メールの送信、転送、返信
e) 不正アクセス・不正プログラムの進入
f) 正規のアクセス(脅迫・買収・情けから内部犯罪)

「脅威を与える動機やきっかけ」としては

a) うっかり(重要性の把握欠如・他人の情報なので)
b) 情報の売買
c) 愉快犯(泣き面に蜂)
d) 幹部追い落とし
e) VIPが危険(あるいは特殊)な状態なのでその情報を入手したい



(JIPDEC資料より抜粋)

図9 規模の階層構成

3.5 規定の作成

規程を作成するためにはJIS Q 15001のコンプライアンス・プログラムの要求事項にそって実施方法を文書化する。規程の構成は図9のように「個人情報保護方針」、「基本規程」、「実施および運用規程」、最下部に「実施手順および運用マニュアル、様式等」の4階層に分けることを推奨する。

「基本規程」および「実施および運用規程」は「～すべき」ことを規定する。マニュアルは「～すること」と規定し、誰が実施しても同じ作業に成るレベルまで記述する。マニュアルは機器の更新や組織の変更により必要に応じ改定するつもりで気軽に作成できる必要があり、実際に作業する場所に近い人が作成する。また、その体制を整えておく必要がある。特に後述の「適正な管理」に対しては、リスク分析をおこなった対策が規定またはマニュアルに盛り込まれているか確認する。

3.6 情報主体からの同意

情報を収集する場合には患者から以下の項目について通知し同意を取る必要がある。同意の取り方としては、新患時の問診表提出や入院手続きの際に行うことが考えられる。

a) 医療施設の内部の個人情報に関する管理者名、所属、連絡先
b) 収集目的(診療・経営・診療報酬請求・研究・教育)
c) 提供:個人情報の提供目的、当該情報の受領者、個人情報の取扱いに関する契約の有無
d) 個人情報の預託を行うことの予定(外注検査・診療報酬計算の外注)
e) 情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に生じる結果
f) 個人情報の開示を求める権利、当該情報の訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法

3.7 適正管理義務

適正管理には「正確性の確保」と「安全性の確保」に分かれ、前者は「個人情報は、収集目的に応じ必要な範囲内において、正確、かつ、最新の状態で管理しなければならない。」とされ、後者は「個人情報に関するリスク(個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えい)に対して合理的な安全対策を講じなければならない。」とされている。リスク分析に基づいた対策を運用マニュアルとして記述する。また、電子カルテ等で保存義務のある情報を電子保存する場合は厚生労働省が発行している電子保存に関する基準を満足しなければならない。安全性を高めるにあたり、医療の場合は緊急時も使用できるように可用性の確保も重要である。

対策としては予防対策と発生時に被害を最小限にとどめるための緊急時対策も重要で、そのためにはアクセスログをとり、すぐに分析できるできことも重要である。これは内部犯罪の予防にもつながる。

4. プライバシーマーク取得のポイント

保健医療分野のプライバシーマーク取得は指定機関である(財)医療情報システム開発センター(MEDIS-DC)に申請を行う。MEDIS-DCでは書類審査をしたあと現地調査をおこなう。問題がなければ付与認定を申請者に連絡し、且つ付与機関である(財)日本情報処理開発協会(JIPDEC)へ付与認定の報告をおこなう。申請者はJIPDECとマーク付与の契約を行い、マークが使用できるようになる。申請手数料、現地調査料およびマーク使用料が別々に計算され、また、申請機関の規模によってもそれぞれの費用が異なっている。

審査のポイントはJIS Q 15001に沿って「現在の保護レベルが適切か」「PDCAを継続できる体制にあるか」の2面を審査する。JIS Q 15001は図10に示すようにPDCAサイクルをまわしてステップアップを継続できる体制の確立を要求している。医療機関がリスク分析に従った対策をたて実施し、それを維持しつつ、新しい情報システムの導入時や、業務体制が

変わった場合も新しい規定が必要か判断し必要であれば作成する行動が自動的に行われる体制を要求している。

JIS Q 15001 はこの PDCA のマネージメントサイクルを回し、維持するための仕掛けとして、「トップの意識」「教育」「内部規定違反に対する罰則規定」「監査」「苦情処理」「経営会議等のトップ会議による定期的フォロー」を組み込み、重要視している。従ってプライバシーマーク申請時点でこうしたマネージメントサイクルが 1 回以上回っている必要があり、その証拠が要求される。

監査も個人情報保護管理者とは独立している必要があり、監査責任者は幹部クラスである必要がある。監査責任者は個人情報保護管理者を通さずに医療機関の代表者に直接結果を報告できる体制とする。

医療保険分野のプライバシーマーク取得に関する関連情報は「http://privacy.medis.jp/」(MEDIS-DC のプライバシーマーク制度関連のホームページ)にあるので詳細はそちらを参考にしていただきたい。

5. 医療機関としての注意事項

5.1 医療機関と認定指針

個人情報保護法では「人の生命、身体又は財産の保護のために緊急に必要がある場合はこの限りではない」というような表現がところどころにあって、医療情報は医療機関が自由裁量で取り扱って良いのではないか。また、「大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者が学術研究の用に供する目的で使用する場合」は適用除外となるので、医療情報はもともと次世代の医療のために貢献する研究要素を含んでいるので医療情報は適用除外ではないか。

一方、JIS Q 15001 では「特定の機微な個人情報の収集の禁止」の要求事項があり、機微な情報に「保健医療及び性生活」と明記され、医療情報の収集はそもそも禁止されているのではないか。逆に「宗教等、機微な情報として収集を禁止している医療以外の情報も収集しないと診療ができない」という疑問もでてくる。

そのために、「個人情報保護に関するコンプライアンス・プログラム 医療機関の認定指針」が出されていて、http://privacy.medis.jp/file/shisin030917.pdf からダウンロードできる。この指針の体裁は、最初に「JIS Q 15001 の要求事項」をあげ、それに対する「医療機関としての解釈」を述べ、次に「最低限のガイドライン」と「推奨されるガイドライン」に分けて記述している。推奨されるガイドラインは個々の機関の状況に応じて選択して実施する項目である。

医療機関の認定指針では、患者の同意は極力とることを原則とし、取れない場合はその理由を明確に記録するか、事後にとるかを求めている。運用上取扱いの判断に窮する場合は上長あるいは倫理委員会の判断を仰ぐこととしている。目的外の収集は極力おさえ、必要最低限の収集とする。例外的な収集はその必要な理由を明確にし、記録しておく。また、各機関でのポリシーを明確にし、取扱者や患者によって個人情報の取り扱いが都度異なることがないことを求めている。各機関の特性に応じて、情報に対するアクセス権限管理が異なっていても差し支えないが、患者にもそのポリシーを公表しておく必要がある。

5.2 医療機関でプライバシーマーク制度を推進する場合の注意

医療機関でプライバシーマーク制度を進めるにあたって、一般の情報システムとは異なっているところもあり、医療と一般の商取引が異なっているところがあり、次のような考え方も理解しつつ進める必要がある。

a) 医療は「民法上の委任契約に準じて行われるもの」(通常の商契約に基づいてなされる行為ではない。善意の管理義務)
b) 医療従事者に法律で守秘義務。安全管理上の問題は民法上の問題だけではなく、刑事的な問題になる。

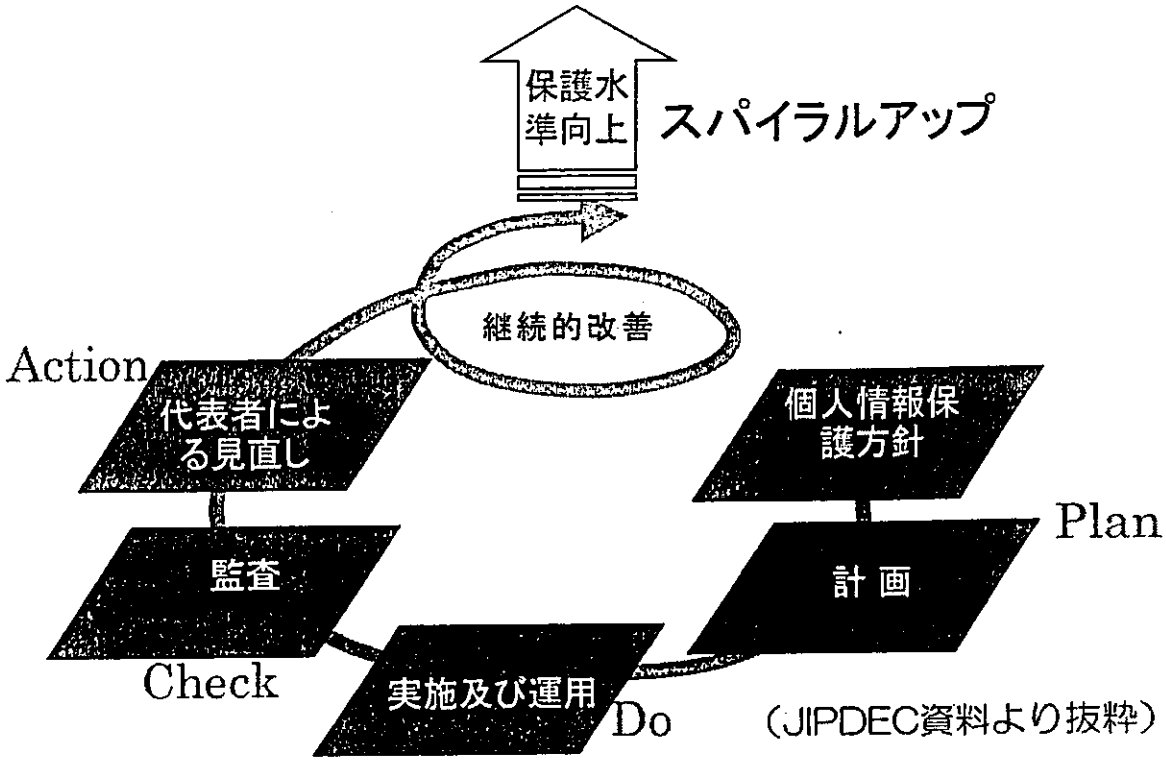


図10 コンプライアンス・プログラムの基本モデル

c) 情報管理者失策による情報安全管理上の問題が、医療従事者や医療機関の損失に直接つながらない。守秘義務違反は親告罪。

d) 損害の対価の算出が困難。ある患者にとって価値がなくても、別の患者にとってきわめて重要な価値を持つことがある。(事故の非可逆性)

e) 医療従事者が情報管理上のリスクの把握が得意でない。医療が委任契約的な行為で、善意を前提に成立しているので医療従事者はミスを過敏なほど考慮するが、悪意を想定することに強い抵抗を持つ。

f) 緊急避難として刑法37条に「自己又は他人の生命、身体、自由又は財産に対する現在の危機を避けるため、やむを得ずにした行為は、これによって生じた害が避けようとした害の程度を超えなかった場合に限り、罰しない。ただし、その限度を超えた場合は、情状により、その刑を軽減し、又は免除することができる。」と規定されている。

また、セキュリティシステム構築の注意事項として

通常の物の売買での商取引では

a) 売主は金を貰えるかが関心事(クレジット番号)

b) 注文者は想像どおりの物をもらえるかが関心事

であるが、医療情報の交換では次のような観点に基づいたシステム構築が必要である。

a) 情報提供者は金をもらっても与えてはいけない情報がある(情報の売買が対象ではない。与えても良い相手か・相手が誰かを認証するのが重要)

b) 情報請求者は情報の出所、真正性・責任者が重要な関心事

c) 本人確認と医師・看護婦・技師等ライセンスの有無の確認が必要

d) 情報価値が人/時間により異なる

e) 受益者あるいは情報主体と情報取扱者が異なる

f) 挙証責任は患者

6. おわりに

医療機関は 6 割ぐらいの業務がアウトソーシングになっていると言われている。従って個人情報保護を確実に行うためにはプライバシーマークを取得しているアウトソーシング先を選択するほうが監督責任を安心して果たせるようになる。

これは、情報システム開発のベンダーに対しても同様で、保守やシステムの据付時に個人情報保護上問題となる行為がないかも監督する必要があり、システム開発ベンダーもプライバシーマークを取得することをお勧めしたい。

プライバシーマークを申請するかは別にして、JIS Q 15001 に従って、個人情報保護体制を構築することをお勧めする。その延長線上として管理レベルを上げ、外部に対して説明責任を果たし、また、内部の保護活動としてのシンボルとするために申請されることをお勧めする。

個人情報保護法は個人の権利を保護しつつ、情報を活用していくための交通規則のようなものであり、価値観が変わっているため、最初はなかなかなじめないところもあるが、患者側も医療機関側も慣れるに従って適切な関係ができてくるものと思われる。

プライバシーマーク取得の効果は個人情報保護の動きへの対応だけでなく、以下の効果もあるので是非、早急にスタートされることをお勧めしたい。

a) 電子カルテ導入で社会的・経済的損失を防ぐために必須
b) 自分の情報を誰が知っているのかに対する説明
c) 患者さんの治療に対する積極的参加意識
d) 診療スタッフの患者情報に対する意識向上
e) 情報管理の明確化
f) 情報管理レベルの向上
g) 取得活動による業務フローの改善と職員の活性化

メモ