医業経営マネジメントレポート

『病院における情報漏えい防止策』

2005 年 4 月完全施行　個人情報保護法

≪　目　次　≫

1　迫る個人情報保護法の完全施行

(1) 個人情報保護対応に遅れる医療機関

「個人情報保護に関する法律（以下「個人情報保護法」という。）」の制定からまもなく２年が経過し、2005 年４月１日からは、同法が罰則も含め完全施行されました。

医療機関で取り扱われる個人情報は、他の業種よりも数および関係する場所が多く、さらにはよりセンシティブに取り扱われるべき性格のものでありながら、現場によっては日常的に放置され、粗雑に扱われているケースも否定できません。

従来、情報保護は医師や看護師等が負う守秘義務を遵守することによって確保されるとされてきましたが、個人情報保護法の施行によって、医療機関が取り扱う個人情報は原則として、本人の承諾なしに利用することができなくなります。すなわち、同法への対応が遅れると、適切な個人情報の管理・運用がなされていないことによって、患者やその家族からの信頼を損なう危険が生じるということを意味します。

○医療機関における主な個人情報の漏えい事例

２００４年 １０月	春日部市立病院（埼玉県春日部市） 患者約2,500人分の個人情報が保存された病院所有パソコン５台が盗まれたことが判明
８月	沖縄赤十字病院（那覇市） 患者の氏名が入った数百人分の病理組織標本が医療廃棄物として適正処理されずに流出。リサイクル会社が回収した資源ごみに混入した。
６月	八戸市立市民病院（青森県八戸市） 心臓疾患の患者約 50 人の病状などを、患者の同意を得ずに病院ホームページに掲載
４月	済生会宇都宮病院（宇都宮市） 市内のごみ収集所で、患者の氏名や病歴が記されたレセプトの下書き約 150 人分が見つかった。自宅に持ち帰った職員がごみと一緒に処理
	鳥取県立厚生病院（鳥取市） 患者名を記した封筒にエックス線フィルムを入れたまま産廃処分業者に渡していた。同業者がトラックで搬送中、荷台から約 400 枚が落下して発覚
３月	奈良県立三室病院（奈良県三郷町） 約 7,500 人分の患者らの個人データが入った病院のパソコン５台が盗難
	国立病院機構釜石病院（岩手県釜石市） 病院はデータシステムの保守を委託する企業が約3,000人分の患者データを保存するパソコンを紛失
	金沢医科大学病院（金沢市） 病院勤務の医師８人が自分のＩＤとパスワードを医学生に教え、電子カルテを自由に閲覧させた
２００３年 ８月	高知県立安芸病院（高知県安芸市） 患者の病名等約240人分の情報がネット上に流出。薬剤師が自身のホームページに掲載。告知を受けていないがん患者の情報が数十人分含まれていた
６月	松阪市民病院（三重県松阪市） 約１５人分の患者の病名や職員約 400 人分の給与額などが記載された内部文書が流出

（2）個人情報保護法制定の背景

個人情報の取り扱いに関する社会的関心が高まっているなか、消費者すなわち患者の意識は向上し、事業者において個人情報が適切に取り扱われているか否かというポイントは、消費者等が事業者を選択するための「基準」になりつつあるといえます。

また、大量の個人情報を取り扱う企業等、あるいはよりセンシティブな性格を有する情報を扱う企業等においては、万が一の場合のリスク回避のために予め取り組みを始めているケースが多いのも事実です。

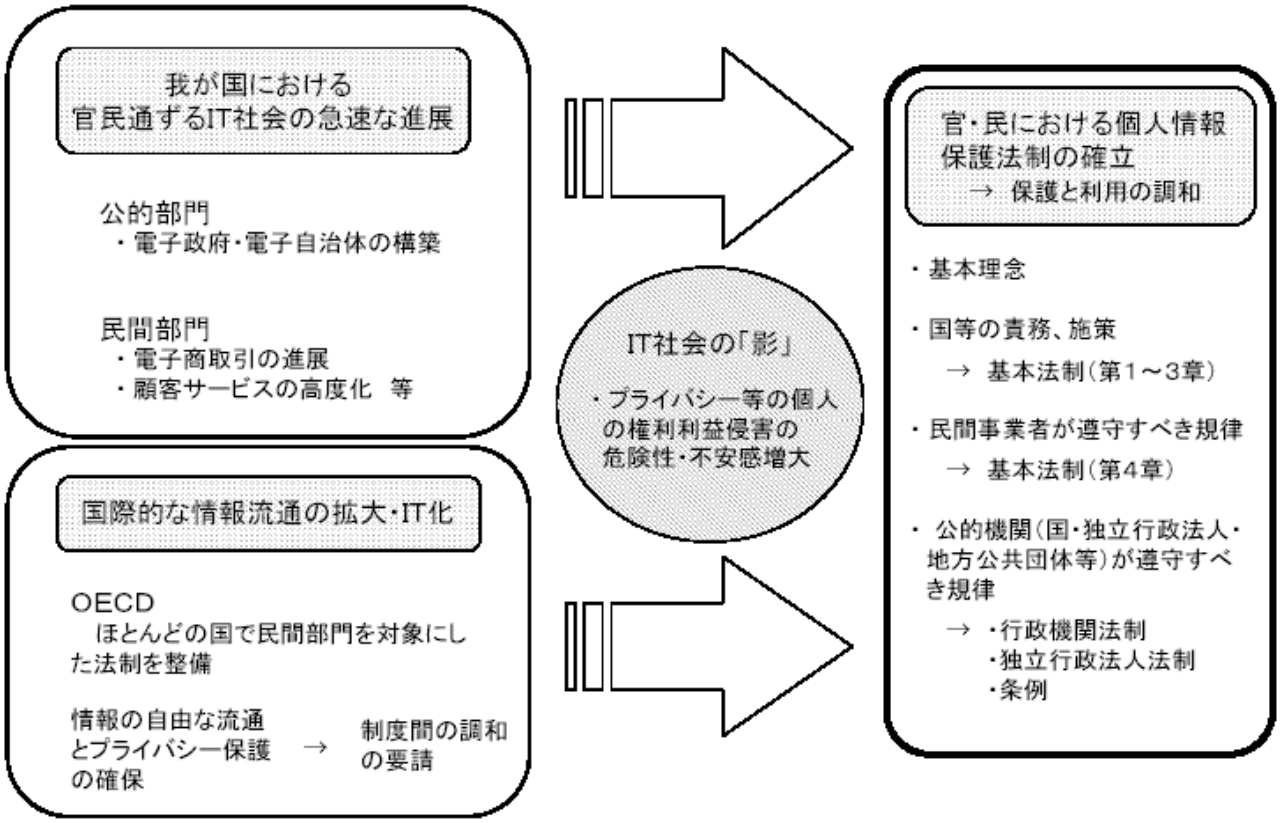
一方で、一般企業等における個人情報漏えいによる大きなリスクの事例が相次いで報道されました。

○企業等の個人情報漏えい事例

業種	内容
コンビニエンスストア	会員データ 18 万件の流出が判明し、顧客に対する補償として 1 億 8,000 万円以上を支出
地方自治体	住民基本台帳データ 21 万件が漏えい。一人当たり賠償額 1 万 5,000 円（うち弁護士費用 5,000 円）の支払いを命ずる判決
インターネット接続サービス	加入会員約 450 万件の個人情報が流出、謝金として一人当たり 500 円相当の金券送付のため 12 億円以上（既存加入者分のみで）を支出

こうした不祥事が相次いで起こる背景には、近年、ユビキタス社会の進展によって様々な個人情報を含むデータが常時大量に収集し処理され、利用されているという時代の流れと、これを取り扱う事業者側の意識のギャップがあるのかもしれません。

○個人情報保護法制整備への流れ



「個人情報保護法」の精神は、あくまでも個人情報の「有効利用」と「保護」にあります。有効に利用するためには、適切な個人情報の取り扱いが不可欠であるという考え方に基づいているのです。

昨今の個人情報の目的外利用や情報漏えいといった、情報セキュリティ面のリスクの増大に対して社会の関心が高まっています。この分野で一旦事故を起こせば直接的、間接的に、事業者は多大なダメージを受けることになります。

さらに、医療機関の場合は、基本的な個人情報に加えて、カルテなど機密性が高く極めてセンシティブな個人情報を扱っているため、万が一情報流出という事態が生じた場合、前述のような事件とは比較にならないほど大きな社会問題に発展しかねません。

では、世界的に個人情報保護への動きが活発化し、その各国で取り組みが行われるようになったのは、どのような背景があるのでしょうか。

○主たる国際的な動き

1970 年代	各国が独自に個人情報保護に関する法律を定める
1985 年	OECD にて個人情報保護のガイドライン「OECD８原則」が定められる
1990 年	EU 指令 ⇒ 個人情報が保護されない第三国への個人情報移転禁止
2001 年	米国にて Safe Harbor 原則の制定
2005 年	日本にて 個人情報保護法の完全施行

1970 年代以降、IT の進展によって大量の個人情報が処理されるようになると、欧州各国と米国で個人情報を保護する法律が制定されました。しかしながら、法律やガイドラインが国ごとに異なると、国際ビジネス上の問題の発生が推測されるため、1980 年に OECD（経済協力開発機構）は、各国の個人情報保護レベルを一定にするためのガイドラインを制定しました。このときに定められた個人情報取扱の原則を「OECD８原則」といいます。この８原則を基本として日本や諸外国の法律等が作られています。

1995 年になると、欧州議会は「個人データ処理に係わる個人情報保護及び当該データの自由な移動に関する欧州議会及び理事会の指令」（いわゆるＥＵ指令）を発令します。これはＥＵ各国に法的強制力を持ち、「第三国が十分なレベルの保護を保証しない場合は EU 域外への個人情報の移転を禁止する」という内容が含まれたものです。このため世界各国が早急な対応が求められました。

2001 年、アメリカでは EU 指令に対応するため Safe Harbor 原則を EU と合意しました。Safe Harbor 原則は、OECD８原則を基にしたもので、EU と取引をする企業は Safe Harbor の原則を遵守しなければならないというものです。

そしてわが国では個人情報保護法を制定し、2005 年４月の全面施行によって対応を図ろうとしているのです。

2　個人情報取扱事業者が負う義務と責任

個人情報保護法は、私人間における個人情報の取得・利用のルールを詳細に規定しており、これらのルールに違反し、行政庁の指導・勧告等に従わなかった場合の罰則も定められ、最終的に刑罰が科せられることになっています。

つまり、個人情報を保護するため、従来公務員の守秘義務違反という罰則は存在したものの、損害賠償で解決を図るしかなかった私人間の情報保護に関して、法の制定・施行により重要な行政的規範、刑罰法規として定められたということです。

個人情報保護法は６章構成になっており、2003 年５月の発布時点では「国及び地方公共団体の責務」などについて述べられた１章から３章までが施行となりました。事業者に直接関わる第４章（個人情報取扱事業者の義務等）は２年間の施行猶予期間が設けられ、この間に個人情報取扱事業者は個人情報保護体制を確立することが求められており、2005 年４月１日より完全施行されました。

(1) 事業者が負う義務

個人情報保護法の考え方は、「ＯＥＣＤ８原則」にその根源があります。これら各原則に対応して、個人情報取扱事業者（過去６ヶ月以内のいずれの日においても 5,000 件以上の個人情報を扱う事業者）の義務が定められています。

○ **ＯＥＣＤ８原則**

１.収集制限の原則
同意を得た個人データのみに限定
２.データの正確性の原則
正確、完全かつ最新のものに保つ
３.目的明確化の原則
データの利用目的は収集時に定められる
４.利用制限の原則
明確化された目的のみのために利用される
５.安全保護の原則
合理的な安全保護措置によって保護される
６.公開の原則
個人情報に関連した開発、慣行、ポリシーおよび連絡先情報を公開
７.個人参加の原則
個人の情報を修正、削除、訂正する権利は本人にある
８.責任の原則
上記諸原則を実施するための措置に従う責任を有する

前述の原則をもとに個人情報取扱事業者には様々な義務が課せられますが、「１.利用目的の特定・公表」「２.適正管理、利用、第三者への提供」「３.本人の権利と関与」「４.本人の権利への対応」 「５.苦情の処理」の５つのカテゴリーに大別することができます。

○個人情報取扱事業者の義務

個人情報保護法	
第１５条	利用目的の特定
第１６条	目的外利用の禁止
第１７条	不正取得禁止
第１８条	取得時の利用目的公表義務
第１９条	正確かつ最新内容の保持義務
第２０条	安全管理措置義務
第２１条	従業者監督義務
第２２条	委託先監督義務
第２３条	第三者提供の禁止
第２４条	利用目的等の備置義務
第２５条	保有個人データ開示義務
第２６条	訂正等義務
第２７条	利用停止等義務
第２８条～第３０条	２４～２７条の理由説明・手続・手数料
第３１条	苦情の処理義務（適切・迅速）

(2) 責任と罰則

個人情報保護法第６章においては個人情報取扱事業者の罰則について定めがあります。前項記載の表からも明らかなように、「情報の漏洩をしてはいけない」という義務は規定されていません。よって、仮にこれらの義務に反した場合にでも直ちに罰則に至るものではなく、次のような指導・勧告プロセスが定められています。

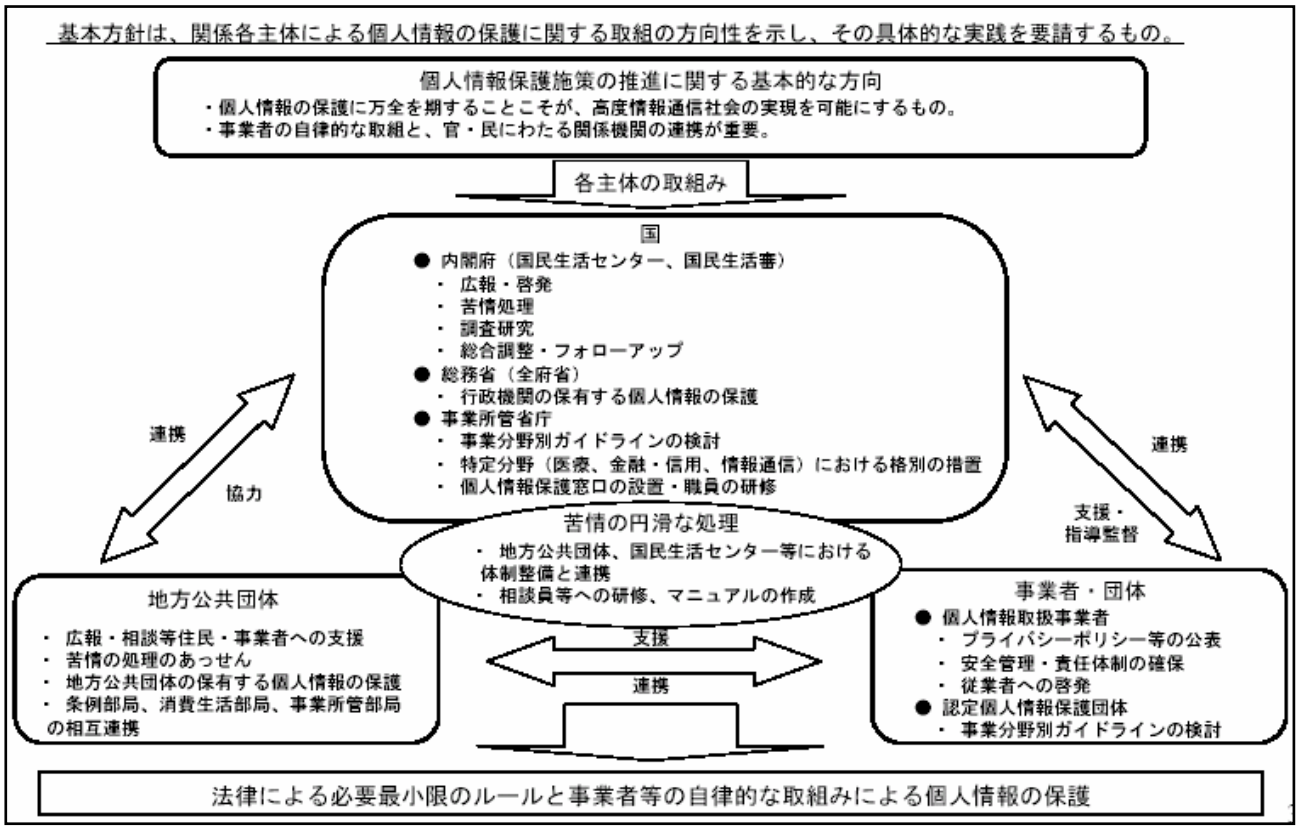
＊　報告義務違反（怠慢・虚偽）　　30 万円以下の罰金

①改善勧告　　違反行為の中止その他是正措置の勧告
　↓　正当理由なく従わないため、重大な権利利益侵害の切迫
②改善命令　　違反行為の中止その他必要な是正措置命令発令
　↓　命令に応じない
③刑　　罰
　６ヶ月以下の懲役または 30 万円以下の罰金

また、前述の勧告・命令をなすのは、条文上の規定から監督官庁の主務大臣すなわち医療機関の場合は厚生労働大臣になりますが、その権限は現在のところ、都道府県知事に委任されています。よって、各知事が改善勧告や命令を出さなければならない対象としての個人情報取扱業務者たる医療機関は相当数に上ることは想像に難くありません。これはすなわち、「改善勧告」「改善命令」を受ける可能性は、顧客・消費者からのクレームや内部告発などにきっかけを頼らざるを得ないという要素も含めると、そう高い確率ではないといえるでしょう。

この点から、医療機関の経営幹部にとって重要なのは、「個人情報保護法に定められる刑罰対策」よりも「医療機関経営のコンプライアンス策定」ということになります。個人情報取扱事業者としての義務を果たさないばかりか、これを放置するようなことはコンプライアンスに反する行為だといえます。

一方で、病院生き残りのためには、個人情報保護法に則った経営を実践し、社会・患者の信頼獲得、および他院との差別化を図ることが戦略的に重要課題であると捉える必要があります。



3　医療機関に予想される具体的影響

個人情報保護法の 2005 年４月全面施行を受けて、繊細な情報を扱う医療機関においては、それぞれ人、場所、ネットワーク上の安全対策という３つの問題について早急なシステム構築が求められています。

これら安全管理措置の具体的基準は、法の条文上に示されていないため、個人データの重要性、脅威の程度とこれに対する脆弱性を鑑み、その内容と性質および利用方法に照らして、「保護」と「利用」のバランスを図りながら必要性を判断することが重要であるといえます。

(1) 適用される事業者の範囲

個人情報保護法第２条３項において、「個人情報取扱事業者」とは、「個人情報データベース等を事業の用に供している者」と規定されています。この詳細な定義は、「個人情報の保護に関する法律施行令（政令第 507 号)」に定めがあります。

すなわち、条文解釈上では

> ①個人情報データベース等を構成する個人情報によって識別される特定の個人の数若しくは電話番号のみが含まれる情報を編集し、又は加工することなくその事業に用に供する事業者
> ②当該個人情報データベース等の全部又は一部を構成する個人情報によって識別される特定の個人の数を除いた合計が過去６ケ月以内のいずれの日においても、5,000 件（電話帳、カーナビ掲載分を除く）を超えるもの

と規定されます。

個人情報取扱件数 5,000 件未満の場合（いわゆる小規模事業者）には、取り扱う個人情報の量および利用方法からみて、個人の権利利益を害するおそれが少ないとして除外されています。

○「5,000 件以上」の意義

電話帳データや、カーナビゲーションや市販の住所地図（オプトアウト）などを、加工せずそのまま利用する場合は、個人データとして考える必要はなく、5,000 件の内には含まないものとしています。

ただし、これらのデータを抜き出し、新たな情報を追加するなどして、データベースを構築した場合には、件数に含めなければなりません。また、これらによって個人情報を取得した場合は「通知」や「公表」、「本人同意」を含む個人情報としての一連の措置が必要になります。

また、６ヶ月以内に削除するデータは「一過性の利用」のためのデータとして考え、同様に 5,000 件のカウントには含みません。

⇒　厚生労働省ガイドライン（詳細次章）によって、医療・介護事業者に対し、法令上の義務を負わない小規模事業者にもこれを遵守する努力を求めています。

（2）対象となる個人情報

○「個人情報」の定義

個人の氏名、住所、生年月日、電話番号はもちろん個人情報ですが、防犯カメラに記録された情報や音声であっても本人を識別できるものであれば個人情報となります。
また、数字と記号からなるメールアドレスやIDなど、それ自体では本人を特定できなくても、他の情報と照合することによって容易に特定の個人を識別することができれば個人情報となります。

例えば、第三者にとっては個人を特定できないID（患者・カルテ番号等）であっても、院内にIDと住所･氏名が対応づけられた情報がある場合、そのIDは個人情報となります。

○体系的に整理されている状態（個人情報データ・個人情報データベース）

個人情報が含まれる情報の集まりで、検索可能な状態になっているものは「個人情報データベース」と定義され、これを「体系的に整理されている」状態といいます。

住所･氏名がIDで検索できるようなデータベースは当然のことながら個人情報データベースですが、取引経過が記録されているログ情報ファイルも個人情報データベースです。紙ベースの住所録や名刺であっても、個人や部門で適当に保管してある状態では対象外ですが、５０音順に並べられ、他の人も利用できる状態であれば個人情報データベースとなります。名簿業者等に販売できる状態になっているからです。

⇒　医療機関では、次のようなものが該当します。

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

4　厚生労働省ガイドラインの分析
～　医療機関がなすべき主な取り組み

個人情報保護法の 2005 年４月完全施行に向け、厚生労働省「医療機関等における個人情報のあり方における検討会」は、2004 年 12 月 24 日「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」を公表しました。

今後も個別法の制定も視野に入れた議論が続けられることになっておりますが、このガイドラインに準拠して、各医療機関では自院の取り組み方法を具体的に示すプライバシーポリシーを作成し、これを公開することが求められています。

まずは、ガイドライン内容を十分に吟味し、院内でなすべき取り組みを決定する必要があります。

（1）基本方針と特徴

ガイドラインの特徴は、次の３点です。

①取扱情報 5,000 件以下の医療機関に対しても患者情報保護を求める
→　個人情報保護法（以下「法」という。）では「個人情報取扱事業者」の対象外とされる小規模事業者たる診療所に対しても、医療情報が有する高い機密性を理由として患者情報保護を要請している

②死亡患者の個人情報も保護対象として明記
→　生存者の個人情報に限定する法規定を加重し、死と向かい合う機会の多い医療現場では、死亡患者情報も保護対象とする

③保護と利用のバランスを具体的に明示
→　法第１条の規定する「個人情報の有用性に配慮」の趣旨の例外として、本人の同意にかかわらず高い公益性から医療の特殊性を考慮した「利用」の重視を明記

（2）行政が求める方向性と考え方

「医療機関等における個人情報保護のあり方に関する検討会」の協議に従って、厚生労働省は、個別の法制化に向けた議論を再開しました。

わかりやすさ、患者・職員に対する説明の容易化の観点からは、法制化に向けて前向きな意見も多いものの、法的義務の具体的内容を明示したガイドラインの公表に加えて、さらに別の法律を加える必要性に関する疑問を払拭するには至らず、個別法制化は見送られる

公算が大きいと見られています。

しかし、これらの整備を前提に、①医療情報にはより手厚い法的安全管理措置が必要か、②患者（遺族を含む）が自己情報をコントロール可能とする特別な法的措置が必要か、という２点を焦点にした議論が継続されており、今後の行政対応には留意が必要です。

医療機関における個人情報の取り扱いに係る課題としてガイドラインが指摘するのは、

① 安全管理
② 自己情報コントロール
③ 死者の情報の取扱い

の各問題です。

とりわけ②については、診療録等の開示問題と関連して、法の趣旨である個人情報の有効活用の概念にのっとり、その妥当性の評価基準の策定が困難であることは想像に難くありません。
「診療情報の提供に関する指針」によれば、インフォームド・コンセントの理念等を踏まえ、医療従事者・患者間の良好な関係構築に向けた信頼関係構築に基づく診療情報提供の取り組みがうたわれているところですが、同指針の内容に配慮した開示方法の策定が求められていると考えられます。

また、厚生労働省は、ガイドラインに加えてＦＡＱ（一問一答）を作成する方針を打ち出しています。その具体的内容としては、相談窓口機能のあり方や本人同意を得る方法、委託業者に対する留意事項、あるいはプライバシーポリシーの院内掲示方法等、想定される問答集であり、ガイドラインの下に位置づけられるものとなります。

（3）医療機関がなすべき具体的対応策

個人情報保護法において、医療機関が個人情報保護のため果たす義務として最初に明記されているのは、措置の透明性の確保と対外的な明確化です（同法第３条）。
つまり、個人の人格尊重の理念の下に個人情報を慎重に扱うべきことが指摘されているほか、関係法令およびガイドラインを遵守すること等、さらに同法に定める事項を具体的に規定している「個人情報の取扱に関する規則（以下「個人情報取扱規則」）という。」においては、個人情報に係る安全管理措置の概要、本人等からの開示等の手続、第三者提供の取扱、苦情等への対応等について、具体的に定めることが必要となるものと考えられます。

利用目的等を院内掲示・ホームページ上に掲載するという手段で広く公表することについては、

> ①個人情報が利用される意義について患者等の理解を得ること
> ②医療機関・医療関係事業者において、法を遵守し、個人情報保護のため積極的に取り組んでいる姿勢を対外的に明らかにすること

というふたつの趣旨があることに留意しなければなりません。

以下には、ガイドラインが求める個別の対応ポイントを解説します。

①個人情報の匿名化

患者の個人情報から、当該情報に含まれる氏名、生年月日、住所等の個人を識別する情報を取り除くことにより、特定の個人を識別できないよう留意する必要があります。顔写真については、一般的には目の部分にマスキングする等の措置、また必要な場合には、当該個人と無関係の符号または番号を付す等の措置も検討されるべきです。

しかしこの場合、院内で得られる他の情報や付された符号または番号と、個人情報との対応表と照合することで特定の患者が識別される可能性も否定できません。匿名化にあたっては、当該情報の利用目的や利用者等を勘案した処理を行う必要があり、併せて本人の同意を得る等の対応を考慮する必要があります。

例えば、特定の患者の症例を学会発表もしくは学会誌に報告する場合等では、一般的には氏名、生年月日、住所等を消去することで匿名化されると考えられますが、症例により十分な匿名化が困難な場合は本人の同意を得なければならないことになります。

②本人の同意

個人情報を目的外に利用する、あるいは第三者に提供する場合、法は原則として本人の同意を要求しています。つまり、医療機関において通常必要と考えられる個人情報の利用範囲を施設内への掲示によって明らかにしておき、患者側から特段明確な反対・留保の意思表示がない場合には、これらの範囲内での個人情報の利用について同意が得られているものと解されます。

また、意識不明ではないものの、患者の意識レベルにより本人の意思を明確に確認できない状態の場合については、意識の回復に合わせて、速やかに本人への説明を行い、同意を得ることが必要になります。

これらの場合においては、患者の理解力、判断力などに応じて、可能な限り患者本人に通知し、同意を得るよう努めることが重要です。

③家族等への説明

病態によっては、治療等を進めるにあたり本人だけではなく家族等の同意を得る必要があると判断される場合もあります。本人以外の者に病状説明を行う場合には、本人に対して、あらかじめ病状説明を行う家族等の対象者を確認し、同意を得ることが望ましいといえます。この際に本人から申出がある場合には、治療の実施等に支障の生じない範囲において、現実に患者の世話をしている親族及びこれに準ずる者を、説明を行う対象に加える、また家族のうち特定者を限定すること等の取り扱いとすることもできます。

一方で、意識不明の患者の病状や重度の痴呆症の高齢者の状況を家族等に説明する場合は、本人の同意を得ずに第三者提供できるケースに該当しますが、この場合、医療機関において本人の家族等であることを確認した上で、治療等を行うにあたり必要な範囲で情報提供を行うとともに、本人の過去の病歴、治療歴等について情報を取得します。

その後、本人の意識が回復した際には、提供および取得した個人情報の内容とその相手について本人に説明するとともに、本人より申出があった場合には取得した個人情報内容の訂正等、および病状の説明を行う家族等の対象者の変更等を行うこととなります。

ここで、患者の判断能力に疑義がある場合には、意識不明の患者と同様の対応を行うとともに、判断能力の回復に合わせて速やかに本人への説明を実施し、同意を得るものとします。

5　個人情報保護体制構築のポイント

（1）医療機関内へ向けた取り組み

厚生労働省ガイドラインが医療機関に対して求めるものは、具体的には、次のような事項への取り組みです。

①プライバシーポリシーの策定
②安全管理者の設定等の体制整備
③個人情報取扱規程･マニュアルの策定
④職員に対する研修
⑤情報システムに関するセキュリティ評価の実施

ガイドラインに定める「利用目的の公表」としての院内掲示のため、この前提としてプライバシーポリシー策定も不可欠な取り組みとなります。

上記事項のうち、取り組み・運用が困難なものと考えられるのは、職員の監督義務に基づく研修等だと考えられます。

具体的には、基本的な保護体制内容のレクチャーおよび意識向上を図る目的の研修の他、技術面としてのセキュリティ等の整備、医療機関内規定の整備、労働契約内容等の整備、内部監査、事故発生時における適正な懲戒処分等の検討などが挙げられます。

（2）対外的に求められる取り組み

ガイドラインを遵守することにより、医療機関が入手した個人情報について適切な管理と運用がなされていることを、患者やその家族および潜在的患者を含む社会に対して明確にし、情報管理に関わる不安を取り除き、信頼を得るためには次のような取り組みが求められます。

この中には、従来行われてきた措置である委託先の監督強化も含まれます。

①責任体制の明確化
②患者等問い合わせ窓口機能の設置
③利用目的等の公表（院内掲示･ＨＰ上掲載）
④委託先の監督

○第三者認証取得の活用

第三者による認証取得は、組織が適正な個人情報保護体制や情報セキュリティ体制を構築していることを顧客に積極的にアピールするために適当な方法だといえます。

自院の一方的なアピールだけでなく、第三者から認証を取得したという事実をアピールすることで、社会的な安心、信頼を得ることができます。

現在、個人情報保護関連、情報セキュリティ関連の第三者認証として広く知られているものには、プライバシーマーク、ＴＲＵＳＴｅ、ＩＳＭＳ等があります。

○プライバシーマーク

事業者が JIS Q15001 を基準に個人情報保護法の遵守体制を構築していることに対する認証制度
コンプライアンス・プログラムに基づくマネジメントシステムが確立されていることの証です。

＊JIS Q 15001 ：1999 年に制定された JIS 規格
日本における個人情報保護マネジメントシステムのスタンダードになっていると同時に、プライバシーマークの認証基準
個人情報保護方針を定め、Plan（計画）、Do（実施運用）、Check（監査）、Action（事業者の代表者による見直し）というマネジメントサイクルを回すことで管理レベルをスパイラル状に向上させていく仕組み

○ＴＲＵＳＴｅ

米国のプライバシー保護第三者認証制度
多くの米国企業が認証取得しており、漏えい保険や苦情処理の機構等に独自の仕組みをもっています。

○ＩＳＭＳ

情報セキュリティに重点を置いた基準
災害対策、犯罪対策といった物理的セキュリティ対策や、システムやネットワークなどの技術的セキュリティ対策など、データを安全かつ正確な状態に保つことに重点を置いています。

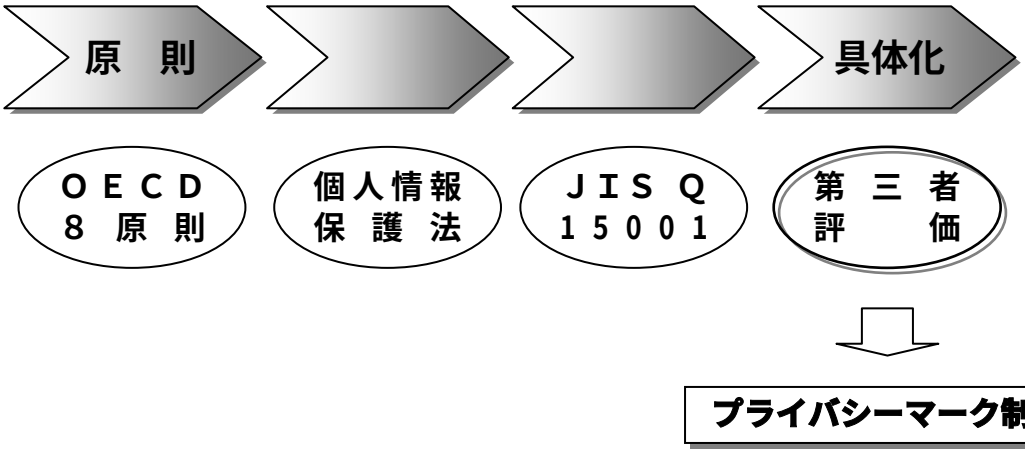
最も重要なのは、組織内における個人情報保護体制を、法に基づいてあるいは JIS Q15001 に基づいて一定水準で構築することであって、第三者認証はその先にあるインセンティブだと理解すべきだということです。

第三者認証取得ありきの個人情報保護体制構築ではなく、実質的に機能し有効な個人情報保護ガバナンス・プロセスの確立に向けた取り組みが求められます。

6　プライバシーマーク制度の概要

（1）制度の概要、認定取得基準、必要性

○個人情報保護の体系



○制度概要

プライバシーマーク制度とは
個人情報取扱事業者に対して、個人情報保護を実践している証として「プライバシーマーク」の使用を認める制度

プライバシーマークの認定にあたっては、個人情報保護のための JIS 規格（JIS Q 15001：1999）に準拠した コンプライアンス・プログラム（CP）に基づいた運用が行われているかについて、 第三者認証機関である財団法人日本情報処理開発協会（JIPDEC)、 またはその指定機関が評価および審査を行います。

つまり、プライバシーマークを使用することができる事業者とは、JIS Q 15001 に基づいた個人情報保護のマネジメントシステムを持ち、それを運用していると認められた事業者なのです。

○付与されるプライバシーマーク

有効期限　　２年
以降　２年毎更新

登録番号
６桁+(２桁)の数字

○プライバシーマークの必要性

個人情報保護法は、情報保護の観点から見ると、個人情報保護の基本レベルの義務内容しか記述されていません。個人情報保護法の全面施行に伴い、社会の関心と消費者の意識が更に高まることから、個人情報を持つ事業者は個人情報保護法への対応に加えて、プライバシーマークなどの個人情報保護や情報セキュリティ分野の第三者認証取得への取り組みが必要となると考えられます。

プライバシーマークは、民間事業者が積極的に推進する自主的な規制、努力にインセンティブを与え、わが国における個人情報保護を一層促進させるための手段です。これにより情報主体である個人は、プライバシーマークによって民間事業者、すなわち医療機関における患者は、個人情報の取扱いが適切であることを容易に判断することが可能となり、医療機関としても積極的な取り組みを展開して、情報保護体制構築をアピールすることにより、他院との差別化を図ることができます。

（2）取得により期待できる効果

○メリット、デメリット

メリット
- **国民（患者、潜在的患者）からの信頼**
- **委託元からの信頼**

デメリット
- **人的、物的リソースの確保**
- **コンサルタント、管理コスト、専任の担当者、入退室管理システム、セキュリティ対策ソフト導入等コスト**
- **社会的評価基準の厳格化**
- **漏えい事故による社会的信用の失墜**

（3）取得のために必要な取り組み

○取得に当たっての検討事項

・プライバシーマークを取得する目的　⇒　十分な認知
・取得スケジュール　⇒　現状業務の見直しを前提
・取得のための体制と取得後の運営体制　⇒　組織、技術、人的、物理的各問題
・コンサルティング企業の活用　⇒　コストとメリットのバランス

○新たに取り組みが必要な業務

・コンプライアンス・プログラム（ＣＰ）の策定

【医療機関におけるＣＰ策定のポイント】

- **個人情報の特定とリスク分析**
- **患者からの同意の取り方**
  - **時期(初診時等)**
  - **同意の範囲（診療、保険、研究等）**
  - **方法(チェック、サイン等)**
  - **例外時の扱い(救急等)**
- **部門別取扱い**
  - **各診療科、病棟看護部、ナースステーション、病室、医局**
  - **リハビリテーション科、放射線科、栄養科、薬剤科**
  - **臨床検査科（外注検査）**
  - **事務課、医事課**
  - **診療相談室、診療情報管理室、地域医療推進室**
- **開示、苦情及び相談**
  - **開示の範囲、条件、費用、手続**

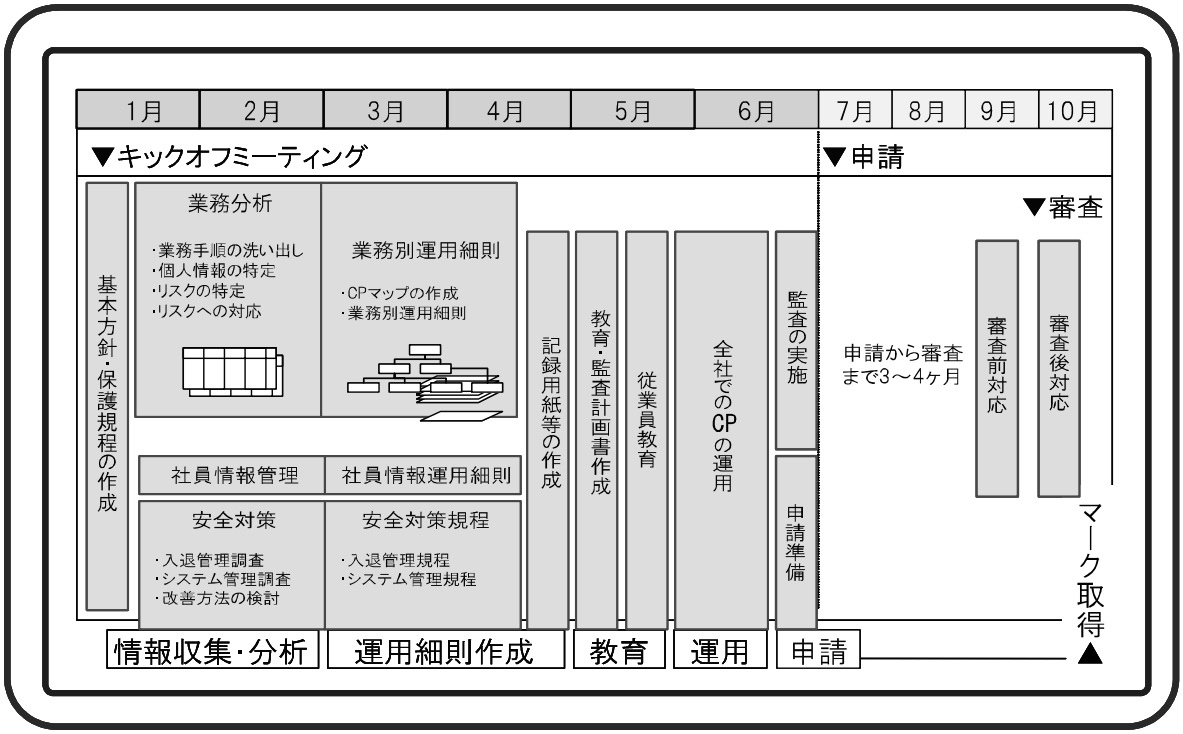
○付与の条件

付与認定基準に合格することが条件となっています（下記は具体例）

- **通産省の個人情報保護ガイドライン又は業界ガイドラインに準じた C/P(実践順守計画) を定めている**
- **C/P に基づいて個人情報の管理が適切に実施されている**
- **個人情報を適切に取り扱う体制が整備されている**
- **個人情報の管理者が指名されている**
- **企業外部への個人情報の提供、取扱いの委託を行う際には、 責任分担・や守秘に係る契約を締結する等、個人情報について適切な保護が講じられるよう措置されている**
- **年１回以上、個人情報の機密保持に係る周知徹底の措置を講じている**
- **年１回以上、事業者内部の個人情報の保護の状況を監査する**
- **個人情報保護に関する相談窓口が常設されている**

7　プライバシーマーク取得モデル

○標準的スケジュール例



○取得までの流れ

１．取得方針の決定

プライバシーマークを取得する目的の明確化
会社としての個人情報保護に対する姿勢の明確化
取得体制・取得スケジュールの決定

２．コンプライアンス・プログラム（ＣＰ）の策定

会社が取り扱う個人情報の取り扱い方法の決定
入退室管理など物理的なセキュリティ確保
ウィルス対策・アクセス制御などネットワークセキュリティの確保
監査・教育などマネジメントシステム運用のための計画立

３．運用開始

従業員教育の実施
ＣＰに基づいた個人情報保護の実施
監査の実施
監査の結果に基づく運用の見直しとＣＰの見直し

４．プライバシーマーク付与申請

プライバシーマーク付与機関あるいは付与指定機関による審査
審査における指摘事項への対応

５．プライバシーマークの付与

プライバシーマークの使用開始