資料1

「医療情報システムの安全管理に関するガイドライン」改定原案について

第30回医療情報ネットワーク基盤検討会

2016/12/21

改定原案のご確認

第4.4版の改定概要

改定の背景

サイバー攻撃の手法の多様化・巧妙化、地域医療連携や医療介護連携等の推進、「IoT(モノのインターネット)」と称される新技術やサービス等の普及等、医療情報システムを取り巻く環境の変化に対応するため、ガイドラインの中で関連する1章や6章を改定するとともに、第4.2版の公表以降に追加された標準規格等への対応等を行う。

改定概要

【1章】・本ガイドラインの対象に、病院、一般診療所、歯科診療所、薬局、助産所、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者における電子的な医療情報の取扱いに係る責任者が含まれることを明確化する。

【3章】・「3.1　7章及び9章の対象となる文書について」に、e-文書法の対象範囲である介護事業者の文書等を追記する。

【5章】・新たに加わった厚生労働省標準規格やJAHIS標準データ交換規約等について追記する。

【6章】・「6.1　方針の制定と公表」、「6.2　医療機関等における情報セキュリティマネジメントシステム(ISMS)の実践」において、規格の更新を受け所要の改定を行う。
また、6.2章に「『製造業者による医療情報セキュリティ開示書』ガイド」(MDS)について追記する。
・「6.5　技術的安全対策」において、利用者の識別・認証については、認証技術の端末への実装状況等を鑑み、約10年後を目処に2要素認証を原則とすることを想定する旨を追記する。併せて、識別・認証に関する考え方を整理する。
また、「(6)医療等分野におけるIoT機器の利用」を設け、IoT機器の利用時に順守すべき事項を規定する。
・「6.6　人的安全対策」、「6.10　災害、サイバー攻撃等の非常時の対応」において、サイバー攻撃等への事前及び事後の対応や連絡先等について規定を設ける。このことに併せ、6.10章を改題する。
・「6.9　情報及び情報機器の持ち出しについて」において、公衆無線LANや個人所有又は個人の管理下にある端末の業務利用(BYOD)の取扱い等、モバイル端末の使用時における順守事項を明確化する。
・「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」において、オープンなネットワークを介したSSL/TLS接続における順守事項や留意点を示す。
・「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」において、C項における「活用するのが望ましい」の記述を「推奨される」に変更する。

【7章】・「7.1　真正性の確保について」において、診療録等の代行入力を時間確定することの取扱いを明確化する。

【10章】・これらの改定に合わせて所要の改定を行う。

上記の改定に加え、分かりやすさの観点から全般的に表現の修正を行い、本ガイドラインが参照している資料について、最新の版に合わせ名称等を更新した。

改定テーマ一覧

第4.4版では、下記の13テーマに沿って改定原案の検討を行ってきた。次頁以降、改定テーマごとに改定内容を説明する。

#	改定テーマ
1	電子カルテの代行入力を時間経過で自動確定することへの言及
2	「製造業者による情報セキュリティ開示書」ガイドVer.2.0への言及
3	モバイルデバイスへの対応
4	標的型攻撃への対応
5	個人情報保護法への対応
6	TLS1.2によるオープンネットワーク接続への言及
7	小規模医療機関が順守すべき項目の明確化
8	医療情報システムの対象範囲の検討
9	IoTセキュリティへの対応
10	2要素認証の採用
11	電子署名の採用
12	わかりやすさへの対応
13	規格変更への対応

1. 電子カルテの代行入力を時間経過で自動確定することへの言及

改定方針

診療録等の代行入力を行う際に、時間経過で自動的に記録確定する運用が認められるかを明確化する。

論点	改定案
論点① 電子カルテ等の代行入力を行う際に、時間経過で自動的に記録確定する運用が認められるか	「7.1 真正性の確保について」C項において、代行入力を行う際は、作成責任者による確認を行わずに確定することは認められない旨を追記する。(P.103)※

※ ( )内はガイドライン改定原案の参照ページを示す。

2.「製造業者による情報セキュリティ開示書」ガイドVer.2.0への言及

改定方針

保健医療福祉情報システム工業会(JAHIS)標準及び日本画像医療システム工業会(JIRA)規格となっている「『製造業者による医療情報セキュリティ開示書』ガイド」(MDS)に言及する。

論点	改定案
論点① 安全管理ガイドラインにおいて、「『製造業者による医療情報セキュリティ開示書』ガイド」(MDS)をどのように取り扱うか	「6.2 医療機関等における情報セキュリティマネジメントシステム(ISMS)の実践」B項において、MDSのチェックリストが情報のリストアップ、リスク分析・対策に役立つ旨を紹介する。(P.40)

3. モバイルデバイスへの対応

改定方針

院外で利用するソフトウェアを限定することや、他のアプリの影響を受けないこと等といった運用や技術的対策について記載する。院内での対応については現行の記述で対応できていると考えられるため、院外での対応を中心に記載する。

論点	改定案
論点① オープンネットワークへのTLS接続に言及したことを受けて、公衆無線LANの取扱いを改めるべきか	「6.9 情報及び情報機器の持ち出しについて」C項に、公衆無線LANは使用できないが、公衆無線LANしか使用できない環境に限って、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の基準に則って使用できることを明記する。(P.67)
論点② モバイル端末の運用について、強調して記述するか	6.9章C項D項で規定されている下記事項を6.9章B項に追記し、強調する。(P.66) ・運用管理規程を設けて管理する。 ・端末に保存されているデータを暗号化する。 ・端末にインストールするソフトウェアを必要最低限とする。 ・公衆無線LANは使用禁止であるが、公衆無線LANしか使用できない場合には6.11章の基準に則り使用できる。 ・個人所有又は個人管理下にある端末の業務利用(BYOD)は原則として行わない。 ・覗き見防止対策を行う。

3. モバイルデバイスへの対応

論点	改定案
論点③ モバイル端末の認証について、強調して記述するか	6.9章C項D項で規定されている下記事項を6.9章B項に追記し、強調する。(P.66) ・盗難、紛失及び覗き見防止のため、必ず端末ロックする。 ・アプリケーション自体にパスワードを設定する。

4. 標的型攻撃への対応

改定方針

サイバー攻撃に関する記述は第2版から存在するが、時勢に沿った改定が必要であり、有事の際を考慮した技術的対策や所管機関への連絡体制や情報共有体制、教育等について追記する。

論点

論点①
サイバー攻撃に対する準備について

改定案

「6.6 人的安全対策」B項において、医療システムが被害を被る具体例にサイバー攻撃を追加する。(P.60)

「6.10 災害等の非常時の対応」B項を下記のように改定する。(P.69-72)
- 医療システムが被害を被る具体例にサイバー攻撃を追加する。
- BCP発動の際に所管官庁等の関係機関に連絡する旨を追記する。
- サイバー攻撃を受けた際の対処項目を追加する。

6.10章C項を下記のように改定する。(P.72)
- サイバー攻撃を受けた際の対処項目を追加する。
- 関係機関の連絡先として、厚生労働省医療技術情報推進室、標的型攻撃への対応支援を行っている情報処理推進機構(IPA)の連絡窓口を追記する。

このことに併せ、6.10章の章題を「災害、サイバー攻撃等の非常時の対応」に変更する。

4. 標的型攻撃への対応

論点	改定案
論点② ランサムウェア等への対応について	6.6章B項に、マルウェア等の感染に備え、数世代分のデータをバックアップすることが望ましい旨を追記する。(P.72)
論点③ 医療機関等の職員への教育・啓発について	6.6章B項において、日本医療情報学会の「標的型メールへの対処について」及びIPAの「対策のしおり」シリーズ等の内容を参考に、サイバー攻撃への対応に関する教育を行うことを求める。(P.60) また、6.10章B項において、6.5章、6.6章の内容を参照し、サイバー攻撃への事前の対策を行うよう求める。(P.72)

5. 個人情報保護法への対応

改定方針

平成27年9月に公布された改正個人情報保護法及びその関連法令に合わせて、本ガイドラインの改定を検討したが、「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」の今後の取扱いを踏まえ、改めて検討を行うこととする。

6. TLS1.2によるオープンネットワーク接続への言及

改定方針

本年8月にQ&Aを改定した件について、医療情報システムの現状に鑑み、情報処理推進機構の「SSL/TLS暗号設定ガイドライン ～安全なウェブサイトのために(暗号設定対策編)～ Ver.1.1」に基づき、適切な設定を行う必要がある旨を記載する。

論点

論点①
TLSによりオープンネットワークへ接続する場合に準拠すべきことへの言及がない

改定案

6.11章C項に、TLSによりオープンネットワークに接続する場合は、「SSL/TLS暗号設定ガイドライン」における「高セキュリティ型」の要求設定に則るべき旨を追記する。(P.92)

また、同B項にTLS1.2によりオープンネットワークに接続する場合の留意事項を追記する。(P.82)

※本ガイドライン第4.4版の発出に併せ、8月に公表したQ&Aの該当部分を削除する。

6. TLS1.2によるオープンネットワーク接続への言及

論点	改定案
論点② セッション間の回り込みのリスクについて	6.11章C項に、ソフトウェア型のIPsec若しくはTLS1.2により接続する場合、セッション間の回り込み（正規のルートではないクローズドセッションへのアクセス）等による攻撃のリスクがあるため、適切な対策を実施すべき旨を追記する。（P.92） 併せて、同B項に下記を追記する。（P.82-83） ・適切な経路設定を行うことで、セッション間の回り込みを回避することが可能である。 ・保健医療福祉情報安全管理適合性評価協会（HISPRO）の「支払基金等へのレセプトオンライン請求用IPsec＋IKEサービス」チェックリスト項目集が参考になる。
論点③ 脆弱性リスクに関する情報収集について	6.11章B項に、セキュリティインシデントの報道や事業者からの情報提供等を通じて、医療機関等がSSL/TLS等の脆弱性リスクについて注意、認識しておくべき旨を追記する。（P.83）

7. 小規模医療機関が順守すべき項目の明確化

改定方針

本ガイドライン付表では、医療機関の規模別に運用管理の実施項目例を示しており、当該付表の内容の見直しや充実化を図る。

論点	改定案
論点① ガイドライン付表における更新範囲	付表1を下記のように修正する。 ・「システム管理者や運用責任者の責務」に外部サービスの利用時の留意事項を追記する。 ・「一般管理における運用管理事項」に、「IoT機器利用に関する事項」を新設する。 ・「技術的と運用的対策の分担を定めた文書の管理規程」にMDSの確認について追記する。 ・「持ち出し対象となる情報及び情報機器の規程」にBYODの原則禁止に係る事項を追記する。 ・「持ち出した情報及び情報機器への安全管理措置」に公衆無線LANの使用禁止と公衆無線LANしか利用できない環境でのみ使用を認める旨を追記する。 ・「自然災害等による非常時の対策」に「サイバー攻撃」を追記し、官公庁の連絡先の確認について言及する。

7. 小規模医療機関が順守すべき項目の明確化

論点	改定案
論点② 付表1の監査に関する記述について	付表1において、③及び⑪の監査に係る記述が重複していることから、③の監査責任者の義務に係る記述を削除し、⑪に集約する。

8. 医療情報システムの対象範囲の検討

改定方針

介護事業者及び医療情報連携ネットワーク運営事業者を本ガイドラインの対象範囲とする。

論点	改定案
論点① 「医療機関等」の範囲の明確化 （介護事業者や医療情報連携ネットワーク運営主体まで含むか）	「1　はじめに」でガイドラインの対象を下記のように修正する。(P.3) ・「病院、診療所、薬局、助産所等における診療録等（「医療機関等」）の電子保存に係る責任者」 →「病院、一般診療所、歯科診療所、薬局、助産所、訪問看護ステーション、介護事業者、医療情報連携ネットワーク運営事業者等（「医療機関等」）における電子的な医療情報の取扱いに係る責任者」
論点② 介護事業者が作成、保存する文書について	「3.1　7章及び9章の対象となる文書について」に、次頁に挙げる文書を含め、介護事業者が取り扱う文書がｅ-文書法の対象範囲でかつ当該文書の内容に医療情報が含まれる場合には、7章、9章の対象になる旨を追記する。(P.15-17)

8. 医療情報システムの対象範囲の検討

介護事業者が取り扱う e-文書法の対象文書(一部)

1. 指定居宅サービス等の事業の人員、設備及び運営に関する基準(平成11年厚生省令第37号)第73条の2第2項の規定による訪問看護計画書及び訪問看護報告書
2. 同 第154条の2第2項(第155条の12において準用する場合を含む。)の規定による短期入所療養介護計画
3. 同 第191条の2第2項及び第192条の11第2項の規定による特定施設サービス計画
4. 指定介護老人福祉施設の人員、設備及び運営に関する基準(平成11年厚生省令第39号)第37条第2項の規定による施設サービス計画
5. 介護老人保健施設の人員、施設及び設備並びに運営に関する基準(平成11年厚生省令第40号)第38条第2項の規定による施設サービス計画
6. 指定訪問看護の事業の人員及び運営に関する基準(平成12年厚生省令第80号)第30条第2項の規定による訪問看護指示書、特別訪問看護指示書、精神科訪問看護指示書、精神科特別訪問看護指示書及び在宅患者訪問点滴注射指示書
7. 指定介護予防サービス等の事業の人員、設備及び運営並びに指定介護予防サービス等に係る介護予防のための効果的な支援の方法に関する基準(平成18年厚生労働省令第35号)第73条第2項の規定による介護予防訪問看護計画書及び介護予防訪問看護報告書
8. 同 第194条第2項(第210条において準用する場合を含む。)の規定による介護予防短期入所療養介護計画
9. 同 第244条第2項及び第261条第2項の規定による介護予防特定施設サービス計画
10. 指定地域密着型サービスの事業の人員、設備及び運営に関する基準(平成18年厚生労働省令第34号)第3条の40第2項の規定による定期巡回・随時対応型訪問介護看護計画及び訪問看護報告書
11. 同 第40条の15第2項の規定による療養通所介護計画
12. 同 第128条第2項の規定による地域密着型特定施設サービス計画
13. 同 第156条第2項(第169条において準用する場合を含む。)の規定による地域密着型施設サービス計画
14. 同 第181条第2項の規定による居宅サービス計画、看護小規模多機能型居宅介護計画及び看護小規模多機能型居宅介護報告書

このほか、e-文書法の対象でかつ内容に医療情報を含む場合は、7章、9章の対象となる。

9. IoTセキュリティへの対応

改定方針

総務省、経済産業省、IoT推進コンソーシアムが策定した「IoTセキュリティガイドライン」等、各種ガイドライン及び医療の現場の状況を鑑み、修正を行う。

論点

論点①
本ガイドラインにおいて規定すべきIoTの考え方は何か

改定案

本ガイドラインでは、情報セキュリティの観点からIoTセキュリティについて記述する方針により改定を行う。

具体的には、「6.5 技術的安全対策」B項に、「(6)」医療等分野におけるIoT機器の利用」を新設し、IoTに関する考え方を下記のように規定する。(P.54-55)

・安全管理ガイドラインにおけるIoTの対象範囲
「IoT機器(センサ等で自動的に情報を取得し、若しくは他の機器が自動的に取得した情報を中継し、ネットワークを通じて他の医療情報システムに送信する機器)によって医療に関する個人の情報を取得し、ネットワークを介して収集する仕組み 」
・IoTの実用例として、下記を記載する。
①医療機関等の内外で用いられる医療機器やバイタルを測定するウェアラブル端末等から患者のデータを収集し、医師の診療支援や経過観察等に活用すること
②医療機関等内における職員の位置情報や動線を分析し、病床や人員の配置等を改善すること

9. IoTセキュリティへの対応

論点	改定案
論点① 本ガイドラインにおいて規定すべきIoTの考え方は何か	具体的には、「6.5 技術的安全対策」B項に、「(6)」医療等分野におけるIoT機器の利用」を新設し、IoTに関する考え方を下記のように規定する。(P.54-55) ・安全管理ガイドラインでは、医療情報の適切な保全を目的としてIoT機器の適切な取扱いに関する要件を定めており、「医薬品、医療機器等の品質、有効性及び安全性の確保等に関する法律」において定める医療機器のサイバーセキュリティの保全については、厚生労働省医薬・生活衛生局が発出する「医療機器におけるサイバーセキュリティの確保について」等を踏まえ、医療機器の製造販売業者と必要な連携を図る。 ・新しい分野であり、今後の動向等を注視すべき旨を記載する。
論点② IoT機器貸し出し時の患者のリスク受容についてどのように規定するか	6.5章B項(6)・C項に、IoT機器を在宅設置等で利用する際には、事前に患者に対してセキュリティリスクに関する説明を行い、リスク受容について合意する必要がある旨を追記する。(P.55、P.58)

9. IoTセキュリティへの対応

論点	改定案
論点③ IoTセキュリティガイドラインと比較し、安全管理ガイドラインにおける対策が十分でないと考えられる規定はあるか	IoTセキュリティガイドラインを踏まえ、下記について安全管理ガイドラインに追記する。 【IoT機器・システムの動作異常の検知について】 下記を6.5章B項(6)・D項に規定する。(P.55、P.59) ・IoT機器を含むシステムの接続状況や異常発生を把握するため、IoT機器・システムがそれぞれの状態や他の機器との通信状態を収集・把握し、ログとして適切に記録する。 下記を6.5章B項(6)に追記する。(P.55) ・IoT機器を含むシステムが単独でログ管理や、暗号化等の対策を行うことが難しい場合、他にログ管理のための機器を用意する等、上位のシステムやサービス全体で対策を行う。 【IoT機器の脆弱性への継続的な対応について】 下記を6.5章B項(6)・C項に追記する。(P.55、P.58) ・システム、サービスの特徴を踏まえ、ファームウェア等、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用する。

9. IoTセキュリティへの対応

論点	改定案
論点③ IoTセキュリティガイドラインと比較し、安全管理ガイドラインにおける対策が十分でないと考えられる規定はあるか	IoTセキュリティガイドラインを踏まえ、下記について安全管理ガイドラインに追記する。 【使用終了後の電源オフについて規定されていない】 下記を6.5章B項(6)・C項に追記する。(P.55、P.58) ・使用終了又は使用停止したIoT機器がネットワークに接続されたままであると不正に接続されるリスクがあるため、電源を切る等、対策を講じる。
論点④ 運用管理についてどのように規定すべきか	6.5章B項(6)・C項にIoT機器の利用に係るリスク分析の実施と運用管理規程の作成に係る規定を設けるべき旨を追記する。(P.55、P.58)

10. 2要素認証の採用

改定方針

2要素認証の原則化について検討するが、医療現場への影響を考慮し、猶予期間を設けて段階的に移行を進めること等も併せて検討する。

論点	改定案
論点① 2要素認証を原則化するか	6.5章B項に、下記を追記する。(P.50) ・現状では、2要素認証の追加実装により医療機関等の負担が増加すると考えられる。このような技術は、本来システムにあらかじめ実装されているべきであり、今後、認証に係る技術の端末への実装状況等を考慮し、できるだけ早期に対応することが求められる。 ・認証技術の端末等への実装状況等を鑑み、約10年後を目途にC項とすることを想定する。
論点② 2要素認証の採用に当たって、医療機関等に過大なコストがかかるおそれがあることから、猶予期間を設けるか	認証技術の端末等への実装状況等を鑑みて、約10年後を目処にC項に移行することを想定する。(P.50)

10. 2要素認証の採用

論点	改定案
論点③ パスワードとバイオメトリクスの組み合わせは認められるか	6.5章B項において、現在のバイオメトリクス機器の精度は、個人を1対Nで識別するには十分でないという考え方が示されており、ユーザIDは必要となる。 現行の記述では上記の旨が読み取りにくいため、6.5章B項に追記すると共に、2要素認証の採用例を紹介する。(P.52)
論点④ ICカード等を使用できない状況における対応について規定するか	現行の6.5章B項の記述を基に、ICカード等のセキュリティ・デバイスが破損した場合等の、緊急時の代替手段による一時的なルールの策定について、6.5章D項に追記する。(P.59)
論点⑤ 管理区域内のモダリティ等をどのように取り扱うか	6.5章B項C項に、情報システムを利用する端末に2要素認証が実装されていないとしても、端末操作を行う区画への入場に当たって利用者の認証を行う等して、入場時・端末利用時を含め2要素以上の認証がなされていれば、2要素認証と同等と考えられる旨を追記する。 (例)・放射線管理区域のモダリティの取扱い ・薬局における薬歴の参照・入力　等 (P.51、P.58-59)

10. 2要素認証の採用

論点	改定案
論点⑥ シングルサインオンをどのように取り扱うか	6.5章B項に、一台の端末でシングルサインオンを用いる場合には、最初のログイン時に2要素認証を行えばよい旨を追記する。(P.51) ただし、一度の認証で複数端末からログイン可能とすることや、ログインしたまま長時間放置するといった運用は認められない。

11. 電子署名の採用

改定方針

平成28年度の診療報酬改定において、電子的診療情報提供書の算定要件に保健医療福祉分野の公開鍵基盤(HPKI)による電子署名の採用が盛り込まれたことに合わせ、ガイドラインの記載の修正を検討する。

論点

論点①
「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」C項において、厚生労働省の定める準拠性監査基準を満たす電子署名の使用が求められ、HPKIを活用することが「望ましい」とされているが、平成28年度の診療報酬改定を受け、HPKIに係る記述を改定するか

改定案

6.12章C項における「活用するのが望ましい」の記述を「推奨される」に変更する。(P.95)

12. わかりやすさへの対応

改定方針

・「医療情報システムを安全に管理するために」(平成21年3月 厚生労働省)や「『医療情報システムの安全管理に関するガイドライン』対応のための手引き」(平成28年3月 デジタル・フォレンジック研究会)等を参考に、医療機関等の管理者の観点で理解を促進できるような読本等を作成する。併せて、医療機関等の管理者の観点で資料を作成することで、理解の促進が可能かをヒアリングで確認し、適宜反映する。
・ガイドライン全体の表現について、再度確認を行う。

論点	改定案
論点① 「医療情報システムを安全に管理するために」の改定範囲	「医療情報システムを安全に管理するために」は4版を基に作成されていることから、4.3版までの改正点と今回の改定について、追記等を行う予定。
論点② ガイドライン本文において参照している外部資料の改訂への対応	ガイドラインが参照している他の資料について、最新の版に合わせて名称・公表月等を修正する。(P.57、P.95、P.129、P.134)
論点③ ガイドラインの文書校正	ガイドラインで用いられている言葉遣いや用語、表記等について平仄をとる。 7章、8章、9章の冒頭に、適用対象を明確にする文章を挿入する。(P.97、P.113、P.128)

13. 規格変更への対応

改定方針

規格変更への対応として、ガイドラインの記載を修正する。

論点

論点①
第4.2版の公表以降に変更された各規格について、本改定でどこまで対応するか

改定案

- 「5.1.1 厚生労働省標準規格」に平成28年3月28日付で追加された4つの厚生労働省標準規格を追記する。(P.33)
- 「5.2 データ交換のための国際的な標準規格への準拠」のJAHIS規格の説明に関する修正を行う。(P.35)
- 「5.3 標準規格の適用に関わるその他の事項」において、日本IHE協会の「地域医療連携における情報連携基盤技術仕様」が厚生労働省標準規格として採択されたことを受け、追記を行う。(P.35-36)
- 「6.1 方針の制定と公表」及び6.2章におけるJIS Q27001:2006の引用をJISQ27001:2014の内容に合わせて修正する。(P.38、P.40)