別　紙

# 「医療情報システムの安全管理に関するガイドライン　第4.3版」に関するQ&A

平成２８年　８月



※下線部を付したところが今回追加したところ

## 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 他の医療機関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「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　以下「施行通知」という。）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、他の医療機関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。

Q－４　このガイドライン通りにシステム構築をしていても起こった事故について、責任のあり方をどのように考えるべきか。

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。技術的なことだけではなく、運用を含めた安全対策を示したものであり、ガイドラインを順守していたと認められる状況下で起こった事故については、一定の法的責任を果たしていたというこ

とが可能であると思われます。しかしながら、その事故によって患者等の第三者が不利益を被った場合は、すべて免責されると言えない可能性もあります。情報システム運用時の責任についての考え方が第４章に記述してありますのでご参照下さい。

Q－５
①旧版のガイドラインを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適宜見直すこととしております。

Q－６
① 「C.最低限のガイドライン」さえ措置すればよいのか。
② 「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
① 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。
② 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。

Q－７
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　本ガイドラインは、個人情報保護法及びe-文書法が医療分野において執行される際の指針となるもので、医療情報を取り扱う際の法令の執行基準となります。

ガイドライン自体に罰則があるわけではありませんが、ガイドラインに違背した状態は、法令を遵守していないと見做される可能性は十分にあります。

ガイドラインのC項は、法令により要求されている事項が列挙されているため、これに違背することにより、個人情報保護法、e-文書法に求められる要件を満たすことができていないと認められる場合、医療に関係する多くの法令等に違反したとされ、その罰則が適用される恐れがあります。

Q－8　診療所においても、大規模な医療機関と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を通じて、講演会で解説が行われることがあります。

## 「3　本ガイドラインの対象システム及び対象情報」関係

Q－１０　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。）、施行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－１１　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－１２　「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　「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－１３
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求められています。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、それらの特徴と扱い方について理解していることが重要です。

Q－１４　委託と第三者提供の情報管理責任上の違いは何か。

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－１５　第三者提供が成立する時点はいつか。

A　第三者提供は原則本人の同意のもとに情報が第三者に移動し、説明責任を含む管理責任が第三者に生じることを指します。したがって第三者が明確に自己の管理範囲に情報が存在することを確認した時点が、第三者提供が成立した時点になります。したがって何らかの方法で受領確認を行う必要があり、受領確認がなされた時点と考えることができます。

オンラインで情報を送付する場合も同様で、たとえば相手のデータベースに格納されたことを電子的に確認する手続きを明確にした上で、その確認をもって第三者提供が成立することを契約等で同意することが必要です。送り手が送

付したと思い、受け手が受領したと思っていないと言った責任の空白ができないようにする必要があります。

## 「5　情報の相互運用性と標準化について」関係

Q－１６　「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、計画的にベンダに要求していくことが望まれます。

Q－１７
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
① 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に、使用されているコードや用語が標準的でないと、適切な情報交換が難しくなります。また、システムをリプレイスする場合も、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。
② システム更新時のデータ移行に伴う作業によって、見読性、真正性の責任が果たせなくなることがあります。

Q－１８　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、保証はされません。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－１９　外字の使用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－２０　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指針が「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」に記載されており、真正性、見読性、保存性があります。さらに、紙媒体の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」に記載されています。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－２１　ウイルス対策等が大変なので、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 ポートなどを利用する場合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、ガイドラインをご参照ください。

Ｑ－２２　「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－２３　「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　明確な基準はありませんが、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、明確な規程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－２４　「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　情報システムを導入していない場合にも行われているように、外来やナースステーションでは患者や家族の入退はあるものの、その事実をカルテ等に

記録することにより来訪を記録できます。

Q－２５　「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　パスワードファイルが盗まれる等で、無制限に繰り返して解析が可能であれば、８文字のパスワードは数時間～１０数時間で破られることは良く知られています。ここで「８文字以上の文字列が望ましい」としていますが、パスワードファイルは盗まれることなく、また３回パスワードを間違えると、一定期間入力できないなどの対策が取られていることが前提です。この対策の程度によって、安全と見なされる文字数や同じパスワードを使い続けて良い期間が変わります。少なくとも８文字で、長くても２ヶ月以内に変更、としていますが、ガイドラインではパスワードだけによる認証は推奨しておりません。理由は前述のように、パスワード入力時の繰り返し解析を防止する対策が不十分であったり、いくつかのパスワードを循環させて使うなどの運用上の脱ルール行為があれば、安全とは言えないからです。できるだけ早く２要素以上の認証を組み合わせることを推奨しています。

Q－２６　「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－２７　「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　当該情報機器が個人情報を記録しているか否かで取り扱いが異なります。
　個人情報を記録している機器や媒体であれば持ち出しには細心の注意が必要です。このような機器や媒体は、原則として持ち出すべきではないという基準にすべきです。その上で、やむを得ず持ち出す際には、情報機器を持ち出す

必要性や漏洩リスクを総合的に判断したうえで、運用管理規定などに機器持ち出しの許諾ルールと判断基準を策定することが大切です。また、持ち出す機器については、6.9 項に示す適切な防護措置を施すことが必要です。

リモートサービスなどにより医療機関の情報にアクセスすることが可能な機器の場合、個人情報を機器に記録していなくても、機器そのものの盗難や置き忘れが情報漏えいのリスクになります。このような場合、機器に対する防護措置に加え、リモートサービスそのものでの防護措置が必要であり、6.11 項に示された安全管理対策が実施されていることが条件になります。

上記以外の情報機器については、機密情報の有無やその他要件を考慮し、医療機関における管理ルールを策定してください。

Q－２８　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－２９　医療情報を交換する「オープンなネットワーク接続」として SSL/TLS を用いることは可能か。

「電子処方せんの運用ガイドライン」では、ASP サービスを用いた仕組みとして、Web サービス利用時における SSL/TLS 接続について詳細に記載されているが、その他のインターネットを介した医療情報システムへの SSL/TLS 接続について遵守すべき事項はあるか？

A　昨今、SSL/TLS についてプロトコルやソフトウェアの脆弱性をついた攻撃の報告が相次いでおり、SSL/TLS を用いても、適切に利用しなければ安

全性を確保できません。
従って「電子処方せんの運用ガイドライン」と同等の対応が必要です。

例えば IPsec による VPN 接続等によるセキュリティの担保を行わず、インターネット等のオープンなネットワークを介し、 HTTPS を用いて医療情報システムに接続する場合は、SSL/TLS のプロトコルバージョンを TLS 1.2 のみに限定した上で、クライアント証明書を利用した TLS クライアント認証を実施してください。
その際、TLS の設定はサーバ/クライアントともに、「SSL/TLS 暗号設定ガイドライン」に規定される最も安全性水準の高い「高セキュリティ型」に準じた適切な設定が必要です。
また、いわゆる SSL-VPN は偽サーバへの対策が不十分なものが多く、医療情報システムでは原則として使用すべきではありません。

Q－３０　「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や通信経路などの状態、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ェ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ェアの作用を避け、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努める必要があります。

Q－３１　「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、
① ソフトウェアは、安全性の確認対象から外れるのか。

② 安全性を確認するための方法は他に無いか。

A

① 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。

② 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－３２ 「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。

また、通信サービスを提供する事業者等に対しては SLA（Service Level Agreement）を確認し、SLA に記載されていない（不足する）部分があれば、その部分について SLA の修正を要請するか、個別契約で対応してください。

Q－３３ 「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－３４　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ことを必要としています。

Q－３５　通常閉じたネットワークで構築することが多い医療機関において、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。