資料１－１

厚生労働省 ひと、くらし、みらいのために
Ministry of Health, Labour and Welfare

令和３年１２月１７日

# 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について

Ministry of Health, Labour and Welfare of Japan

# 医療情報システムの安全管理に関するガイドラインの改定の背景

医療情報システムの安全管理に関するガイドライン第５．１版（令和３年１月）

医療DX化
サイバー攻撃
等の社会情勢

制度的な動向

- アプリケーション間の連携における認証等に関する考え方の整理
- BYODに関する記載の整理
- タイムスタンプの認定制度の変更
- ２省ガイドラインやその他ガイドラインとの整合性の確保
- 令和２年・３年度改正個人情報保護法への対応

技術的な動向

- 医療機関へのサイバー攻撃の多様化・巧妙化
- 長期署名の参照先の規格の動向
- ガイドラインを確実に遵守できるような記載

「規制改革実施計画（令和３年６月１８日閣議決定）」等への対応

- 電子署名の利用が可能である旨を医師法等の法令を踏まえ、規定する。その際、医療現場のニーズを踏まえ、電子署名の活用促進につながるようなガイドラインの見直しを検討する。
- 医療機関や関係者が電子カルテ等医療情報を授受するに当たって当事者が講ずべき安全措置やセキュリティ対策と併せて、外部ネットワーク等が活用可能であることを分かりやすく周知する。

課題への対応

安全管理ガイドラインの改定（第５．Ｘ版）

# 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に向けた調査一式
# 改定作業班構成員等

| 論点 | 氏名・所属等 |
|---|---|
| 座長・構成員<br>（五十音順・敬称略） | 【主査】<br>山本　隆一　医療情報システム開発センター 理事長<br>【構成員】<br>秋山　祐治　医療ネットワーク岡山協議会 常任理事<br>井上　貴宏　保健医療福祉情報システム工業会電子カルテ委員会委員長<br>小尾　高史　東京工業大学 科学技術創成研究院 准教授<br>門林　雄基　奈良先端科学技術大学院大学 先端科学技術研究科 情報科学領域教授<br>河野　行満　公益社団法人日本薬剤師会 中央薬事情報センター 医療情報管理部 部長<br>武田　理宏　大阪大学大学院 医学研究科 准教授（日本病院会）<br>玉川　裕夫　公益社団法人日本歯科医師会<br>樋口　範雄　武蔵野大学 法学部 特任教授<br>矢野　一博　公益社団法人日本医師会　総合政策研究機構 主任研究員 |
| オブザーバー | • 総務省　情報流通行政局　地域通信振興課　デジタル企業行動室<br>• 経済産業省　商務・サービスグループ　ヘルスケア産業課<br>• 厚生労働省 医政局 研究開発振興課 医療情報技術推進室 |
| 事務局 | • 株式会社エヌ・ティ・ティ・データ経営研究所 |

2021年12月～2022年3月に4回開催予定

# 安全管理ガイドラインの改定の指摘と対応箇所

## ➢ 制度的な動向

| 指摘 | 対応箇所 | 対応方針 |
|---|---|---|
| ◆ **アプリケーションごとに**外部の利用者（自院職員以外）の**認証・認可を行うための考え方**等について整理することが必要（参考資料3） | 6.5章 | ● 現行のガイドラインでは、ご指摘のことに対応する記載はない。<br>● そのため、新項を作成する。左記のご指摘に対応できるように記載を追加する。 |
| ◆ 個人情報の目的外利用や流出・漏洩等への対策を前提とした医療現場におけるスマートフォン等の活用、**BYOD**（Bring Your Own Device）への指摘があることを踏まえ、**記載の検討**が必要（参考資料3） | 6.9章 | ● 現行のガイドラインでは、原則行うべきではないと記載している<br>● しかし、すでにQ＆Aでは、行うべき対策を具体的に示しているため、ガイドライン本文にも記載をする。 |
| ◆ 「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）により、**タイムスタンプを行う認証は、総務大臣の認定業務**となったことに伴う改定が必要 | 6.12章 | ● 制度改正に伴い、記載を更新する。 |
| ◆ **2省ガイドライン**では事業者について、JIS Q 27001及び15001を必須としていることとの**整合性**を検討することが必要 | 8.1.2章 | ● 現場のニーズも踏まえて、検討する。 |
| ◆ **令和２年・令和３年改正個人情報保護法**の施行に向けて、ガイドラインでの対応が必要 | 8.1.3章 | ● 共同利用型の仮名加工情報については、実臨床への影響を考え、Q＆Aに分かりやすく記載する。 |

## ➢ 技術的な動向

| 指摘 | 対応箇所 | 対応方針 |
|---|---|---|
| ◆ 本ガイドラインの記載は、制度的な要求事項を主とし、**技術的な記載や措置は例示として分けて整理すること**、<br>◆ 特に、リスク分析の結果にもとづき、対策を行うべきであり、必ずしも例示の全てを求めるものではないことを**分かりやすく記載**することが必要ではないか。（参考資料3） | ガイドライン全体 | ● 非専門家でも分かりやすい言葉を用いるようにし、記載も工夫する。<br>● 技術的な記載や措置に関しては、別冊を作り、参照できるようにする。 |
| ◆ **ランサムウェアによる被害**により、医療機関等における診療等業務に大きな影響が生じている状況を踏まえて、これに対する注意喚起を行うことが求められると考える。 | 6.10章 | ● ランサムウェアに関しては、現行のガイドラインで記載はない。<br>● ランサムウェアに関して、バックアップデータまで被害が拡大しないよう対策を記載するほか、新項を設けることも含め検討を行う。 |
| ◆ **長期署名方式**についてJIS規格を参照することとしているが、2008年以降改訂されておらず、実務的な影響を生じている。 | 6.12章 | ● 参照先をJISからISOに変更することを、有識者会議で検討し、実務的な影響範囲を確認したうえで、参照先の変更を検討する。 |

# 安全管理ガイドラインの改定の指摘と対応箇所

➢「規制改革実施計画（令和３年６月１８日閣議決定）」等への対応

| 指摘 | 対応箇所 | 対応方針 |
|---|---|---|
| ◆医療機関や関係者が電子カルテ等医療情報を授受するに当たって当事者が講ずべき安全対策と併せて、**外部ネットワーク等が活用可能であることを分かりやすく周知**すべき（参考資料３） | 6.11章 | ● 外部ネットワークへの接続は可能であること、また、その場合に求められる具体的な措置等について、ガイドライン利用者にとって分かりやすい記載とする。 |
| ◆電子署名の利用が可能である旨を医師法等の法令を踏まえ、規定する。その際、医療現場のニーズを踏まえ、**電子署名の活用促進**につながるようなガイドラインの見直しを検討する。（参考資料4） | 6.12章 | ● 「本人確認」と「資格確認」とに分けた上で、それぞれに求められる手続等を整理。<br>● 上記整理の際、認定認証事業者や医療機関による、医師等の国家資格の確認・認証の方法についても検討する。<br>● クラウド型署名を用いる場合に求められる手続についても言及する。 |

# 外部のアプリケーションとの連携における認証・認可について

## 6.5. 技術的安全対策

●背景　HL7 FHIRの規格を用いてAPIで接続する仕組みの実現に向けて、アプリケーションごとに外部の利用者（自院職員以外）の認証・認可を行うための考え方等について、整理が必要とされているところ。

- 外部のアプリケーションとの連携における認証・認可に関して、現行のガイドラインでは**記載がない**。
- 院内のシステムと外部アプリケーションを連携して用いる場合等に、システム間連携のインタフェースとして連携のしやすさから**REST API**（Representational State Transfer Application Programming Interface）が用いられることが想定される。

改定の方向性（案）

- REST APIのセキュリティ確保のために、①APIを利用する範囲を限定すること、②外部からの攻撃を防止できるよう、認証・認可に関する仕組みを設けること、が必要であることを記載
- REST APIのセキュリティの技術的な内容に関しては、参考資料として記載
- ゼロトラストの考え方を盛り込む
- ゼロトラストを理解するために「ゼロトラスト導入指南書」（情報処理推進機構　2021年6月）などが参考になること」等の外部参照先を、ガイドラインに記載
- REST APIやAPIといった言葉をそのまま使わず、非専門家もわかりやすい言葉で説明

# BYOD（Bring Your Own Device）について

## 6.9. 情報及び情報機器の持ち出しについて

●背景　個人情報の目的外利用や流出・漏洩等への対策を前提とした医療現場におけるスマートフォン等の活用、BYODへの指摘があることを踏まえ、記載の検討が必要とされているところ。

- 現行のガイドライン(p.69)では、B項の考え方で、『個人の所有する、あるいは個人の管理下にある端末の業務利用（以下**「BYOD」（Bring Your Own Device）という。）は原則として行うべきではない**。上記の要件を実現するためには端末のOSの設定を変更する必要があるが、この機能は管理者に限定されなければならない。管理者以外による設定の変更を技術的あるいは運用管理上、禁止できない限り、BYODは行えない。』と記載している。D項の推奨でも、おおむね同様の記載となっている。
- しかし、すでにQ＆A(p14-15)では、行うべき対策を具体的に示したうえで、BYOD を認める場合、管理者が遵守することも言及している。
- また、以前よりも端末の値段は低下してきており、BYODによるセキュリティ管理のコストについても言及するべきとの意見もある。
- 一方で、実際には端末を複数台そろえることにコストを割けない医療機関もある。

改定の方向性（案）

- ガイドライン本体にも、Q＆Aに記載されている対策を記載
- 現場がBYODの対策をきちんとできるよう、分かりやすい記載に修正
- 管理されていない端末でBYODを行う場合の危険について言及

# タイムスタンプの制度の変更について

## 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

●背景　2021年4月1日に総務省より、「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）が公布・施行され、それによりタイプスタンプの総務大臣認定制度への変更となったところ。

- 「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）により、タイムスタンプを行う認証は、**総務大臣の認定業務となり**、一般財団法人日本データ通信協会は、その指定調査機関として指名されている。
- 現行のガイドライン(p99)では、『(1)タイムスタンプは、第三者による検証を可能にするため、「タイムビジネスに係る指針－ネットワークの安心な利用と電子データの安全な長期保存のために－」（総務省、平成16年11月）等で示されている時刻認証業務の基準に準拠し、一般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使用すること。』と記載されている
- 参照先は「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）に変更になり、認定事業者も今後、総務大臣から認定を受ける。

**改定の方向性（案）**

- 上記を考慮し、参照先を「時刻認証業務の認定に関する規程」（令和3年4月1日、総務省告示第146号）とする
- タイムスタンプは、上記の規程に基づき、認定された事業者（認定事業者）が提供するものを使用する、といった内容に記載を修正

# ２省ガイドラインとの整合性について

## 8.1.2.　外部保存を受託する事業者の選定基準及び情報の取扱いに関する基準

●背景　2省ガイドラインでは事業者について、JIS Q 27001及び15001を必須としているため、整合性をとるべきとの議論がある。

- 現行のガイドライン(p121)では、C項に『外部保存を受託する事業者を選定する際は、(1)から(8)のほか、少なくとも次に掲げる事項について確認すること』として、JIS Q 27001及び15001の有無を確認することに言及しているものの、 JIS Q 27001及び15001を必須とする記載はない。

改定の方向性（案）

- 現場のニーズも踏まえて、必須とするか、記載する文書の選定（ガイドライン本文、Q＆A等）も含めて検討中

# 令和２年・令和３年　改正個人情報保護法への対応について

## 4章　電子的な医療情報を扱う際の責任のあり方＋8.1.3.　個人情報の保護

●背景　令和２年改正個人情報保護法(令和２年６月１２日公布)が令和４年４月１日に施行されるにあたって、個人情報保護法上新設された概念や手続等について、ネットワークのセキュリティといった点から、ガイドライン上の対応が求められる。

- 現行のガイドラインでは、第４章(p21-)、8.1.3章(p123-124)などで、電子的な医療情報を取り扱う際の責任のあり方や個人情報の保護について言及している。
- 令和２年・令和３年改正個人情報保護法が施行されるにあたって、**「仮名加工情報」**等に関連した、ガイドラインへの影響を検討し、対応することが求められている。
- 医療情報連携ネットワークを通じた情報提供は、第三者提供型を想定して4.3章は記述されているが、共同利用型も想定される。

改定の方向性（案）

- 医療機関内における仮名加工情報・個人関連情報のユースケースや共同利用として個人情報が取り扱われる場合について、現状を踏まえた上で、Q&Aへ記載することも含めて、検討を行う

# ガイドライン全体の見直しについて

## ガイドライン全体

●背景　技術的な記載や措置は例示として分けて整理し、わかりやすく記載することが必要ではないか。とのご指摘をいただいているところ。

- 本ガイドラインはA項(**制度上の要求事項**)、B項(**考え方**)、C項(**最低限のガイドライン**)、D項(**推奨されるガイドライン**)の構成となっているが、考え方の部分に技術的な記載や具体例が掲載され全体の分量が多くなっている。
- ガイドライン本体の対象は、**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**とされているが、一部の医療機関では、その責任者がITの専門家でない者が担当する可能性もある。

## 改定の方向性（案）

- 技術的な記載や措置に関しては、別冊を作成。その際、ガイドライン本体を理解するための内容に不足がない形で別冊に移動する部分を選定
- 上記を考慮し、ITの非専門家でも分かりやすい言葉で記載

# サイバー攻撃の対応について

## 6.10. 災害、サイバー攻撃等の非常時の対応

- 現行のガイドライン(p74)には、（3）サイバー攻撃を受けた際の非常時の対応を記載しているが、昨今、**サイバー攻撃によってバックアップデータまで被害を受けた事例もみられる**。
- サイバー攻撃の多様化、巧妙化に対応するべく、具体的な対策の記載が求められている。
- また、ランサムウェア等、最新のサイバー攻撃への対策として、VPN 機器に対する脆弱性対策が、PC における脆弱性対策と同様に重要になっている。
- 端末やサーバ装置の活動を監視し、不正プログラム等の検知や対処を行うEDR（Endpoint Detection and Response）ソフトウェア等の利用や、主体の操作に対する常時アクセス判断・許可アーキテクチャ（ゼロトラストアーキテクチャ、ゼロトラストセキュリティ等）での制御等の記載についても検討が必要である。

**改定の方向性（案）**

- 現行では、「災害時」と「サイバー攻撃」の対応が「非常時」としてまとめて記載されているが、ランサムウェアの被害も出ていることから、バックアップデータまで被害が拡大しないよう対策を記載。新項を設けることも含め検討
- バックアップまで被害を受ける事例に関して、対策として、バックアップを保存する電磁的記録媒体等の種類、バックアップの周期、世代管理の方法、バックアップデータを保存した媒体を端末及びサーバ装置やネットワークから切り離して保管すること等を考慮する必要があること等、具体的に記載
- あわせて、詳細な対策について、NISCの「政府機関等のサイバーセキュリティ対策のための統一基準群（令和３年度版）」、「ランサムウェアによるサイバー攻撃に関する注意喚起」等の参照先を記載。
- 医療機関における、災害時の訓練と同様に、サイバー攻撃を想定した訓練なども必要であることも言及

# 長期署名の参照先の規格について

## 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

●背景　長期署名方式についてJIS規格を参照することとしているが、2008年以降改定されておらず、実務的な影響を生じている。

- 現行のガイドライン(p98)では、『近年、デジタルタイムスタンプ技術を利用した長期署名方式の標準化が進み、長期的な署名検証の継続が可能となり、JIS規格としても制定された（JIS X 5092:2008 CMS利用電子署名(CAdES)の長期署名プロファイル、JIS X 5093:2008 XML署名利用電子署名(XAdES)の長期署名プロファイル）。』との記載があるが、JIS規格は2008年から改定されていない。
- ISOは2021年に国際規格の改定がされている。
- 参照先を**JISからISOに変更する**ことも検討する。

改定の方向性（案）

- 実務的な影響範囲を確認したうえで、参照先の変更について検討中

# 外部ネットワークが活用可能であることのわかりやすい周知について

## 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

●背景　医療機関や関係者が電子カルテ等医療情報を授受するに当たって当事者が講ずべき安全措置やセキュリティ対策と併せて、外部ネットワークが活用可能であることをわかりやすく周知することが必要とされているところ。

- 現行のガイドライン(p84)では、B項の考え方でⅡ．オープンなネットワークで接続する場合に『「盗聴」、「侵入」、「改ざん」、「妨害」等の様々な脅威が存在するため、十分なセキュリティ対策を実施することが必須である』等、その他、詳細に記述している。
- またC項の最低限のガイドラインでは具体的にプロトコルやプロトコルバージョンにも言及しているが、**外部ネットワークへの接続について明確に示されておらず**、外部ネットワークへの接続に躊躇する原因となっているとの指摘もある。

改定の方向性（案）

- 接続していることを前提とした記載に変更。誤解を与えないよう記載を工夫
- B項の考え方の中で、技術的な記載や措置について記載されている箇所は、例示として別冊（解説書）に移動
- 見やすい記載にした上で、安全対策で必須の考え方は、漏れがないように記載

例）「医療機関等において医療情報を外部と交換する場合、外部ネットワークを利用することが考えられること」、「その場合、管理されていないネットワーク、機器、サービスを用いないこと」、「管理されているネットワーク、機器、サービスのモニタリングを適切に行うこと」

# 電子署名について

## 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

●背景　電子署名の利用が可能である旨を医師法等の法令を踏まえ、規定すること、その際、医療現場のニーズを踏まえ、電子署名の活用促進につながるようなガイドラインの見直しを検討することが必要とされているところ。

- 現行のガイドライン(p98)では、C. 最低限のガイドラインで、厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI認証局又は認定特定認証事業者の発行する電子証明書のほか、同等の本人確認等を行った上で発行する電子証明書、「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」に基づく公的個人認証サービスを用いて電子署名を施すことを記述しているが、**電子署名の利用が進んでおらず、医師等の国家資格の確認が必要な文書における当該資格の確認方法や確認する考え方について記載が必要**との指摘がある。

### C. 最低限のガイドライン

法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う必要がある。

1. 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI認証局又は認定特定認証事業者等の発行する電子証明書を用いて電子署名を施すこと

(1) 保健医療福祉分野PKI認証局は、電子証明書内に医師等の保健医療福祉に係る資格を格納しており、その資格を証明する認証基盤として構築されている。したがって、この保健医療福祉分野PKI認証局の発行する電子署名を活用することが推奨される。
ただし、当該電子署名を検証しなければならない者の全てが、国家資格を含めた電子署名の検証が正しくできることが必要である。

(2) 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項の要件を満たすことは可能であるが、同等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。

(3) 「電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律」（平成14年法律第153号）に基づき、平成16年1月29日から開始されている公的個人認証サービスを用いることも可能であるが、その場合、行政機関以外に当該電子署名を検証しなければならない者が全て公的個人認証サービスを用いた電子署名を検証できることが必要である。

# 電子署名について

## 作業班構成員のご意見

- 現在の紙の処方箋における判子の役割は、処方医師以外が代行して押印したとしても、その医師が責任を負うことの法的否認ができないという意味合いが強い。これを電子署名で行う際にクラウド署名を利用した場合、三文判を押すこととクラウド署名をすることの手間を直接比較することは困難だが、大幅な手間の違いが生じるとは考えにくく、責任の所在を明らかにする有用性は向上すると考える。
- 医師等の資格確認を組織（医療機関）に認証させることに関しては、多様な医療機関がある中で（保険診療、自由診療、医師一人のみの医療機関等）、医療安全の観点から、全ての医療機関で認証で行うことは困難と考える。
- 大病院では、全職員にHPKIを取得させるのは現実的に難しい可能性がある。組織としての資格の認証を検討する上では、認証を許可するためのしっかりとした基準を設け、第三者機関などへの申請や定期的な監査をクリアできる医療機関を前提とすれば、組織による医師の資格確認の仕組みを考慮できるかもしれない。クリニック等では、むしろHPKIを取得した方が楽となるだろう。
- 薬剤師は、調剤時に医師が医師の資格をもって処方箋に電子署名していることを”リアルタイムに電子署名の検証”できなければならない。
- 薬剤師が既知の医療機関でない処方に関して調剤する必要が出てきた場合、これが間違いなく都道府県知事等の許可を受けた医療機関であって組織認証を許可された医療機関であること、その医療機関が医師の資格を責任もって証明できることが必要である。
- また、法律で「医師が」「薬剤師が」と記載されている中で、組織による資格確認で実際に問題が起こった場合の責任の所在の明確化なども必要である。

## 改定の方向性（案）

- 法令で有資格者による作成が求められている文書等については、電子的な本人確認に加え、同時に、医師等の資格確認が電子的に検証できることが必須
- クラウド型電子署名の利用が可能である点について追記
- 認定認証事業者や医療機関による、医師等の国家資格の確認・認証の方法については、引き続き検討を続ける。その際、国家資格の確認方法に一定の基準を設け、申請や定期的な監査をクリアできること等の前提も含めて議論　　等

# 中長期的な安全管理ガイドラインの改定の論点

- 以下の項目は十分な検討が必要と考え、中長期的な論点として検討を継続する予定である。

| 論点の概要 | 論点の背景 |
|---|---|
| クラウドサービス利用の拡大 | ● 院内の多様なシステムに関して、オンプレミスとの関係を整理し、クラウド利用を想定し、現行ガイドラインに不足している内容を検討<br>● 端末の持ち出しだけでなく、クラウドサービスによる情報の持ち出しについて現行の課題を抽出し、対策を検討 |
| 多様化するサイバー攻撃への対応 | ● 医療機関等における内部ネットワークについて、「ゼロトラスト」の考え方を参考にした記載や、セキュリティ自動監視などについても検討 |
| 新技術への対応 | ● PHSサービスに代わり、５Gサービスが今後使用される可能性を考え、前もって議論 |
| 制度・規格関係 | ● 医療情報連携ネットワークを通じた、情報提供について、共同利用型などを想定し、記載を検討 |