参考資料２

個人情報保護に関するコンプライアンス・プログラム

(JIS Q 15001)

医療機関の認定指針

Ver. 1.02

2002年10月

(財) 日本情報処理開発協会

はじめに

1）指針作成の背景

個人情報をコンピュータに蓄積し、ネットワークを通じて交換するネットワーク社会では、さまざまな媒体やネットワークサービスなどを通じて多くの個人情報が拡散することや、不正に入手した個人情報が悪用されることなど、従来にないプライバシーの侵害が行われることが想定される。

わが国の民間部門における個人情報の保護については、従来から自主的な規制によって対応してきた。その根拠として、行政機関が独自に定めた、いわゆる個人情報保護ガイドラインを基準としてきた。例えば、経済産業省が 1997 年 3 月に改訂して制定した「民間部門における電子計算機処理に係る個人情報保護に関するガイドライン」が代表的なものである。

自主基準を一段と推進する必要から、あらゆる産業分野に適用する国内基準として、1999 年 3 月にこれらのガイドラインをベースとした日本工業規格「個人情報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）が制定された。当該 JIS には、この利用方法として、機関が自己の個人情報保護の取組みが JIS に適合していることを自ら評価するために用いることができるとともに、第三者による評価の基準としても活用できることが記述されている。このことから、1998 年 4 月から既にスタートしていた「プライバシーマーク制度」が、JIS を基準とした第三者認証制度として本格的に運用を開始した。

プライバシーマーク制度は、JIS Q 15001 に基づいた個人情報の適切な保護のための体制を整備している事業者に対し、その申請に基づいて、審査を行い、認定の旨を示すプライバシーマークの付与を行う制度である。

医療においても電子カルテやレセ電算システムの普及により患者や医療関係者の利便性が拡大する反面、医療機関のコンピュータに蓄積されている患者情報の漏えいによってプライバシー侵害のリスクが大きくなる。こうしたことから医療機関においてもプライバシーマーク制度の導入が期待されている。

JIS Q 15001 は、あらゆる産業分野に適用することが可能であるが、そのために産業分野に偏らない内容となっている。一方、分野によっては個人情報の取扱いにおいて、その産業独自の慣行等特殊な事情があることから、JIS Q 15001 の適用においてはその分野の特殊性を勘案しなければならない。特に、個人情報の取扱いが複雑で多岐にわたっている医療関連機関においては、この傾向が強い。そのため、医療分野の個人情報保護の推進を加速させることを目的として、JIS Q 15001 の適用を容易にする必要から、医療分野の専門家による「医療機関の認定指針検討 WG」を設定して、医療分野に JIS を適用する際の指針となる解説書を作成することとした。

2）指針の構成

指針はJIS Q 15001の項目番号と項目名ごとに下記の構成になっている。

A．JIS Q 15001の要求事項

JIS Q 15001の要求事項を原文通りに記載し、四角の枠で囲んでいる。

B．医療機関としての解釈

医療機関にJIS Q 15001を適用する場合の要求事項の解釈を記載している。

C．最低限のガイドライン

最低限実施しなくてはならない方策の指針を記載している。

D．推奨されるガイドライン

最低限のガイドラインに医療機関の実情を配慮し、追加した方が望ましい方策を含めた指針を記載している。

3）医療機関のプライバシーマーク取得の概要

医療機関がプライバシーマークを取得するには、JIS Q 15001に基づき、医療機関が保有する個人情報を保護する為の方針、組織、計画、実施、監査、及び見直しを含むマネジメントシステムを構築・運用して申請する。

具体的な内容は、医療機関で取り扱う診療録、処方伝票、検査依頼伝票、検査結果報告書、看護記録、レセプト等の個人情報を含む保護対象を抽出し、リスク分析を行い、患者からその利用目的の同意をとり、目的に添って診療情報の収集をおこない、適切なセキュリティの管理のもとに同意の範囲内で利用をおこなう。さらに教育，監査、苦情処理窓口の設置、及び幹部によるフォローにより継続的実施と是正を行う。こうしたことが適切に運用されるように規程化する。単に審査の時点で要求された水準を満足していることのみではなく、個人情報保護マネジメントが継続して実施されるか否かも重要な審査ポイントである。

1980年のOECDプライバシー・ガイドラインの採択により、プライバシーの概念はそれまでの「一人にしておかれる権利」から「自己に関する情報の流れを自身でコントロールする権利」となった。従来、医療機関でプライバシーというと前者で捕らえられることが多く、一人部屋にすべきとか、中待合室で前の患者さんの診察内容が聞こえないようにすべき等に注意が行きがちであったが、新しい個人情報保護の概念では、さらに個人情報を患者の同意に基づいた利用目的にそって活用していくこと、逆に同意の取れない利用目的には使用しないことが要求される。

すなわち、個人情報保護を行うということは、患者情報が外部にもれないようにするため、できるだけ使用しないように消極的に管理することではなく、活用を望む患者さんのデータは、その同意した利用目的や利用者の範囲が守られるように安全に管理し、同意に基づいた適切な活用を可能にすることである。

こうした個人情報保護のための活動は、医療情報の開示、医療の透明化を支援し、患者さんからの信頼を高め、患者さんが主体的に診療に参加する、開かれた医療を実現するために、必要

であり、かつ重要な活動であると考えられる。

4)指針検討WGの委員

＜主査＞

大阪医科大学　病院情報部　助教授	山本　隆一

＜委員＞

労働福祉事業団　関西労災病院　医療情報部	
部長	清谷　哲朗
神戸大学　医療情報部　　教授	坂本　憲広
ベリングポイント(株)　ディレクター	豊田　　建
(財)医療情報システム開発センター　研究開発部	
主任研究委員	相澤　直行
(財)医療情報システム開発センター　普及調査部	
課長	武隈　良治

＜事務局＞

日本情報処理開発協会情報セキュリティ対策室	
プライバシーマーク事務局　事務局長	関本　　貢
日本情報処理開発協会情報セキュリティ対策室	
プライバシーマーク事務局　主席研究員	喜多　紘一

1．適用範囲

A．JIS Q 15001の要求事項

この規格は、個人情報の全部もしくは一部を電子計算機などの自動処理システムによって処理している、又は自動処理システムによる処理を行うことを目的として書面などによって処理している、あらゆる種類、規模の事業者に適用できる。

B．医療機関としての解釈

医療機関においては、診療録等が書面であっても、その情報を用いて、診療報酬請求や検体検査の外注などを行っている。その際に用いられる個人情報は自動処理システムによって処理されていると考えられる。従って、この規格は、ほとんどの医療機関において適用されると判断される。なお、この規格が適用される個人情報とは、患者情報だけではなく、それぞれの医療機関が雇用する個人に関する個人情報や採用情報も対象としている点について留意する必要がある。ただし、従業員等に関する個人情報の取扱いに関しては、他の業種と大きな違いはないと考えられるので、このガイドラインにおいては医療機関に特有な側面、すなわち患者さんの個人情報に関する取扱いに焦点を絞って解説する。また、看護学校等を併設している場合はその成績情報等を含めた個人情報も管理対象となる。

4．コンプライアンス・プログラム要求事項（「2．引用規格」、「3．定義」省略）

4．1　一般要求事項

A．JIS Q 15001の要求事項

事業者は、コンプライアンス・プログラムを策定し、実施し、維持し、及び改善しなければならない。その要求事項は、この4・全体で規定する。

B．医療機関としての解釈

コンプライアンス・プログラムとは、個人情報を保護するための方針、組織、計画、実施、監査及び見直しを含むマネジメントシステムをいう。すなわち、単に個人情報を保護するための方針を策定すればよいのではなく、それを実現するための組織体制を整え、具体的な計画（Plan）を立て、それを実施（Do）し、その状況を監査（Check）し、監査結果を評価（Assessment）する必要がある。さらに、その評価に基づき、個人情報を保護するための方針をより確実に実現できるように、計画を練り直すという具合に、この P→D→C→A を繰り返すことが要求されている。こうした個人情報保護のためのコンプライアンス・プログラム遵守活動は、医療情報の開示、医療の透明化を支援し、患者さんからの信頼を高め、患者さんが主体的に診療に参加する、開かれた医療を実現するために、必要であり、かつ重要な活動であると考えられる。

4．2　個人情報保護方針

A．JIS Q 15001 の要求事項

事業者の代表者は、次の事項を含む個人情報保護方針を定めるとともに、これを実行し維持しなくてはならない。事業の代表者は、この方針を文書化し、役員及び従業員に周知させるとともに、一般の人が入手可能な措置を講じなくてはならない。

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。

B．医療機関としての解釈

事業の代表者は、医療機関ではその管理者と考えられる。従って、一般的には管理者は院長と考えられ、院長が以下のａ）～ｄ）を含む個人情報保護方針を明確な決意表明の形で策定し、従業員に周知、教育し、遵守させるようにしなければならない。また、この個人情報保護方針は単に院内の規程として周知徹底するだけではなく、書面等に文書化し、さらに、医療機関を受診する患者さんもその内容を知ることができるようにしなければならない。具体的には、医療機関の受付けや診察室に掲示する、診療案内や診察券などに印刷する、診療時に書面を配布し説明する、医療機関のホームページ等で公開する、などの方法が考えられる。

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。

①個人情報の収集

医療機関においては、診察行為が、本来個人情報の収集そのものと考えることができる。従って、医療機関においてコンプライアンス・プログラムを遵守するためには、個々の医療従事者が十分な自覚を持って適切な個人情報の収集に努めなければならない。特に、診療現場においては、患者さんの立場は弱く、また、健康上の問題から自分自身の個人情報保護に十分配慮することができない場面にも頻繁に遭遇するので、これらの点に関して十分な配慮が行われることが期待されている。

②個人情報の利用

また、利用に関しては、診療に関して患者情報を用いるのは当然との意識があるが、どこまでが診療か、どこまでが病院管理かなど、明確な定義が出来ない場合もある。そのため、患者さんの個人情報が何に利用されているのかを具体的に示しておくのが望ましいと考えられる。例えば、「ご家族への病状説明に利用します」、「診療報酬の請求に利用します」など、これまで暗黙の内に当然の利用目的としていたものに関しても、文書化しておけば、患者さんの理解をより得やすくなるであろう。

③個人情報の提供

提供に関しても、同様で、外注検査の際や、専門医の意見を得る際に、個人情報を提供する事があることを明示する必要があると考えられる。

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。

個人情報への不正アクセス、紛失、破壊、改ざん、漏えいなどに関して、物理的セキュリティ（建物や部屋の強度や出入りの制限など）、組織的セキュリティ（管理者やアクセス権限の設定など）、ネットワークセキュリティ（インターネットからのアクセス制限など）、コンピュータセキュリティ（ウィルスの混入防止など）をどのように確保し、予防に努めているのかを示す必要がある。

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。

医療機関においては、患者情報は個人情報保護法だけでなく、医師法及び刑法 134 条などによっても保護されており、これらの規範を遵守するためにも、患者さんの個人情報を保護するように勤めなければならない。

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。

医療機関の代表者は、その個人情報保護方針の中で、コンプライアンス・プログラムを実施し、管理する責任者を定め、どの程度の頻度で監査を行い、コンプライアンス・プログラムの遵守状況を評価し、計画を見直し、改善に努めるかを明確にしなければならない。特に、こうした努力を継続的に行う姿勢が重要である。

4．3　計画

4．3．1　個人情報の特定

A．JIS Q 15001 の要求事項

事業者は自ら保有するすべての個人情報を特定するための手順を確立し、維持しなければならない。事業者は、特定した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、改ざん及び漏えいなど）を認識しなければならない。

B．医療機関としての解釈

（1）保護すべき個人情報の対象及び管理単位

個人情報とは診療録などの文書情報のみならず、医師と患者、医師と看護婦、等の間で交わされる患者に関する会話、病床における名前の表示、面会者への入院患者情報提供、点滴、薬袋などへの名前の表示等も含まれる。個人情報を特定し管理する単位は、管理が有効に働くレベルである必要がある。一般的には、ファイル単位、帳票名単位のレベルでの特定及び管理が良いと思われる。例えば、個人情報管理台帳などによる特定及び管理が考えられる。管理台帳の管理項目としては、個人情報の名称・種類・責任者・使用期間・使用理由・保管場所・アクセス可能者・預託や提供がある場合は相手先・廃棄方法などが

ある。医療機関における個人情報が含まれる書類の例を付録１に示す。

（２）業務の流れにそった個人情報の特定

医療機関においては取り扱う個人情報が部署ごとに異なるというよりは、一人の患者に関連して診療情報等を共有している場合が多い。従って、個人情報を特定、管理するにあたっては、部署毎で行うというよりは医療系（看護系含む）、事務系などで各々責任者等を定め、その責任者を中心としてコンプライアンス・プログラムの開始時、新業務の発生時及び定期的に行うことが望ましい。また、責任者以外の職員も特定作業に漏れがないか意識させることも重要である。特定した個人情報についてのリスクを調査し把握した上で、そのリスクに見合った保護措置を講じる必要がある。

（３）リスク分析

個人情報に関する「原因系リスク」として、不正アクセス、紛失、破壊、改ざん、漏えいなどが代表的である。この原因系リスクが発生した場合の「影響リスク」として、原因究明中の業務中断による損失、患者に対する賠償などの直積的影響及び、社会的信用の喪失や官公庁や報道機関への報告、訴訟への対応など間接的影響などが考えられる。

（４）日常業務としての個人業務の特定手順

個人情報を管理するためには、取り扱っている個人情報すべてについて洗い出しをしておく必要がある。認識されていない個人情報は、紛失あるいは、改ざんされたとしても、検知することが困難だからである。また、取り扱っている情報は経営環境等により変化するため、全ての個人情報を日々の業務活動の中で特定できる手順や仕組みを確立しておく必要がある。

（５）個人情報保護対象の定義

プライバシーマーク制度は個人情報の取扱いについて JIS Q 15001 に準拠したマネジメントシステムが構築されていることを審査するものであり、管理する対象は個人情報となる。したがって、そもそも守らなければならない個人情報をどこまでとするか？という、個人情報の定義、範囲が重要となる。個人情報保護の侵害は人それぞれに考え方の相違があり、一義的に定義することは困難である。よって、個人情報の定義については十分議論し定義する必要があり、特に医療機関においては極めて機微な個人情報を病院全体で取り扱っていることを鑑みると、本ガイドラインでは広範な観点で個人情報を捉えておくものとする。

各医療機関のコンプライアンス・プログラム作成にあたっては、倫理委員会等の審査機関を設け、ここの医療機関での保護ポリシーを作成し、公開しておくことが望ましい。

Ｃ．最低限のガイドライン

医療機関においては取り扱う個人情報の特性を考慮し、医療系（看護系含む）、事務系などで各々責任者等を定め、その責任者を中心に個人情報の特定、管理すること。

個人情報を管理するために医療機関で取り扱う全ての個人情報を把握すること。

業務活動の中に個人情報を特定できる手順や仕組みを確立しておくこと。

4．3．2　法令及びその他の規範

A．JIS Q 15001 の要求事項

事業者は、個人情報に関する法令及びその他の規範を特定し、参照できる手順を確立し、維持しなければならない。

B．医療機関としての解釈

個人情報に関する法令及びその他の規範を調査収集し、従業員がいつでも参照できるようにする必要がある。医療の場合、守秘義務を定めた法律があり、これらを参照可能にしておく必要がある。また個人情報保護に関する規範には各種ガイドラインや倫理綱領などが含まれ、これも数多く存在する。あまり多く取り上げても読むことができないため、重要で基本的なものを収集するべきである。以下に例を示す。この例の実際の条文等については付録３に示す。

法律：

- 憲法 20 条　「信教の自由」
- 刑法 35 条　「正当行為」、37 条　「緊急避難」、134 条　「秘密漏示」
- 国家公務員法 100 条　「秘密を守る義務」
- 地方公務員法 34 条　「秘密を守る義務」
- 労働安全衛生法 104 条　「健康診断に関する秘密の保持」
- じん肺法 35 条の３　「じん肺健康診断に関する秘密の保持」
- 医療法 1 条の 4「医師等の責務」、72 条「秘密漏泄」
- 保健師助産師看護師法 42 条の２　「守秘義務」
- 診療放射線技師法 29 条　「秘密を守る義務」
- 救急救命士法 47 条　「秘密を守る義務」
- 臨床検査技師、衛生検査技師等に関する法律 19 条　「秘密を守る義務」
- 理学療法士及び作業療法士法 16 条　「秘密を守る義務」
- 歯科技工士法 20 条の２　「秘密を守る義務」

規範：

- ヒポクラテスの誓い
- 医師の倫理（日本医師会）
- 患者の権利と責任「勤務医マニュアル」（日本病院協会）
- 個人情報保護法案
- 医療における個人情報保護ガイドライン案

C．最低限のガイドライン

上記を例にその機関で参照すべき法律・規範を調査収集し、すべての従業員が参照可能な状態におくこと。

4．3．3　内部規程

A．JIS Q 15001 の要求事項

事業者は、個人情報を保護するための内部規程を策定し、維持しなければならない。 内部規程は、次の事項を含まなければならない。 a）事業者の各部門及び階層における個人情報を保護するための権限及び責任の規定。 b）個人情報の収集、利用、提供及び管理の規定。 c）情報主体からの個人情報に関する開示、訂正及び削除の規定。 d）個人情報保護に関する教育の規定。 e）個人情報保護に関する監査の規定。 f）内部規程の違反に関する罰則の規定。 事業者は、事業の内容に応じて、コンプライアンス・プログラムが確実に適用されるように内部規程を改定しなければならない。

B．医療機関としての解釈

（1）内部規程の構成

本要求事項に準拠した個人情報保護を目的とする院内規程が必要である。この規程はコンプライアンス・プログラムの中核をなす基本規程、また、従業員等が組織として統一的、合理的に行動し得るよう細則、様式などの詳細規程を整備する必要がある。この基本規程及び細則等の院内規範を包括して内部規程という。内部規程は、従業員に対し十分な告知がなされなければならない。

（2）内部規程の制定・改廃手続

内部規程の制定・改廃手続きについて、規程管理規程などを制定し整備しておく必要がある。

（3）既存規程の内部規程への取り込み

なお、以下のような既存規程に対して個人情報保護を目的とした要求事項を網羅するよう改訂が行われる場合は、既存規程を体系化し、不足分の規定を作成することによりコンプライアンス・プログラムを構築することが可能である。

既存規程の例：

- 情報セキュリティ規程（セキュリティポリシー）
- 規程管理規程
- 入退室管理規程
- 就業規則
- 職務分掌規程

- 職務権限規程
- 文書管理規程
- 外部委託管理規程
- 教育規程
- 監査規程
- オーダーリングシステム運用規程
- 医事システム運用規程
- 電子カルテ運用規程
- ・・・・

C．最低限のガイドライン

医療機関は個人情報保護を目的とする内部規程を策定し、維持すること。

（1）規程に盛込むべき要件

a）各部門及び階層における個人情報を保護する為の権限及び責任

b）個人情報の収集、利用、提供及び管理

- 個人情報（個人情報の属性、例えば住所、氏名の他、病歴、家族構成、投薬歴、手術歴、アレルギー反応、等の個別の属性）を特定及びリスク分析する手順
- 収集、利用、提供に関する詳細手続き（個人情報を収集、利用、提供する目的、根拠の明確化及び本人の同意を得る手続き等）に関する事項
- 個人情報の保管、廃棄、バックアップ等に関する事項
- 個人情報の取扱い場所への立入許可・制限に関する事項
- 個人情報を処理する情報処理システムの利用許可・制限（Need To Know の原則に基づくアクセス権限）等に関する事項
- 個人情報処理の委託に関する委託先の選定基準（委託先の個人情報管理体制の有無等）、契約基準（委託契約に機密保持条項を含めた個人情報保護条項を盛り込む等）等に関する事項
- 運用管理（機器操作、記録媒体の取扱、障害時対応等）に関する事項

c）患者からの個人情報に関する開示、訂正及び削除

- 情報主体からの権利行使の求めに応じて如何に対応するべきか等（患者窓口の一元化、様々な要求に適切に対応するためのマニュアルの整備等）

d）個人情報保護に関する教育（教育・啓蒙活動の実施とその履歴を証跡として管理）

e）個人情報保護に関する監査（モニタリングの実施と改善アクションのフォロー、その履歴を証跡として管理）

f）内部規程の違反に関する罰則

g）個人情報のリスクに対する予防措置（技術面、管理面、物理面）