（ 案 ）

「医療情報システムの安全管理に関するガイドライン　第４版」

に関するＱ＆Ａ

平成　年　月

総論

Q－1
① このガイドラインを遵守すべき対象者は誰か。
② このガイドラインはシステムベンダに読んでもらえば、医療機関の関係者まで読む必要はないのではないか。
③ 再委託が行なわれる場合の再委託する事業者もこのガイドラインを遵守することとなるのか。また他に遵守すべきガイドラインがあるのか。

A
① 医療情報システムを運用する医療機関等の組織の責任者の方です。
② 医療情報システムの管理上の一次責任は医療機関側にあります。安全管理は運用と技術とが相まって一定のレベルを達成するものです。このガイドラインに則った、実際のシステム構築の多くはシステムベンダが行うかもしれませんが、それを管理・運用するのは、あくまで医療機関側の責任です。医療機関の関係者は、このガイドラインの内容をよく理解し、遵守していただく必要があります。
③ 再委託先でもこのガイドラインが遵守されるよう、指導・監督していただく必要があります。安全管理の観点ではこのガイドラインを、医療情報システムで取り扱う個人情報の保護の観点では、「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」を遵守することが必要です。情報処理事業者向けには経済産業省がガイドライン「医療情報を受託管理する情報処理事業者向けガイドライン」を発行しています。こちらも参考にする必要があります。

Q－2　「医療情報システム」とは具体的に何を示すのか。

A　医療機関等のレセプト作成用コンピュータ（レセコン）、電子カルテ、オーダリングシステム等の医療事務や診療を支援するシステムだけでなく、何らかの形で患者の情報を保有するコンピュータ、遠隔で患者の情報を閲覧・取得するようなコンピュータや携帯端末も範疇として想定しています。また、患者情報が通信される院内・院外ネットワークも含まれます。

Q－3
① このガイドラインの対象情報の範囲はどこまでか。
② 他の病院から提供された、電子化された情報の取り扱いは、このガイドラインの対象となるのか。

A　このガイドラインは、医療に関わる情報を扱うすべての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄にかかわる人または組織が対象となっています。

そのため、このガイドラインの対象情報は、前文の情報システムや人または組織の中で扱われる情報のうち、①施行通知※に含まれている文書、②施行通知には含まれていないものの、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成 16 年法律第 149 号　以下「e-文書法」という。）の対象範囲で、かつ、患者の個人情報が含まれている文書等（麻薬帳簿等）、③法定保存年限を経過した文書等、④診療の都度、診療録等に記載するために参考にした超音波画像等の生理学的検査の記録や画像、⑤診療報酬の算定上必要とされる各種文書（薬局における薬剤服用歴の記録等）、等が対象です。

したがって、他の病院から提供された電子化された情報についても、電子化の状態で利用・保存する限りはこのガイドラインの対象となります。

なお、いわゆる医療情報の取り扱いについては、個人情報の保護に関する法律（平成１５年５月３０日法律第５７号　以下「個人情報保護法」という。）並びに「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」を参照してください。

※　「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成１７年３月３１日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知）

Q－4
① このガイドラインに違反した場合の罰則等はあるのか。
② ガイドラインを遵守しなかった場合、個人情報保護法、e-文書法以外に抵触する法令はあるのか。
③ ガイドラインのC項を実施しなかった場合、具体的に罰則規定があるのか。

A　ガイドラインに罰則規程はありません。ただし、このガイドラインは個人情報保護法をはじめとする、医療情報を取り扱う法令を遵守するためのガイドです。したがって、このガイドラインに違反した状態で情報事故等を来した場合は法令を遵守したとは言えない可能性が高く、法令により罰せられる可能性は高いと言えます。

Q－5　このガイドライン通りにシステム構築をして起こった事故に対する責任はどこにあるのか。国の責任も発生するのか。

A　このガイドラインは、個人情報の保護に関し、厚生労働大臣が法を執行する際の基準となるものの一つです。国にはガイドラインを適宜改訂する責任があるとも言えますが、このガイドラインは技術だけではなく、運用を含めた安全対策を示したものであり、個々の医療機関等の安全対策として、最新情報等を収集し対応することも求めています。

技術は日進月歩であることから、ガイドライン策定時には予想できなかった脅威が発生する可能性もあります。そのためこのガイドラインを遵守していたことをもって、医療機関等に全く責任が無いとはいえません。

Q－6
① ガイドラインが既に第３版まで出されているが、全て読む必要があるか。
② 技術の進歩は著しいが、このガイドラインは定期的に見直すのか。

A
① 全て読む必要はありません。旧版の内容は最新版で変更、削除等されている場合がありますので、最新版のみお読みください。
② このガイドラインは定期的に見直すこととしております。

Q－7　「C.最低限のガイドライン」さえ措置すればよいのか。

A　各項目での「C.最低限のガイドライン」は、制度上の要求を満たすための文

字通り「最低限」実施すべき事項です。施設の規模や体制によって要求される事項は異なってきますので、「D.推奨されるガイドライン」を考慮し、最適の対策を行う必要があります。

Q－8　大規模な病院も、診療所も同じような対策が必要なのか。

A　制度上の要求事項は同一ですので、規模にかかわらず制度上の要求事項を満たす必要がありますが、具体的な対策については、医療機関等の規模に応じて対策のレベルが変わることがあります。たとえば医師１名のみで運営している診療所においてはシステムの利用者は１名になりますので、「6.5　技術的安全対策」の利用者の識別と認証における技術的対策として求められている「C.最低限のガイドライン」5.の医療従事者や関係職種のレベルに沿ったアクセス管理は事実上不要になります。具体的な対策の要否や対策レベルについては各医療機関の規模や物理的な構造、運用形態で適切な対策が異なりますので、各章のＢ考え方を参考にしてご検討ください。

Q－9　このガイドラインの説明会や研修会などは実施されていないのか。

A　厚生労働省として実施しているものはありませんが、日本医療情報学会や保健医療福祉情報システム工業会等の講演会で解説が行われることがあります。

Q－１０　第３版からの変更点はどこか（変更点一覧があれば読みやすい。）

A　「1　はじめに」の「改定概要」を参照してください。

Q－１１　「C.最低限のガイドライン」だけまとめた表はないか（技術的背景も大切ですが、量が多くて読みきれない。）

A　「C.最低限のガイドライン」には、適用のための条件がある項目が少なからずあります。したがって、ここだけを抜き出した表のみを参照してシステム構築や運用を行うことは、それらの適用条件の考慮が抜けることが懸念されます。ご面倒ではあっても、「B.考え方」の内容をご理解の上、「C.最低限のガイドライン」を参照してください。

Q－１２　「C.最低限のガイドライン」は守っていたが、「D.推奨されるガイドライン」を守っていなかったせいで、裁判で不利になるようなことはないか。

A　このガイドラインは個人情報保護法並びに e 文書法に対応したガイドラインであるため、それ以外の民事訴訟、刑事訴訟に対して「D.推奨されるガイドライン」を遵守しているかどうかは直接的な判断基準とはならないと考えられます。裁判に至る個々の事例により事情は異なると考えられるので、不利になるかどうかについては一概に言えるものではないありません。「D.推奨されるガイドライン」の採否については医療機関等の方針に基づいて適切に判断して運用してください。

「3　本ガイドラインの対象システム及び対象情報」関係

Q－１３　電子保存が認められている文書とは具体的に何か

A　「厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令」（平成 17 年厚生労働省令第 44 号　以下「e-文書法省令」という。）、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律等の施行等について」（平成 17 年３月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知）で定められた文書で、具体的には「3.1 第７章及び第９章の対象となる文書について」に列挙されたものです。

「4 電子的な医療情報を扱う際の責任のあり方」関係

Q－１４　情報等の漏洩事故があった場合は、受託する事業者に対応をさせればよいのか。

A　漏えい等の事故に際しては、当該情報の一次管理している医療機関側に、善後策を講ずる責任が発生します。もちろん事故を起こした事業者側も責任を免れるものではなく、両者が協力して善後策を講じる必要があります。

Q－１５　「通常運用における説明責任」を果たす際に、患者に説明すべき範囲はどこまでか。

A　通常は「診療情報を適正に保存するとともに、適正に利用すること」を「基本方針」の中に盛り込み公表し、詳細は苦情・質問を受け付ける窓口を設け、「4.1　医療機関等の管理者の情報保護責任について」（１）①の項目の問合せに回答できるように準備をしておく必要があります。

Q－１６
① 請負事業者との対応にあたる「個人情報保護の責任者」になる要件はあるのか。
② 「個人情報の保護について一定の知識」とは何か。

A
① 具体的な要件が定められているものではありませんが、医療に関わるすべての行為は医療法等で医療機関等の管理者の責任で行うことがもとめられています。そのため、結果的には、個々の医療機関等の管理者が、権限を一部委譲するに適当と考える者を「個人情報保護の責任者」として選任することになると考えられます。
② 「電子化された個人情報の保護についての一定の知識」についても、具体的な条件が示されているわけではありませんが、電子化された情報は、紙媒体の情報に比べ、いとも容易に、大量の情報が漏洩する可能性があるという特徴を持つことから、それら特徴と扱い方について理解していることが重要です。

Q－１７　委託と第三者提供の違いは何か。

A　委託とは契約書等に基づき業の一部（例えば臨床検査）を外部に託すものであり、その情報の管理責任は一義的には委託元にあります。したがって委託元は委託先の情報管理を監督しなければなりません。それに対し第三者提供（例えば紹介状による治療情報の提供）とは、患者等の同意のもとに情報を他の事業者等に提供することです。第三者提供では情報提供が確実に行われた時点で提供された情報の管理責任は提供先に移動します。ただし、電子化情報は提供が行われた場合でも提供元にも同じ情報が残ることが多く、残った情報の管理責任がなくなるわけではありません。

Q－１８　第三者提供が成立するタイミングはいつの時点か。

A　ネットワーク経路を利用した第三者提供では、提供元と提供先の間で、責任分界点を定め、普通時や事故発生時の対処を含め、あらかじめ契約等で合意しておく必要があります。

「5　情報の相互運用性と標準化について」関係

Q－１９　「５　情報の相互運用性と標準化について」は具体的に何を遵守すればよいのか。

A　「５　情報の相互運用性と標準化について」では、相互運用性の重要性と、それを実現するために医療機関がシステムベンダに要求すべき内容が記述されています。具体的には、医療機関はシステムベンダーの標準化に対する基本スタンス、標準に対応していないならばその理由や対応案をシステムベンダから説明を受け、一定の理解を等しくしておくことを求めています。さらに、現在導入しているシステムの更新やシステムの新規導入の際に、システム間でのデータ互換性やシステム接続性が確保されるように医療機関においても相互運用性につき中長期的なビジョンを持ち、計画的にベンダーに要求していくことが望まれます。

Q－２０
① 相互運用性と標準化を行うことのメリットは何か。
② 基本データセットや標準的な用語集、コードセットを実装しなかった場合、どのような不利益が想像されるのか。

A　標準化のメリットには、システム間の相互運用性、データの長期的可用性などがあります。患者紹介や地域連携などで、外部の医療機関等と診療情報をやり取りする場合、使用されているコードや用語が標準的で無い場合、適切な情報交換が難しくなります。また、システムをリプレースする場合も、データ変換などが必要になってしまいます。これらの場合に、コードや用語が標準化されていれば、データ変換の手間や変換機能の実装に必要な費用と時間の節約が期待できます。

Q－２１　基本データセットを利用し、MEDIS-DC の標準マスタを組み合わせた場合は、情報システムのリプレイス時の相互運用性は保証されるのか。

A　基本データセットおよび標準マスタを活用することは相互運用性の確保を容易にはしますが、保障はされません。基本データセットに含まれない項目や標準が定められていない用語・コードも存在します。しかし、基本データセットや標準マスタは概ね重要あるいは実装頻度の高いものを対象にしており、採用することによって相互運用性を確保するためのコストを大幅に下げることができます。

Q－２２　外字等の作成について注意すべき点は何か。

A　外字を使用したシステムではあらかじめ使用した外字のリストを管理し、システムを変更した場合や、他のシステムと情報を交換する場合には表記に齟齬のないように対策する必要があります。

「6　情報システムの基本的な安全管理」関係

Q－２３　医療情報を電子化するにあたって定められた要件は何か。

A　電子化する対象である全ての記録に対してのガイドが「６　情報システムの基本的な安全管理」に記載されています。さらに保存義務のある記録の電子化には、ｅ文書法省令に従った内容が「７　電子保存の要求事項について」に記載されています。真正性、見読性、保存性があります。さらに、紙原本をスキャナで読み取り、電子文書化する場合の記載が「９　診療録をスキャナ等により電子化して保存する場合について」にあります。保存義務の無い書類であっても、これらの記載に準拠することが求められています。

Q－２４　ウイルス対策等大変なので、外部と遮断した環境を設定する方が望ましいのか。

A　外部と遮断することによって、ウイルス侵入のリスクを低減できることは事実ですが、それだけで侵入をすべて防げるわけではありません。従業者が不用意にUSBなどを利用するなどでも侵入することがあります。ウイルス対策ソフトの導入、ぜい弱性の対策を行ったソフトウェアの利用等の対策が必要です。

また、医療情報の有効な利用を図るために、外部との接続を行うことも、最近は広く行われるようになってきています。このような環境でのウイルス侵入等の脅威は確かにありますが、効果的な対策を行うことで、リスクを許容範囲に収めることは可能です。対策方法については、このガイドラインをご参照ください。

Q－２５　「個人情報保護に関する方針を策定し、公開していること」とあるが、公表公開の方法は問わないのか

A　「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」に明記されているように患者が確認できる院内掲示は必要です。さらに広報誌やホームページ等で明示する方法があります。

Q－２６　「小規模医療機関等において役割が自明の場合は、明確な規程を定めなくとも良い。」とあるが、小規模の基準は病床数や職員数で決められているのか

A　明確な規定はありませんが、自明とは「なんら説明を要しない」という意味になります。例えば、役割を果たすための有資格者がその施設内に唯一人しか存在しない場合などです。そのため、明確な規定がなくとも説明責任を果たすことが可能であるかを検討する必要があります。

Q－２７　「個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること」とあるが例えば、外来、ナースステーション等では、それらの措置は困難ではないか。

A　個人情報が管理できない環境下におくことが問題です。外来やナースステーションでは患者 and/or 家族の入退はあるものの、患者本人である等来訪者の識別ならびに来訪の事実をカルテ等に記録することにより来訪記録はできており医師や看護師により情報管理されていると思われます。ただし、機器修理等本来の医業以外の目的で来訪した者の記録、識別、制限等管理することは重要です。

Q－２８　「英数字、記号を混在させた８文字以上の文字列が望ましい。」とあるが、８文字の根拠は何か。

A　英数字８桁（大小文字＋数字の全 62 文字からの選択）が推奨される理由は、毎秒４０万回のペースでパスワードを解析しようとした場合、パスワードが解析されるのに、計算上では約１７年を要するとされているためです。これが６桁だと約１．６日となります。この計算はあくまでも現在の一般的なコンピュータの計算速度を元にしていますので、将来は、もっと短時間で解析されてる可能性が高くなります。また、推測しやすいパスワードは、より容易に解析される可能性が高くなります。したがって、ガイドラインでも類推しやすいパスワードの使用禁止と、適当な期間でのパスワード変更を推奨しています。

Q－２９　「確実に情報の破棄が行なわれたことを確認すること」とは立ち会いを前提としているのか。

A　立ち会いを前提とはしていません。破棄のマニフェストをもらう等、「6.6 人的安全対策」「(2)　事務取扱委託業者の監督及び守秘義務契約」「C.最低限のガイドライン」の内容を順守し、確実に確認を行っていただければ問題ありません。

Q－３０　「情報機器を持ち出してよいのか、持ち出してはならないのかの切り分けを行うことが必要である。」とあるが、具体的にどのような基準で判断をすればよいか。

A　「具体的な基準」は、施設のセキュリティに対する考え方や、持ち出す情報機器、情報そのもの、持ち出した環境によって大きく異なります。各施設においての業務内容と手順から、情報機器持ち出しの必要性とそれに伴う情報漏えいリスクを総合的に判定することになります。事前に判断基準を決めることと判定結果の文書化が大切です。

Q－３１　災害等で電子システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは真正性の観点から問題にはならないのか。（システムへの入力時のタイムスタンプが有効になるのではないか）

A　適切な安全管理が実施されていれば問題ありません。「6.10 災害等の非常時の対応」において災害等の非常時の対応について要求事項が記載されていますのでそちらを参照してください。また、紙データを電子システムに反映させる際には、紙データをオリジナルとして保存する必要が生じると考えられます。オリジナルの紙データをスキャナ等により電子化して保存する場合は、「９　診療録等をスキャナ等により電子化して保存する場合について」を参照してください。また、電子カルテなどに転記した場合は転記した情報で診療などを実施することに問題はありませんが、オリジナルとしての紙もしくはスキャナ等で電子化したデータは別途適切な安全管理を実施したうえで定められた期間保存する必要があります。

Q－３２　「サイバー攻撃で広範な地域での一部医療行為の停止等、医療サービス提供体制に支障が発生する場合は、所管官庁への連絡を行うこと。」とあるが、所管官庁の連絡先や連絡内容等はどのようにすればよいのか。

A　医療機関等からの連絡先や連絡内容については、各都道府県を経由して厚生労働省医政局医療機器・情報室へ連絡します。詳細は、（準備中の通知）を参照して下さい。

Q－３３　「従業者による外部からのアクセスに関する考え方」に「仮想デスクトップを導入した際の運用等の要件にも相当な厳しさが要求される」とあるが、どの程度か

A　従業者による外部からのアクセスで問題となることは、利用するＰＣや通信経路など状態および周囲から窃視されるなどの作業環境が管理できないことです。例えばＰＣにキーボードロガーのような不正ソフトウエアがインストールされているかも知れませんし、空港や喫茶店などでアクセスすれば周囲の人に覗かれるかも知れません。仮想デスクトップは不正ソフトウエアの作用を避け、ＰＣ上に情報が残留することを防ぐ目的で使用します。また通信経路の安全性も確保するためにＶＰＮの成立と連動して稼働することが望まれます。さらに運用としては周囲の環境に十分注意し、窃視を防止するとともに、過去のログイン時間の確認を確実に行うこと等で、不正アクセスの検出につとめる必要があります。

Q－３４　「セッション乗っ取り、IP アドレス詐称等のなりすましを防止する対策をとること。上記を満たす対策として、例えば IPSec と IKE を利用することによりセキュアな通信路を確保することがあげられる。」とあるが、IPSec と IKE を利用して、セキュアな通信路を確保するための具体的な方法としてはどのようなものがあるのか。

A　２通りの方法があります。

１）IPSec と IKE で通信可能なソフトウエア VPN 製品を用いてネットワークを構成する。

２）IPSec と IKE で通信可能なハードウエア VPN 製品を用いてネットワークを構成する。

Q－３５　「ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。」とあるが、ソフトウエアは、安全性の確認対象から外れるのか。

A　ここでいうソフトウェアが「ルータ等のネットワーク機器の機能をソフトウェアで実現しているもの」を指すのであれば、その当該ソフトウェアに対して安全性が確認できる必要があります。「ルータ等のネットワーク機器」を当該ソフトウェアに読み替えて対応ください。

Q－３６　「ルータ等のネットワーク機器は、安全性が確認できる機器を利用し、施設内のルータを経由して異なる施設間を結ぶ VPN の間で送受信ができないように経路設定されていること。安全性が確認できる機器とは、例えば、ISO15408 で規定されるセキュリティターゲットもしくはそれに類するセキュリティ対策が規定された文書が本ガイドラインに適合していることを確認できるものをいう。」とあるが、安全性を確認するための方法は他に無いか。

A　ISO/IEC 15408 で認証された機器を導入することが必須ではありません。このガイドラインが求める安全対策のための要求事項を、導入を検討している機器ベンダに示し、回答を求めてください。満足する回答が得られれば、安全性が確認できた機器と判断していただいて結構です。

Q－３７　「通信事業者やシステムインテグレータ、運用委託事業者、遠隔保守を行う機器保守会社等多くの組織が関連する。そのため、次の事項について、これら関連組織の責任分界点、責任の所在を契約書等で明確にすること。」とあるが、契約書の記載方法を教えて欲しい。

A　「C.最低限のガイドライン」６に上げてある事項に関し、個別に責任範囲及び共同対応範囲を定め、誰が何をどのタイミングで行うかを文書化してく

ださい。

Q－３８　「患者等に対する説明責任の明確化」とありますが、どのような手段、タイミングで患者に伝えればよいか。

A　通常の運用における送受信の仕組みや関連事業者間での安全管理体制の説明は、患者側から質問された時が典型的に想定されます。質問者の理解度にも差があるため一概には決められませんが、説明する場合に備えた資料を準備しておくことが有効です。院内に掲示しておくとことも考えられます。また、医療情報について何らかの不都合な事態（典型的には漏えい）が生じた場合の双方において、具体的な説明責任遂行のためのタイミング等はケースごとに異なるため、定められたものはありません。しかし、情報に関する事故は、説明に際して受託する事業者の情報提供や分析が不可欠な場合が多いと考えられることから、医療機関等との密接な連携の上、対応することが必要と考えられます。

Q－３９　「電子署名法の規定に基づく認定特定認証事業者の発行する電子証明書を用いなくてもAの要件を満たすことは可能であるが、少なくとも同様の厳密さで本人確認を行い、さらに、監視等を行う行政機関等が電子署名を検証可能である必要がある。」とあるが具体的にどのようなものが想定されるのか。

A　電子署名法に基づく認証業務の認定は、一定の基準を満たせば国が認定し、認定を受けた者の義務を定めるものであって、認証業務における信頼性の目安を提供するものです。

従って、それ以外の者としては、民間の認証事業者全般が想定されます。ただし、一般利用者が信頼性を容易に確認できない場合には、認定特定認証事業者の発行する電子証明書を利用することが推奨されます。

Q－４０　タイムスタンプはパソコンの時間と同じでよいか。

A　タイムスタンプは電子署名を含む文書全体の真正性等を担保するために必要なものであることから、このガイドラインでは財団法人日本データ通信協

会が認定した時刻認証事業者のものを利用する必要があります。

Q－４１　通常閉じたネットワークで構築することが多い病院施設において、１枚１枚の文書にリアルタイムにタイムスタンプを付与することは、実装が非常に困難ではないか。

A　「6.12　法令で定められた記名・押印を電子署名で行うことについて」は、対象が紹介状、診断書等の「法令で定められた記名・押印を電子署名で行うことについて」であり、これら以外の文書等の一枚一枚へのタイムスタンプの付加を必須要件とはしていません。タイムスタンプを付与するにはセキュアなタイムスタンプ環境を構築する必要があります。

「7　電子保存の要求事項について」関係

Q－４２　部門系で発生する記録等は、ガイドラインで言う診療録等としての適用を受けるのか。

例えば、エコー検査の紙画像や心電図の紙波形結果など、院内で発生した文書（ワープロやシステム出力）で、かつ手書き情報の付記がなければ、スキャニングして電子化情報を原本とし、元の紙は廃棄できるのか

※　スキャニングする際、「どの患者の結果で、誰が、いつ記録したか」は登録することを前提。

※　紹介状や同意書など、外部からの文書や押印して初めて効力が発生する文書は、紙を原本として残すのが原則。

上記の場合、診療録等として、確定することになるのは、どの行為の時になるのか

スキャニング時の作業責任者と情報作成管理者は、どのようになるのか

また、情報作成管理者は、有資格者等である必要があるのか

手書きの付記などがある場合は、どのように行えばよいのか

A　診断の根拠となる記録や診療方針に影響を与える記録等についてはオリジナルを定められた期間保存する必要があります。

オリジナルの紙データをスキャナ等により電子化して保存する場合は、「9

診療録をスキャナ等により電子化して保存する場合について」を参照してください。その際、確定操作は必要ありません。紙の記録が作成された時点で記録は確定しており、確定された記録を電子化しているので「９　診療録をスキャナ等により電子化して保存する場合について」で求められている電子化した際の証跡を残すことで電子化されたデータをオリジナルと同等として扱えます。（オリジナルの紙を破棄出来ます）作業責任者と情報作成管理者は運用管理規定などで内部ルールを定め、適正に運営されていることを監査すること等が求められますが、有資格者である必要はありません。（医療機関等の内部で独自に資格を定め、運用することを妨げるものではありません）

Q－４３　電子カルテを導入した場合、それまでの旧カルテ（紙カルテ）について保存義務があるか。あるとすれば何年か。

A　紙の診療録の法定保存期間は医師法で一連の診療の終了後５年とされていますが、電子カルテの導入により、以前の紙の診療録をスキャナ等で適切に電子化した上に管理責任者によって保存義務の対象が電子化された診療録であると認められれば、紙の診療録に法定上の保存義務はありません。このような処理を行わない場合は法定通りの保存義務があります。

なお、スキャナ等で電子化して運用する場合でも、情報の真正性・保存性の確保の観点から、元の媒体である紙の診療録も保存することは有効であり、法定期限に限らず外部保存を行うことが望ましいです。ただし、この場合も電子化および外部保存に関しては、「９　診療録をスキャナ等により電子化して保存する場合について」等を参照の上適切に行われなければなりません。

Q－４４　画像撮影装置(モダリティ)にて取得した画像を専用端末に転送表示し、診療放射線技師が、画像を評価し、オーダに応じた画像情報が取得できていること、付帯情報が正しく入っていること、などを確認し、必要に応じて修正したり、画像の方向、順序などを変更したり、不必要な画像を削除したりなど、医師の読影作業を支援する作業は“検像”と呼ばれ、PACS の機能として、普及が進んでいる。この場合、検像前の画像情報を原本として保存すべきか、それとも検像後の画像情報を原本としてすべきか。また、後者の場合、検像に関わる作業の履歴保存が必要か。

A　検像後の画像を保存義務の対象とすることができます。運用管理規程で検

像後の画像情報を保存義務の対象として定めてください。ただし、照射記録と検像後の画像情報が一致しないなどの場合は、画像を削除した履歴を保存するなどの措置が必要です。

Q－４５　真正性の確保について、記載されている情報と作成責任者には具体的にどのような組み合わせがあるか。

A　情報と作成責任者の組み合わせとしては下記のような例があります。

例１）　医師が患者の診察時にカルテに所見を記述する。
　　情報　：所見
　　作成責任者　：実際に診察を行った医師

例２）　看護師が医師の指示に基づく処置を行った際に実施状況を看護記録に記述する。
　　情報　：処置実施記録
　　作成責任者　：実際に処置を行った看護師

例３）　読影担当医が放射線画像の読影レポートを作成する。
　　情報　：読影レポート
　　作成責任者　：読影を行った放射線科医師

例４）　検査技師が検査ラインから出力された検査結果のバリデーションを実施し、システムに取り込む。
　　情報　：検査結果
　　作成責任者　：バリデーションと取り込み操作を行った検査技師

例５）　夜間等で当直医が主担当医の電話での指示により、指定された薬剤のオーダ入力を行った。
　　情報　：投薬指示
　　作成責任者　：実際にオーダを実施した当直医

Q－４６　記録を確定する方法として、①操作者が情報を入力画面を見ながら入力して記録する場合、②外部機器等から確定されていない情報を取り込み記録する場合、③外部システムで確定された情報を取り込み記録する場合が考えられるがそれぞれどのように対応すべきか。

A　確定操作は、文書の責任者が誰で、操作の時点で対象とする文書の記述に誤入力や改ざん等がないことを保証し、記載に対して責任をもつという意味合いがあります。そのため、①「操作者が情報を入力画面を見ながら入力し

記録する場合」・・・この場合には、確定するという操作を行うことで内容を「責任者が」保証することになります。「責任者が」としたのは、文書の入力を責任者が自ら行う場合や代行者が行う場合があるからです。いずれの場合も、規則によって決められた責任者が確定したということになります。また、処理としては署名を施すなどになります。②「外部機器等から確定されていない情報を取り込み記録する場合」・・・この場合には操作者が、記述の改ざんや誤入力等がないことを確認した上で、スキャナ等による読み込みを行い、誰の記録であるかを関連づけし、①のような確定操作を行うことになります。③「外部システムで確定された情報を取り込み記録する場合」・・・改めて受け取り側で確定操作を行う必要はありませんが、外部システムで確かに確定されていることを確認することは必要です。ただし、確定された情報しか取り込まれないようにシステムが構築されている場合はその限りではありません。

Q－４７　Ｘ線ＣＴの検査で、オリジナルの画像の他にオリジナル画像から生成した３Ｄ画像も使って診断している。
　電子保存を行う際に、オリジナル画像さえ保存しておけば、診断に使用した３Ｄ画像は消去してしまってもかまわないか
　3D 画像作成時のパラメータは保存されていないため、診断の際に生成した３Ｄ画像を完全に再現することは難しい状況である。

Ａ　オリジナル画像から当該画像を生成することが原理的に可能であれば、直接診療に使用した処理画像データを保存しておく必要はありません。しかし、この例では、３Ｄ画像作成のパラメータがないと診断に用いた画像を完全に再現することが困難であるということなので、オリジナルの画像を消去することはできません。

Q－４８　外部の医療機関等から持ち込まれたＸ線写真（コピー）や画像データを当院での診療に用いた場合、保存義務は生じるのか

Ａ　原本の保存義務はもとの医療機関にありますが、持ち込まれた診療情報を診療に利用した場合は、当該医療機関においても保存義務が発生します。

Q－４９　代行入力を行う場合、代行を許可した証拠はどのように残しておけばいいのか。

Ａ　代行入力を容認する場合には、必ず入力を実施する個人毎に ID を発行し、その ID でシステムにアクセスし,入力者のログ、あるいは作業報告等の台帳を作成し、記録を残す必要があります。
　これらを含めた代行入力に関する規定の策定が必要です。

Q－５０　モダリティから PACS へ垂れ流した画像はいつ確定なのか。

Ａ　各施設において運用管理規程に具体的決めることになります。例えば、PACS が受信した時点、PACS で受信後一定時間経過後、PACS で受信後一定時刻を過ぎた時点、などが考えられます。モダリティ（画像撮影装置）にて取得した画像全てを原本とする他に、例えば、診療放射線技師が「検像」作業を実施する場合は、検像後の画像を原本とすることもできます。この場合、運用管理規程で検像後の画像情報を原本として定めてください。ただし、照射記録と検像後の画像情報が一致しないなどの場合は、画像を削除した履歴を保存するなどの措置が必要です。

Q－５１　事前の確認時と状況が変わり請負事業者が倒産するなどでソフトウェアの保証が無くなった場合、見読性は確保されていないことになるのか。

Ａ　倒産ではなくソフトウエア事業を廃止する場合は見読性を確保する条項等契約書に明記することで見読性確保は可能です。しかし、倒産の場合は使用継続は保証されるものの、長期見読性は保証されないこととなり、使用者がこれを担保しなければならなくなります。診療等に差し支えない期間内に見読性が保障される対策を講じなければならなりません。この対策を容易にするためにもデータ継続性の保証（例えばデータ標準化）は重要です。

Q－５２　「遠隔地」の定義はあるのか。

Ａ　具体的な定義はありませんが、当該医療機関等が地震等の大災害にあった場合でも、それらの被害を受けず、安全に保存が可能であると考えられる地域と考えられます。

Ｑ－５３　ネットワークを通じて外部に保存する場合で「緊急に必要になることが予測される診療録等」とは具体的にどの程度か。

Ａ　各医療機関の機能により判断すべきですが、診療録等の参照が迅速に行えないことで、その方の生命や体に重大な影響を及ぼす恐れがあることが想定されるものが対象となります。例えば、これから手術を行おうとしている方や入院されている方の診療録等が想定されます。通常１週間程度あるいは前回診療データも目安になります。

Ｑ－５４　「診療録等のデータを標準形式が存在する項目に関しては標準形式で、標準項目が存在しない項目では変換が容易なデータ形式にて出力及び入力できる機能を備えること」とあるが、標準形式は正式に定められたものがあるのか。

Ａ　ガイドライン第４版「５　情報の相互運用性と標準化について」に、現時点での標準内容が挙げられていますので、参照して下さい。今後も、追加や更新がされますので、適宜参照して下さい。

Ｑ－５５　医療情報を電子化するにあたって定められた要件は何か。

Ａ　「Ｑ－２３」のＡを参照してください

「8　診療録及び診療諸記録を外部に保存する際の基準」関係

Ｑ－５６　掲示以外の周知方法はどのようなものがあるか。

Ａ　院内掲示以外の周知方法としては、パンフレットの配布、インターネット

ホームページでの公表、問診表への記載、医師・看護師等による口頭説明などがあります。

Ｑ－５７　電子化された診療情報は外部保存できるか。その際の要件は何か。

Ａ　電子媒体による外部保存をネットワークを通じて行う場合は「8.1　電子媒体による外部保存をネットワークを通じて行う場合」に、電子媒体による外部保存を可搬媒体を用いて行う場合は付則１にその要件が記載されていますのでそちらを参照ください。なお、いずれの場合においても「8.4　外部保存全般の留意事項」に留意する必要があります。

Ｑ－５８　民間事業者が外部保存受託機関となる場合が限定されている理由は何か。

Ａ　情報の漏えい等の情報事故に対する医療機関等の責任が相対的に大きいこと、また予期しない情報の利活用による被害者の苦痛や権利回復が困難であるため、外部保存を行うにあたり、法的に守秘義務等による厳格な措置が課せられた環境に限定されています。民間のデータセンターを利用する場合、現段階では、これらの行為を規制するための民間等の外部保存を受託する事業者に対する指針は存在するものの、その適否や遵守状況を踏まえながら十分検討が図られるべき状況にあり、厳しい制限を課しています。

Ｑ－５９　行政機関等が開設したデータセンター等には現在どのようなものが存在するのか。

Ａ　一部の自治体等がデータセンターを設置しています。

Ｑ－６０　震災等危機管理上の目的があれば、法令に保存が義務づけられている文書を電子的に作成し、外部に保存することは可能か（バックアップデータということではないのか）

Ａ　原本の保存としても可能です。ただし、受託する外部機関はもちろんのこ

と、委託する医療機関側でも、このガイドラインの要件を満たす必要があります。

Q－６１　民間事業者が外部保存を受託することについて法令等で罰則規定はあるか。

A　民間事業者が外部委託を受託すること自体は法令によって禁止されていないため、罰則規定はありません。受託した情報やそれを取り扱う情報システムの安全管理については個人情報保護法等によって要求事項が定められていますのでそれらを参照してください。また、このガイドラインにおいては医療機関等に対する要求事項を「８　診療録及び診療諸記録を外部に保存する際の基準」に記載しておりますので、医療機関等においてはこのガイドラインを参照し、適切な安全管理を実施してください。

Q－６２　地域連携のための情報システムとして、医療情報の所在だけを管理するレジストリと各医療機関が共有のために確保するリポジトリを設置する形態をとり、利用者側からは、レジストリにアクセスして所在を知り、リポジトリにアクセスして実際の情報を利用する方式をとることができる（IHE　XDS 統合プロファイル*）。この場合に各医療機関は、互いに保管された医療情報を共有する形となるので、“共同利用”という形と考えてよいか。またレジストリは民間などのデータセンターを利用することが適当と思われるが、各医療機関はデータセンターに所在情報を“委託”してもよいか。

*)http://www.ihe.net/

A　診療情報を「共同利用」するためには、個人データを特定のものとの間で共同して利用することを明らかにし、利用する個人データ項目、利用者の範囲、利用目的、個人データの管理責任の所在等をあらかじめ本人に通知等をしている必要があります。（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：参照）本ケースの場合は、こららの要件が不明確ですので、共同利用の要件を満たしていない可能性があり、この場合、他の施設での診療情報の利用は第三者提供にあたります。また、レジストリを民間などのデータセンターを利用する際には、 医療情報を外部保存する場合と同等の要件を満足する必要があります。

「9　診療録等をスキャナ等により電子化して保存する場合について」関係

Q－６３　診療の用途に差し支えない精度の基準はあるか。

A　厳密な精度の基準はありませんが、判読できること、重なりやスキャン範囲外などで見えなくなっている情報がないなど、見読性を確保しなくてはなりません。

Q－６４　汎用性が高く可視化するソフトウェアに困らない形式にはどのようなものがあるのか。

A　医療情報にはさまざまな形態の情報があります。画像、図形、波形、テキスト、数値、グラフなどの形式のデータから構成されています。これらのデータを一様に見ようとするならば、画像化しておくことが、恐らく最も汎用性の高い可視化手段となるでしょう。デジタル情報を画像化するには、PDF（Portable Document Format)が最も一般的なものだと思われます。紙やフィルムの形で存在する場合には、スキャナで画像化することで可視化できますが、この場合には JPEG（Joint Photographic Experts Group)、GIF(Graphics Interchange Format)、 PNG（Portable Network Graphics)などを利用することができます。これらのフォーマットはPCに組み込まれていたり、容易にダウンロードすることで取得できるソフトウェアによって可視化することができます。

Q－６５
① 診療録等をスキャナで電子化した場合、原本の取扱いはどのようにすべきか。
② 電子化された場合、法定保存年限を経過した文書も保存すべきと考えるべきか。

A　「9.1　共通の要件」の記載にしたがって電子化し、電子化されたものを保存義務のある原本とする場合は、スキャンされた原本は個人情報保護の観

点に注意して廃棄しても構いません。しかし、電子化した上で、元の媒体も保存することは真正性・保存性の確保の観点からきわめて有効であり、破棄を義務付けるものではありません。また、法定保存年限を経過した文書の保存期限は、各病院で規定することとなります。

Q－６６　「スキャナで読み取った際は、作業責任者(実施者または管理者)が電子署名法に適合した電子署名・タイムスタンプ等を遅滞なく行い、責任を明確にすること。」とあるが、これは、取り込み責任者を明確にすることか。

A　取り込み責任者を明確にする目的だけでなく、改ざんや成りすましを防止するため、また、作業内容の正確性についての説明責任を果たすために実施するものです。

Q－６７　「改ざんを防止するため情報が作成されてから、または情報を入手してから一定期間以内にスキャンを行うこと。」とあるが、“一定時間以内”は、どれくらいか。
（外来診療の場合、１日の診療が終わった後に、まとめて行なうなどの運用でもよいか）

A　原則は 24 時間以内です。ただし深夜に来院し、次の日が休診である場合などは営業日として 24 時間以内となります。

Q－６８　「緊急に閲覧が必要になったときに迅速に対応できるよう、保存している紙媒体等の検索性も必要に応じて維持すること。」とあるが、どのようなケースで、どれくらいの対応時間内で行う必要があるのか。
　また、通常の診察業務では参照情報として使用しない紙原本の保管方法については、患者別のフォルダで保管する必要があるのか。あるいは帳票ごと、日付ごとなどで一括保管する方法でもよいのか。

A　運用の利便性のためにスキャナ等で電子化を行うが紙等の媒体もそのまま保存を行う場合、電子化した情報はあくまでも参照情報です。
　緊急時とは、例えばシステムダウン等が想定できます。また、一般に「診療のために直ちに特定の診療情報が必要な場合」とは継続して診療を行っている

場合であることから、患者の診療情報が緊急に必要になることが予測される場合は、原本である紙媒体の閲覧を診療に差し支えない範囲で対応できることが必要です。
　なお、通常の診察業務では参照情報として使用しない紙原本の保管方法ですが、検索性を担保しているのであれば、特段の定めはありません。

Q－６９　医療情報を電子化するにあたって定められた要件は何か。

A　「Q－２３」のAを参照してください

Q－７０　災害等で電子システムが運用できない場合で、一時的に運用した紙データを後から電子システムに反映させることは真正性の観点から問題にはならないのか。(システムへの入力時のタイムスタンプが有効になるのではないか)

A　「Q－３１」のAを参照してください

Q－７１　部門系で発生する記録等は、ガイドラインで言う診療録等としての適用を受けるのか。

例えば、エコー検査の紙画像や心電図の紙波形結果など、院内で発生した文書（ワープロやシステム出力）で、かつ手書き情報の付記がなければ、スキャニングして電子化情報を原本とし、元の紙は廃棄できるのか

※　スキャニングする際、「どの患者の結果で、誰が、いつ記録したか」は登録することを前提。

※　紹介状や同意書など、外部からの文書や押印して初めて効力が発生する文書は、紙を原本として残すのが原則。

上記の場合、診療録等として、確定することになるのは、どの行為の時になるのか

スキャニング時の作業責任者と情報作成管理者は、どのようになるのか

また、情報作成管理者は、有資格者等である必要があるのか

手書きの付記などがある場合は、どのように行えばよいのか

A　「Q－４２」のAを参照してください

Q－７２　掲示以外の周知方法はどのようなものがあるか。

A　「Q－５６」のAを参照してください

「10　運用管理について」関係

Q－７３　医療施設がこのガイドラインに基づき、診療録等の電子媒体による保存の運用管理規定を作成し、その規定に沿って運用している場合において、このガイドラインの「C.最低限のガイドライン」を満足していない項目があった場合、問題となるのか

A　例え手段が異なっていても、ガイドラインの趣旨を踏まえて同様な効果を発揮するように実施することが求められます。「C.最低限のガイドライン」を満足していない状態で、なんらかの問題が発生した場合は、安全管理上の必

要な措置を行っていないと見なされる可能性があり、少なくとも、行っていないことの理由の説明を求められます。

「付則」関係

Q－７４　掲示以外の周知方法はどのようなものがあるか。

A　「Q－５６」のAを参照してください

「付表」関係

Q－７５　医療情報システム導入に際して規程等を作成したいがどのようなものが望ましいのか。

A　個人情報保護方針については、「6.1 方針の制定と公表」において個人情報保護対策の制定について説明があり、「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」の6．医療・介護関係事業者が行う措置の透明性の確保と対外的明確化、に要求事項が記載されていますので、参照してください。運用管理規定については、「6.3 組織的安全管理対策（体制・運用管理規程）」において運用管理規定についての説明があり、運用管理規定については付表に作成例が掲載されておりますので参考にしてください。

Q－７６　付表に記載されている文例は全くこのとおりにする必要はないということか。

A　必要ありません。文面は、医療機関等の実情に応じて変更して下さい。

資　料　4

個人に医療情報を提供する際の医療機関等においてなされるべき配慮
及び
医療情報を公益のために利用する際に検討すべき事項

医療情報ネットワーク基盤検討作業班

1　医療機関等による個人への医療情報提供の位置付け

平成 18 年 1 月に発表された「ＩＴ新改革戦略」において「2010 年度までに個人の健康情報を「生涯を通じて」活用できる基盤を作る」ことが目標の一つとして掲げられた。このことと相俟って、地域医療連携等の促進の一環として、個人が自己の健康情報を安全・安心に蓄積し、かつ、参照できるシステムを提供することにより、個人の健康に対する意識の啓発や、健康づくり事業等への参加の動機づけとなること等が期待されている。また、それら情報を個人のコントロールの下、医療従事者の間で必要に応じて共有することにより、一層効果的な健康サービスの実現を目指すといった取組が各方面で進捗中である。

個人が利用する健康情報のうち、医療機関等から提供される医療情報は有用である一方、機微な情報であることから、その保護には細心の注意が必要である。そのため、医療機関等による個人への医療情報の提供について、一定の整理をしておく必要があると考えられる。

「医療情報システムの安全管理に関するガイドライン（以下「ガイドライン」という。）」では、医療情報を外部の者に伝送する場合、個人情報保護法上その形態には、委託（同法第 22 条関係）と第三者提供（同法第 23 条関係）の 2 種類があることを示し、それぞれの形態における情報保護責任のあり方を示した。
しかし本紙で述べる個人への医療情報の提供は、本人の求めに応じて本人に提供されるものであり、委託（同法第 22 条関係）や第三者提供（同法第 23 条関係）のいずれにも当たらない。本人の求めに応じて本人に提供された情報は、個人情報保護法の観点で考えれば、医療機関等が責任を負うことはないといえる。

また同法 25 条に「開示」が示されているが、これは診療記録そのものを開示することを示し、診療情報等の「提供」とは一部異なるものである。
診療情報の開示と提供の違いについては、「診療情報の提供等に関する指針の策定について（医政発第 0912001 号平成 15 年 9 月 12 日厚生労働省医政局長通知）」に詳しいが、診療情報の提供とは「具体的な状況に即した適切な方法」で患者等に情報提供するとされており、必ずしも診療記録そのものを開示することではない。

医療機関等が行う情報提供には、医療機関間のいわゆる紹介状の他、患者に

対する診療情報提供があり、前者には診療情報提供料として診療報酬上の評価があり、後者は「療養の給付と直接関係ないサービス等の取扱いについて（保医発第0901002号平成17年9月1日厚生労働省保険局医療課長・厚生労働省保険局歯科医療管理官通知、平成17年10月1日一部改正）」により、患者から一定の手数料を徴してよいとされている。このことから、患者への情報提供は、医療または医療に関係するサービスであると位置づけられる。

こういった医療機関等で行われる行為の多くには患者に対する「善管注意義務」が求められるという観点から、個人に医療情報を提供する際の医療機関等においてなされるべき配慮について明らかにしておく必要がある。

2　医療情報の提供に関する医療機関の責任について

先述したとおり、本人への医療情報提供は、個人情報保護法上の第三者提供に当たらない。しかし、患者本人の情報保護を目的とするという点に鑑み、「『医療情報システムの安全管理に関するガイドライン』4.2.2　第三者提供における責任分界」の考え方を参考とすべく「第三者」を「本人」と読み替えての援用を試みると、

①本人が何らかの目的で医療情報を利用するために行われるものであり、原則として医療機関等の管理者にとってはその提供の正当性だけが問題となる。
②適切な本人への提供がなされる限り、その後の情報保護に関する責任は医療機関等の管理者から離れることになり、提供を受けた本人に生ずる。
③ただし、例外的に、本人ないしは本人の求めにより提供される先で適切に扱われないことを知りながら情報提供をするような場合は、提供元の医療機関等の責任が追及される可能性がある。

ということになる。

したがって、適切な提供である限りは、その後の責任は本人にあり、個人情報保護法上は、個人における情報の取扱においてまで医療機関等が責任を負わねばならないとは言えない。

しかし患者が情報の取扱等に精通しているとは限らないことから、患者に対しての善管注意義務を果たすという点からは、医療機関等としては患者の不利益にならないような情報の取扱や、前章で述べたような効果を見出しうる診療情報の活用方策等について助言するよう努めることが望ましい。

これは③に関係するが、医療機関等に求められる公共性の高さと併せて考えると、責任の追及とはいえないまでも医療機関等に対する不信を招いてしまう等のことは充分に考えられる。

また、ガイドラインではこの後、

『医療情報が電子化され、ネットワーク等を通じて送受信して情報を提供する場合、第三者提供の際にも、医療機関等から受信側へ直接情報が提供されるわけではなく、情報処理関連事業者が介在することがある。この場合、いつの時点で、第三者提供が成立するのか、すなわち情報処理関連事業者との責任分界点の明確化と言うべき概念が新たに発生する。』

『第三者提供の主体は送信側の医療機関等であることからみて、患者に対する関係では、少なくとも情報が受信側に到達するまでは、原則として送信側の医療機関等に責任があると考えることができる。その上で、情報処理関連事業者および送信側との間で、前項にいうところの善後策を講ずる責任をいかに分担するかは、予め協議し明確にしておくことが望ましい。』

と続くのであるが、これについても「本人」と読み替えての援用が可能である。

地域における医療連携基盤において、このような対患者関係が発生する場合においては、その取組全体を通じて関係者間で予め協議し、それぞれの地域の実情に応じた規約等を定める等により、責任の在り方等について明確にしておくことが望ましい。

3　医療機関においてなされるべき配慮

前述の通り、個人情報保護法上は、適切な提供がなされた限り、個人における情報の取扱においてまで医療機関が責任を負わねばならないとは言えないが、患者に対する関係においては医療機関に善管注意義務が求められる。

適切な提供とは、本人の請求に基づいて、誤りなく本人に情報を提供することを指し、例えば、誤って同姓同名の他人に情報を漏示してしまうことのないように、情報を提供する相手が本人であることを確認する、何らかの認証が必要である。

その反面、例えば、頻繁に来院する、よく顔を見知った患者にまで厳格すぎる認証手続を要求するのは、本人の医療情報の活用の妨げにもなりかねない。

IT を用いて医療情報を提供する場合にあっては、対面による閲覧や書面の交付などに比べて、万が一、情報が漏えいした際の被害が甚大化するおそれや、その被害救済が困難となることに十分な配慮がなされなければならないが、地域における特性なども踏まえながら、医療機関等や患者を含めた地域連携などの関係者の合意によって信頼関係が形成されるべきものであり、それに基づいた適切な認証方法が定められるべきである。

また、本人確認の適切な認証方法を定めることは、原則、本人からの情報提供の請求を受け付ける際の手続きを定めることになるが、何らかの事情で本人が請求手続きをとれない場合などにおいて、それを代理する者による手続きも認められることになる。そのため、それに伴う何らかの慎重な措置も必要になることに留意が必要である。

4　公益のための医療情報の活用

ここまでは、本人が本人の医療情報を本人のために活用する場合の情報保護の考え方について整理してきたところであるが、診療情報は当該個人のために活用されるのみならず、公益に資するものとして活用される場合がある。

医学教育や臨床研究、防疫等の行政や、疫学研究はもとより、医療機関においては日常の診療報酬請求や、監査、評価等を受けるに際しても、診療情報が用いられる場合が想起される。

完全に個人の識別を不可能にしても意義を失わない、すなわち完全に匿名化しても有用に活用できる場合もあるが、特に情報の二重取得を防がねばならない場合や、一定期間における時系列の医療情報が不可欠となる場合などは、情報の蓄積や伝送に際して個人の識別不可能にする等の匿名化を施す必要がありながら、ある時点では連結可能にしておかなければならない場合が想定される。

これについて、医学研究等の具体的な場面を想定した個々事例における個人情報の保護方策として匿名化に言及し、その具体的手段等について明示した指針等があるが、今後、本人を含めた社会基盤としてより広範にかつ多様な医療情報の活用が進むとすれば、匿名化の在り方についても、関係者間の一定の理解を等しくしておくべきであろう。

一定の理解とは、例えば、以下のような論点が考えられる。
- 「匿名化できている」状態とはどのような状態を指すべきか
- 匿名化された情報を誰が何に使うのかを如何に評価するか
- 誰が何の権限に基づいてそれを許すのか
- 誰が「連結可能にするテーブル」を保持するのが適当か
- その仕組み全体を保証、評価または検証等する仕組みをどうするか
- そのような仕組みを講じたとしてもなお、何か不都合な事態が生じた時の責任の所在をどうするか

また、これらの議論を経た上で、個人識別性を有した情報を入手して自ら匿名化の措置を施す場合と、既に匿名化された情報の提供を受ける場合との、それぞれの責任の在り方について、一定の理解を等しくしておくべきである。

医療情報の持つ公共性と、個人のプライバシーとの間の適切なバランスを保持し、個人情報の保護を果たしながら公益に資する医療情報の活用を実現させるために、個人の識別をどの程度可能にしたまま保護方策を講じるかについては、このような一層の検討が必要であると考えられる。

資　料　5

個人が自らの医療情報を管理・活用する基盤を構築する際に必要となる医療従事者の認証方式について

医療情報ネットワーク基盤検討作業班

1. 検討の経緯

近年、情報技術の進展に伴い、個人が自らの健康情報を、自らの健康のために電子的に管理・活用することが可能になってきており、IT 戦略本部においても「個人による健康情報の集積・予防医療等への活用の推進」として「個人が自ら健康情報を管理し健康管理等へ活用するための仕組みの確立」が掲げられている。

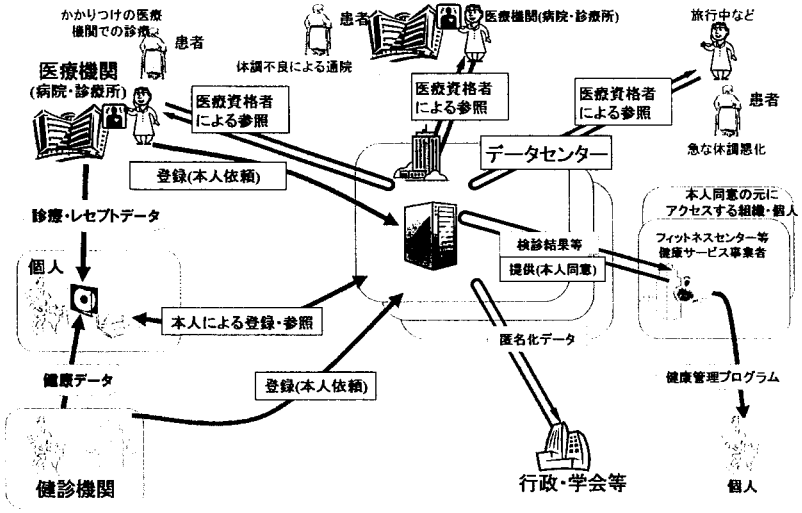
このような動向に対して、医療情報ネットワーク基盤検討会では作業班を設けて、個人自らの健康情報の管理・活用の視点から想定されるユースケースを洗い出し、医療の現場を見据えた議論を行ってきた。

議論に際しては、地域医療連携等において、医療機関等が医療情報を含む健康情報を安全に共有する際に必要な認証機能の要件や認証ポリシの必要性について検討してきたほか、個人が自らの医療情報を管理活用する方策や、その際に求められるセキュリティ等技術的要件について、検討を重ねてきた。その中でも、医療従事者が患者等の医療・健康情報にアクセスする際に必要となる認証方式については、集中して検討が必要と認識された。

2. 検討の前提と医療従事者認証の必要性

2.1　想定する環境

今回の検討は、図 1 に示す通り、個人が健診、レセプト、医療機関等からの情報提供などを通じて入手した自らの医療情報を含む健康情報を、自治体、民間などが運営するデータセンターに自らの希望で保存して管理し、必要に応じて本人、もしくは本人の委託を受けた医療従事者等が参照を行う環境が構築されていることを想定する。



(図 1)

2.2 想定するユースケース

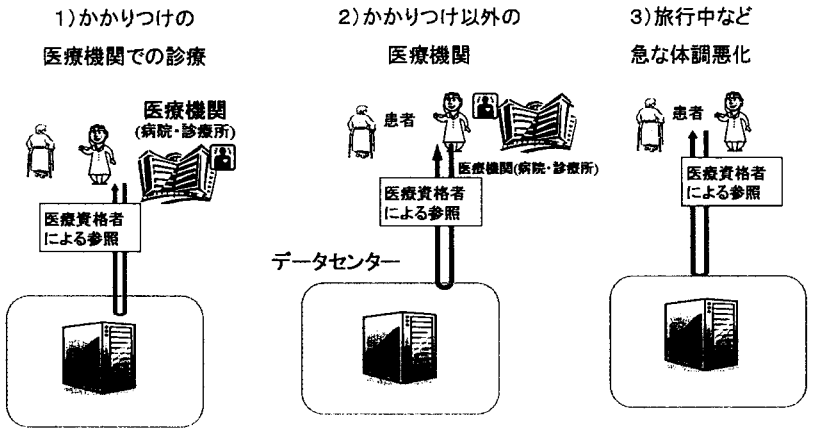
全体としては図 1 のような広範な環境を想定するが、今回の検討は図 2 のような、医療分野に限定した環境を想定する。具体的なユースケースとしては、個人が自らの希望で蓄積した医療情報を含む健康情報を、本人の診療目的のために、国家資格を持つ医療専門職が参照するケースとする。

この際、参照するケースとしては、更に以下の 3 パターンを想定する。

①かかりつけの医師が、患者の医療・健康情報を患者の同意のもと参照する場合。

②かかりつけの医師ではないが、医療機関を受診した患者の医療・健康情報を患者の同意のもと、もしくは緊急に参照する場合。

③医療専門職が旅先などでたまたま居合わせた急病人に対しケアをする際に、患者の同意のもと、もしくは緊急に患者の医療・健康情報を参照する場合。



(図 2)

2.3 医療従事者認証の必要性

今回想定したユースケースでは、いずれも患者の医療・健康情報にアクセスし、情報を参照しなくてはならない。この場合、医療情報を含む健康情報は機微な個人情報であるため、許可された者のみが参照する仕組みが必要であるが、緊急時、特に本人の意識が清明でない場合においては救命活動を優先して行う必要があり、何らかの緊急時の情報参照の仕組みが必要となる。本人同意なしに情報を参照する場合、少なくとも医療の専門家（国家資格保有者）であることが担保されていなくてはならない。更に、医療分野においては、特定の医療専門職のみにしか許されていない医療行為がある。このことから、どの医療専門職であるかどうかを判別することは非常に重要である。また、ユースケースによっては、医療専門職ごとにアクセスできる権限が異なることが想定されるため、ユースケースごとのアクセス条件に応じたアクセス権の付与を行う仕組みが必要になる。

従って、当該医療行為を行うために必要な資格を保有しているかどうかを判断し、機微な個人情報へのアクセスの基本要件とすることは医療分野における必要条件である。

この資格という属性を判断し、アクセスを許可する仕組みを属性認証と呼び、実現する方策のひとつとして公開鍵基盤（PKI：Public Key Infrastructure）がある。

今回想定したユースケースでは、このPKIを活用した医療従事者の認証が有効であり、また、必要でもあるとの認識から検討を進めた。

3. 医療従事者認証に必要な要件

3.1 本人性の確認

資格（属性）の確認の前の大前提として、まず非対面で情報がやり取りされる電子世界の中で、本人が本当に本人であるかを確認しなくてはならない。本人が本人であることを「本人性」と言う。

この、本人性を確認する方法として、厚生労働省の「医療情報システムの安全管理に関するガイドライン」では、記憶（パスワード等）、生体認証（指紋、静脈等）、物理媒体（ICカード等）の三つの要素を示しており、このうちの二つの要素を組み合わせた確認方法（二要素認証）を要求している。

本人性確認方法としてさまざまな認証手段があるが、認証する側は、これらの手段で認証のために使われる情報が確かであることを、何らかの形で管理、運用しなければならない。

単独の医療機関内に限定された環境では、それぞれが独自にルールを決めて採用すればよいが、今回想定する環境においては、全国いずれの場所からでもアクセスできなければならないため、全国共通の本人性確認ルールが必要となる。全国共通の本人性確認ルールを策定する場合は、全国的な規模においても信頼できるスキームを構築する必要がある。

生体認証やパスワード管理を全国統一で実施するためには、全ユーザーの個人情報を統合管理し、維持する必要があるため、一定の安全性を確保し、可用性を担保するための仕組みを構築することは難しい。電子政府や公的個人認証基盤においてPKIが採用されているように、安全性の定量的な担保という点においてはPKIが有効な手段として認識されている。また、PKIをICカードに格納することにより、PKI利用時にパスワードによる確認を行えるため、ガイドラインの要求する二要素認証（物理媒体+記憶）を満たすことが可能である。

3.2 役割をベースとした属性認証

医療分野においては、資格を保有しているかを判断し、個人情報へのアクセスを許可する仕組みは必要条件であることは既に述べた。ただし、医療行為の実施や患者個人情報へのアクセスに関連する業務アプリケーションに対する、より厳密なアクセス制御を行う場合には、医療専門職の役割に応じた属性認証が必要になる。例えば、「医師」と「看護師」では患者個人情報にアクセスできる範囲が異なるかもしれない。

従来は、各医療機関内や地域内で独自の属性認証の仕組みを個別に構築していたため、施設間や地域間での互換性がない状況であったが、今回想定するユースケースにおいては全国共通の認証基盤が必要となる。

4 認証用HPKI環境の構築

4.1 署名用HPKIフレームワークの適用

医療分野においては、署名用PKIとしてヘルスケアPKI（以下HPKI）が構築されている。HPKIであれば、一つの証明書検証で、HPKI認証局が信頼されていれば全国どの組織においても本人性と属性（国家資格）を一度に確認できる。

これを認証フレームワークに適用すると、国家資格という全国共通の属性を各地域で管理する必要がなくなる。すなわち、国家資格の保有について、ルート認証局が信頼点となり保証する環境が構築されれば、異なる地域に属する組織間において属性が担保される。この環境を、現在の署名用のHPKIと区別するために認証用HPKIとする。

認証用HPKIは、既存の署名用HPKIのポリシを証明書の発行ルールに流用可能であるため、最小限の検討によってフレームワークを構築することが可能である。

ただし、実際の発行に当たっては、現在、署名用証明書の発行を行っている諸団体との調整が必要になるため、運用方式や連携方法などについて検討を行う必要がある。

4.2 地域ごとに国家資格管理を行う場合のデメリット

仮に、属性認証に認証用 HPKI を利用しない場合、各地域で各人の国家資格保有の有無を確認し、管理する必要が生じる。利用者は地域ごとに国家資格保有証明を個別に行わねばならなくなる。これは運用管理者にとっても、利用者にとっても非効率的であり、全国共通の確認スキームがあればこの問題は発生しない。

5. 認証用 HPKI の適用範囲の検証

5.1 想定ユースケース以外の認証用 HPKI の活用

認証用 HPKI が構築された場合には、今回想定したユースケース以外にも、地域連携や院内の病院情報システムなどにおける認証に活用が検討されることも想定される。例えば、地域連携システムにおけるアクセス制御に利用することや、医療機関の病院情報システムのアクセスに利用するなどが考えられる。

その場合、地域や院内で配布する認証用のカード等を、認証用 HPKI から配布されるカードで代用でき、情報システム構築コストを低減できる可能性がある。

ただし、認証用 HPKI が提供するフレームワークのみでは、利用者の本人性、実在性、および医療専門職としての国家資格の有無しか担保できないため、実際の運用には不十分である。従って、認証用 HPKI は本人性、実在性、国家資格の有無の確認のみに限定し、地域連携や院内システムにおける国家資格以外の属性を含めた認証要件は、要件を明確にし、システム側で適切な管理・運営を実施しなくてはならない。また、認証用 HPKI のフレームワークを利用する際に生じるリスク（認証局が保証する保証範囲を超えた利用を行う場合の責任のあり方等）などについて分析を行い、必要な運用管理規定や認証ルールを追加構築する必要がある。

5.2 各地域等における独自システムに対するアクセス制御

各地域等において構築される地域連携システム等における個人情報へのアクセスにおいては、業務ごとに国家資格以外の属性を含めたアクセス制御が求められる。その場合、各地域等における業務システムやアプリケーションは独自の属性のコントロール（独自の属性定義とその管理）を必要とするため、全国共通で管理すべき属性と各地域等において管理すべき属性を分けて考える必要が生じる。

医療分野においては認証フレームワークとしてISOやHL7などで役割ベースのアクセス制御の国際標準化が進んでおり、役割をベースとしてアクセス権を設定することで、様々な利用シーンにおけるアクセスを可能にする仕組みが提唱されている。各地域等において属性を独自に定義する際にはそれら国際標準を参考にすべきである。

5.3 各地域の自由度を確保した認証フレームワーク構築

各地域が個々に管理するには煩雑で、全国共通の基盤で管理するほうが利用者、管理者にとって有利なものを全国共通フレームワークとすべきである。地域の独自性を許容し、地域の特性に応じた認証基盤を構築するためには、全国的に担保するのは認証用 HPKI において担保される、「本人性、実在性、国家資格」までとし、それ以外の役割ベースの認証基盤は、地域等ごとにルールを決めて構築するのが現実的である。

医療分野において各医療情報システム間の相互接続を意識した認証フレームワークの検討が IHE や HL7 において行われている。これらの認証フレームワークにおいては、本人確認のベースとして PKI を利用することが可能であり、今回検討を行っている認証用 HPKI も利用可能である。本人性、実在性、国家資格を認証用 HPKI で担保し、それ以外の属性の管理を上記の認証フレームワークで管理することで、全国共通の信頼スキームと、地域ごとの自由な認証フ

レームワークの構築が両立できる。

5.4 地域ごとの認証フレームワークの相互運用性

認証用 HPKI の適用範囲については、地域や院内等で活用する場合、「本人性、実在性、国家資格」の確認までとすべきである。

ところが、各地域が提供する認証フレームワークには、全国共通のユースケースと地域独自のユースケースが存在することもある。この場合、全国共通のユースケースにおいては本人性、国家資格をベースとしたアクセス制御を実施し、地域独自のユースケースにおいては地域が設定した役割をベースにした属性を規定することで、全国共通のユースケースにおいては一定レベルの相互運用性が確保される。

しかし、地域独自のユースケースにおいても特定地域間において情報共有を行うなど、全国共通のユースケースよりも高度な属性管理を地域間で担保したいニーズも想定できる。その際に地域間の相互運用性を担保するためには、各地域が定義する役割が相互に解釈可能でなければならない。相互に解釈可能にするためには、属性を表現する用語やコードを合わせることでも対処できるが、全国共通の属性定義は地域間の調整が困難になることが予想される。そのため、地域独自で定義した属性について、組織的役割を機能的役割にマッピングし、機能的役割をベースにした認証ポリシを構築することが必要となる。また、各地域等が発行した属性について相手方が信頼できることが必須となる。

6 その他の検討項目

6.1 署名用証明書の認証用途での利用

新たに認証用 HPKI を整備しなくても、署名用 HPKI を利用して認証する方法も存在する。

この方式は、署名用証明書を使って署名付チケットで認証する方法であるが、署名付チケットの有効期限が長期間でなければ可用性に問題（チケットに署名する際に GUI 等で署名対象を確認することならびに PIN 入力が必須）となる。

また、チケットを長期利用する場合はチケットの偽造対策など別のセキュリティフレームワークが各地域において必要になる。

また、署名用証明書は実印と同等の効力を持っているため、悪用されないための配慮を十分に行う必要があるが、認証用途で利用する場合、署名用途専用で利用するのに比べ、利用機会が増大するため、悪用される機会も増大する。

6.2 認証用 HPKI の適用範囲とは異なるユースケース

例えば、保険情報などの個人情報に保険請求目的等でアクセスするユースケースが存在する。被保険者証の資格確認や地方公費における確認作業などが代表例としてあげられる。

この場合、利用者は医療専門職ではなく、一般の医事課職員等であることが想定されるため、ここで検討した認証用 HPKI のフレームワークの適用は難しい。この様なユースケースでは、医療機関等に対する職責認証の機能を持つ、職責認証のためのフレームワークが別途必要になる。つまり、認証用途に違いはないが、認証するターゲットが医療従事者個人ではなく、医療機関の医事課職員というような職責となり、医事課職員が「誰か」が問題ではなく、「医事課職員」が認証の対象となる。

この様なフレームワーク構築に当たっては施設の実在性を確認し、施設に対して必要な数の職責に対する認証権限を発行することとなるため、認証用 HPKI を転用することは好ましくない。認証用 HPKI とは異なる別の認証フレームワークの作成が必要となる。

7 結論

これまでの検証結果より、以下のように結論を述べる。

- 想定するユースケースにおいて本人性、実在性、国家資格保有を確認できる全国共通のフレームワークは有用であり、09 年度以降に具体化に向けた検討を行うことが求められる。特に認証ポリシの検討、運用方式の検討、署名用

HPKI 発行主体との連携などについて検討を行う必要がある。

・ 認証用 HPKI の環境を構築することで、地域連携システムや院内の医療情報システムにおける認証部分の構築コスト低減や標準化、共通化を促進することができるため、個人が医療情報を活用する事例以外のユースケースにおいても有効である。利用にあたっては各地域等において個別に運用ルールなどを構築する必要があるが、構築できれば地域等ごとの自由な認証フレームワークに活用できる。この点においても認証用 HPKI を推進すべきである。

・ 署名用証明書の認証用途への利用は不可能ではないが、安全性、可用性の観点からは積極的には推奨できない。また、上記の 2 点において認証用証明書の有用性が確認できるため、あえて署名用証明書を認証用途に利用するよりは、認証専用のフレームワークを構築するほうが社会インフラを提供する観点からは望ましい。

・ 国家資格をもつ医療専門職の本人性・実在性・国家資格を認証する仕組み以外の認証フレームワーク構築の必要性も考えられるので、継続して検討を実施する必要がある。