弁護士法人　三宅法律事務所

Miyake　& Partners

## デジタル・ガバナンス／サイバーセキュリティニュース　No.2

### 医療情報システムの安全管理に関するガイドライン第 7.0 版の公表
### ― 全体像、5 編構成と適用範囲、及び医療機関等に求められる対応 ―

平素より大変お世話になっております。

令和8年7月 15 日、厚生労働省は、「医療情報システムの安全管理に関するガイドライン第 7.0 版」を公表いたしました[1]。意見募集時は第 6.1 版（案）とされていましたが、改訂内容が多岐にわたるとの意見を踏まえ、**第 7.0 版として公表**されています。

今回の改訂は、医療情報の秘密保持や電子保存の適法性にとどまらず、**サイバー攻撃による医療提供の停止、委託先・クラウド事業者との責任分界、経営層による予算・人材の確保及びインシデント対応を、医療機関の経営課題として捉え直すもの**です。

本ニュースレターは総論として、第 7.0 版の全体像、適用範囲、5 編構成と読み方、各編の重要ポイント及び残された論点を整理いたします。各編の詳細な遵守事項及び契約実務への影響については、別途、編ごとのニュースレターでご案内する予定です。末尾には理解度チェック（〇×問題 10 問）を付しておりますので、院内研修等にもご活用いただけますと幸いです。

令和8年7月 16 日
弁護士法人三宅法律事務所

＊本ニュースレターに関するご質問・ご相談がありましたら、下記にご連絡ください。
弁護士法人三宅法律事務所
弁護士　渡邉雅之（執筆者）
TEL 03-5288-1021　FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp

[1]厚生労働省「医療情報システムの安全管理に関するガイドライン第 7.0 版」（令和8年7月 15 日公表）。あわせて、意見募集の結果（「第 6.1 版（案）」に対する意見に対する考え方）も公表されている。本文中の「パブコメ回答項番」は、同意見募集の結果における項番を指す。

## 医療情報システムの安全管理に関するガイドライン第 7.0 版の公表
## ― 全体像、5 編構成と適用範囲、及び医療機関等に求められる対応 ―

**【目次】**



### 1　はじめに

厚生労働省は、令和8年7月 15 日、「医療情報システムの安全管理に関するガイドライン第 7.0 版」を公表した。パブリックコメントでは**計 271 件**の意見が提出され、二要素認証、クラウドサービス、データ保存場所、委託先との責任分界、ランサムウェア対応、ログ監査等について多数の意見が寄せられた。意見募集時の名称は第 6.1 版（案）であったが、改訂内容が多岐にわたることを踏まえ、版数は第 7.0 版に変更された（パブコメ回答項番 3）。

以下では、厚生労働省の対応を、①修正済、②原案維持、③Q&A で補足予定、④継続検討、⑤参考意見にとどまる、の 5 類型に分けて整理する。もっとも、パブリックコメント回答に「修正・追記した」と記載されていても、最終版では提案文言が一般化されている箇所があるため、本稿では最終的に公表された第 7.0 版の本文を基準とする。

**【主要論点の対応状況】**

| 主要論点 | パブコメ項番 | 対応区分 | 最終版でのポイント |
|---|---|---|---|
| 第 7.0 版への変更 | 3 | ①修正済 | 改訂内容の広がりを版数にも反映 |
| 経営層の投資・EOS 判断 | 42・50 | ①修正済 | 予算、人材、補完策、更新・廃止を経営判断 |
| 漏えいのおそれ段階の対応 | 55・242 | ①修正済 | 個人情報保護法上の初動を明確化 |
| 二要素認証の強化 | 181 ほか | ②原案維持等 | 入退室管理による代替を認めず、新規導入・更改時に対応 |
| 身代金支払い | 53 | ③Q&A | 支払いは厳に慎むとの本文を維持 |
| データ保存場所 | 17・72・77・169 | ④継続検討 | 国内保存を一律義務化せず、国外法等の確認を要求 |
| 医療機器の認証対応 | 195・196・206 | ④継続検討等 | 医療安全・実装可能性との調整が残る |
| 生成 AI 固有の規律 | 16 | ⑤参考意見 | 一般原則で対応し、AI 固有リスクは別資料で補完 |

## 2 第 7.0 版の全体像——経営課題としてのサイバーセキュリティ

### (1)根拠法と政策上の位置付け

概説編は、第 7.0 版から本ガイドラインの根拠法にサイバーセキュリティ基本法を追加し、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」との整合性を確保したと説明する(概説編 1 頁、パブコメ回答項番 36・②原案維持)。重要インフラ事業者と本ガイドラインの対象医療機関等は必ずしも一致しないが、第 7.0 版は、医療情報の秘密保持だけでなく、医療提供の継続、患者の生命・身体の保護及び被害の波及防止を含む基準へと性格を強めた。

病院、診療所及び助産所については医療法施行規則 14 条 2 項、薬局については医薬品医療機器等法施行規則 11 条 2 項 1 号が、サイバーセキュリティ確保措置の直接の法令上の根拠となる。その他の対象機関については、それぞれに適用される法令等を確認する必要がある。**本ガイドライン自体は法令ではないものの、法令上の措置義務を具体化する実務上の基準として機能し、監督上の対応や民事責任の判断にも影響し得る。**

### (2)安全管理対策を「コスト」ではなく「投資」と位置付け

経営管理編は、インシデントによる医療提供の停止、患者の生命・身体への影響、行政上・民事上の責任及び復旧費用を指摘した上で、**安全管理対策を「コスト」ではなく、質の高い医療の提供等に不可欠な「投資」と捉え、必要な予算・人材を確保することが重要**であるとする(経営管理編 1 頁、パブコメ回答項番 42・①修正済)。

### (3)保守委託機関編の創設

第 7.0 版では、すべてのサーバのセキュリティアップデート責任を事業者に委託している医療機関等の負担軽減を図るため、保守委託機関編が創設された(概説編 1 頁)。ただし、技術的な実装を外部化しても、事業者の選定、契約内容の確認、管理監督、患者等への説明及びインシデント時の意思決定まで外部化できるわけではない。

## 3 適用範囲と 5 編構成——自院はどこまで対応するのか

### (1)対象となる機関・情報・システム

対象となる「医療機関等」には、病院、一般診療所、歯科診療所、助産所、薬局、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が含まれ、医療情報システムの導入、運用、利用、保守及び廃棄に関わる者が対象となる(概説編 2 頁)。対象文書は医療情報を含む文書全般であり、法定保存義務の有無を問わない。医療機関等が医療情報を患者の管理に委ねた後、第三者が患者から提供を受けて取り扱う場合には、PHR の指針の対象となり得る。

対象となる医療情報システムは、医療情報を「保存する」システムに限られず、**医療情報を入力、送信、解析又は一時的に処理する情報システム全般**である。したがって、電子カルテ等だけでなく、医療情報を扱う AI・画像解析サービス、クラウド型サービス、外部接続サービス等も利用実態に応じて対象となり得る。他方、医療情報を含まない費用請求情報のみを取り扱う会計・経理システム等は対象外とされる(概説編 2 頁)。

### (2)5 編の役割

| 編 | 想定読者 | 主な役割 |
|---|---|---|
| 概説編 | 全読者 | 目的、対象、全体構成、各編共通の前提 |
| 経営管理編 | 経営層 | 方針・予算・残存リスクの判断、指示、報告受領 |
| 企画管理編 | 企画管理者 | 規程・体制・契約・リスク管理の具体化 |
| システム運用編 | システム運用担当者 | 技術的な設計・実装・運用 |
| 保守委託機関編 | 小規模医療機関等の管理者・担当者 | 技術的対応を事業者に委託する前提の統制・管理 |

### (3)保守委託機関編を利用できる条件

概説編の判定フローは、「すべてのサーバのセキュリティアップデート責任を事業者に委託している」場合には概説編

と保守委託機関編、そうでない場合には概説編、経営管理編、企画管理編及びシステム運用編に対応する構造を示す（概説編 3～4 頁）。ここでいうサーバは、医療情報の保存又は主要な処理を担う機器であり、端末上で処理が完結する場合は PC 等も含まれ得る。

**事業者がアップデート責任を負うことが契約書、約款又は SLA 等に記載されている場合にのみ、判定フローで「YES」を選択できる。**記載がない場合又は不明確な場合には事業者に直接確認し、責任の所在を明確にしなければならない。標準約款等に責任が明記されていれば個別の特約が不要な場合はあるが、契約内容の確認自体が不要になるわけではない。

## 4 各編に共通する前提——リスク管理、事業者との協働、クラウド

### (1)リスク評価と継続的改善

概説編は、機密性・完全性・可用性のバランスを考慮してリスクを評価し、安全管理措置を継続的に実施・改善することを求める（概説編 5～7 頁）。重要なのは、対策を一律に導入することではなく、**自院の情報資産、システム構成、医療継続への影響及び委託状況を踏まえ、リスクの回避・低減・移転・受容を選択し、その判断と証跡を残すこと**である。

### (2)事業者とのリスクコミュニケーション

医療機関等は、MDS/SDS、サービス仕様適合開示書、認証・第三者評価資料等を通じて、事業者から技術的対策、再委託、バックアップ、脆弱性対応等の情報を収集し、責任分界と役割分担を契約書・SLA 等に反映する必要がある（概説編 6～8 頁）。第 7.0 版が求めるのは、事業者への丸投げでも、形式的な認証確認でもなく、リスクの所在を双方が理解し、通常時と非常時の対応を文書化することである。

### (3)クラウドの位置付け

第 7.0 版は、適切な事業者への外部保存により、専門的な安全管理措置を利用できることを積極的に評価する。特に、**専任のシステム運用担当者がいない小規模医療機関等について、適切なクラウドサービスの利用を有力な安全管理策として位置付けている**（概説編 8 頁）。もっとも、クラウドを利用すれば責任が事業者へ移るわけではなく、委託先選定、契約、責任分界、定期的な報告確認及び終了時のデータ返却・削除が前提となる。

## 5 経営管理編の要点——判断・予算・インシデント対応

### (1)予算、EOS 及び残存リスクの承認

**パブコメ回答項番 42・50 ①修正済**

情報セキュリティ対策の計画は予算計画と併せて策定する必要がある（経営管理編 9 頁）。特に EOS（サポート終了等）機器について、**経営層は担当者へ情報収集を指示するだけでなく、更新予算の確保、補完的対策、運用廃止又は残存リスクの受容を責任をもって判断すること**が求められる（同 12 頁）。利用を継続する場合には、対象機器、既知の脆弱性、医療継続への影響、補完策、継続期限及び再評価時期を記録することが重要である。

### (2)組織横断の統制

統制の対象には、直接雇用する職員だけでなく、派遣社員やシステム関連事業者の担当者等も含まれる。各部門が独自に導入するシャドーIT を防ぐため、システムの導入・変更を共有・承認する仕組みも必要である（経営管理編 8～10 頁）。

### (3)漏えいの「おそれ」段階からの初動

**パブコメ回答項番 55・242 ①修正済／項番 53 ③Q&A で補足予定**

個人情報の漏えい等又はそのおそれが生じ、個人情報保護法施行規則所定の報告対象事態に該当する場合には、個人情報保護委員会への報告等が必要となる。**ランサムウェア感染時に持出しの事実が未確定であっても、漏えいのおそれを否定できない場合には、フォレンジック調査の完了を待たず速報の要否を判断する必要がある**（経営管理編 13 頁）。身代金の支払いは犯罪組織への支援と同義であり厳に慎むとの基本姿勢が維持され、具体的な判断は別途 Q&A で補足される予定である。

## 6 企画管理編の要点——責任分界と委託先管理

### (1)責任分界は契約と運用文書の二層で

責任分界は、通常時と非常時を分けて整理し、契約書又は SLA 等の拘束力ある合意文書に加え、運用マニュアル、連絡体制表、手順書等に具体化する必要がある（企画管理編 9～12 頁）。**医療機関等が購入した機器について別途保守契約を締結しない場合、原則として管理責任は医療機関等に残る**ため、買い切りの端末、ルーター、検査機器付属 PC 等も棚卸しの対象となる。

### (2)委託先選定は認証だけで完結しない

| **パブコメ回答項番 59・71　①修正済／③Q&A で補足予定** |
|---|

企画管理編 7 は、外部保存等の委託先について、体制、バックアップ、信用度、経営の健全性、P マーク・ISMS、保存場所及び国外法の適用可能性等を確認するよう求める（企画管理編 26～28 頁）。P マーク・ISMS 等が確認できない場合には、ISMAP、SOC2 等の代替的な認証・評価又は有資格者による外部監査結果を用いて同等の能力を確認する経路が示されている。認証取得の事実だけでなく、対象サービスが認証範囲に含まれるか、安全対策の有効性を示す資料があるかを確認すべきである。

### (3)二次利用と約款契約

外部保存の委託契約には、医療機関等又は患者等の許可なく受託した医療情報を分析等の目的で取り扱わないこと、匿名化の妥当性を検証すること、契約終了時の返却方法等を含める必要がある（企画管理編 27～29 頁）。これは個人情報保護法上の個人データに限られない広い範囲の情報について、契約上の管理を求めるものである。約款型クラウドについても、MDS/SDS 等の情報提供、リスク表示及び役割分担を確認した上で利用する必要がある。

## 7 システム運用編の要点——二要素認証・ログ・ネットワーク

### (1)入退室管理は二要素認証の代替にならない

| **パブコメ回答項番 181・186・191・194　②原案維持** |
|---|

**第 6.0 版に存在した、入退室時の認証と端末利用時の認証を組み合わせて二要素認証相当と扱う考え方は、第 7.0 版では維持されなかった**。施錠された診察室・サーバ室に端末があることは物理的安全管理として重要であるが、システム上の当人認証を代替しない。

### (2)新規導入・更改時の二要素認証を原則化

第 7.0 版は、**令和9年4月 1 日時点で稼働が想定される医療情報システムについて、今後の新規導入又は機器入替等を伴う更改の際に、二要素認証又は相当する対応を採用することを求める**。技術的理由等により対応が間に合わない場合には、令和9年度以降の直近の更改・新規導入までを経過措置とする（システム運用編 35～37 頁）。**既存のすべてのシステムについて令和9年4月 1 日までの一律改修を求める趣旨ではない**点に注意を要する。クライアントでは原則としてアプリケーション、サーバでは OS で実装し、OS の一要素とアプリケーションの別の一要素を単純に組み合わせる方式は認められない。

### (3)ログ監視とネットワーク

**パブコメ回答項番 217　①修正済**

個人情報を含む資源についてはアクセスログを収集し、定期的に不正利用の有無を確認する必要があるが、**全ログを人が目視確認することまでは求められていない**。システム監視又は適切な閾値によるスクリーニング後のログを確認する運用が想定される（システム運用編 42 頁）。また、VPN 機器等の管理画面・管理ポートを外部に公開しないこと、リモート保守の接続元、特権 ID、利用時間及びログを管理することが重要であり、ベンダーごとに分散した保守回線は見直しの対象となる。

## 8　保守委託機関編の要点――技術実装を委託しても責任は残る

保守委託機関編は、専任のシステム担当者が不在で、経営管理と企画管理の部門が分離されていないことが多い小規模医療機関等を主な対象とする（保守委託機関編 1～2 頁）。対象となるには、すべてのサーバのセキュリティアップデート責任が、契約書・約款・SLA 上、事業者に委託されている必要がある。

同編は、法令遵守、BCP、責任分界、委託先選定、MDS/SDS、構成図、ID 棚卸し、二要素認証、バックアップ、再委託、インシデント報告、契約終了時のデータ返却・削除等をチェックリスト化している。**小規模医療機関にとって実務的な負担軽減となる一方、事業者の選定・監督、職員教育、患者等への説明及び経営判断は医療機関自身が行う必要がある**。

## 9　残された論点――生成 AI・データ保存場所

### (1)生成 AI 固有の規律は本文に盛り込まれず

**パブコメ回答項番 16　⑤参考意見にとどまる**

パブコメでは、プロンプトへの医療情報入力、外部 AI 基盤への送信、学習利用及び AI 固有のセキュリティリスクへの言及がないことが問題提起されたが、**厚生労働省は今後の参考とするにとどめ、第 7.0 版に生成 AI 固有の規律を追加しなかった**。もっとも、医療情報を扱う生成 AI には、対象システムの範囲、リスク評価、委託先選定、目的外利用禁止、アクセス制御、ログ及び漏えい対応等の一般原則が適用される。これに加え、入力情報の学習利用、保存期間、サブプロセッサ、出力の人による確認、ハルシネーション及びプロンプトインジェクション等を利用規程・契約で補完する必要がある。

### (2)データ保存場所と国外法

**パブコメ回答項番 17・72・77・169　④継続検討／今回は原案維持**

企画管理編は、外部保存先の情報機器等が国内法の適用及び執行の及ぶ範囲にあることを確実にするよう求める一方、**国内保存・国内事業者の利用を一律の要件とはしなかった**（企画管理編 26～27 頁）。委託先選定時には、保存する情報機器の設置場所（地域・国）及び国外法の適用可能性を確認する必要があり、確認を行わずに選定した場合、ガイドライン上の遵守事項を満たさないおそれがある。契約主体だけでなく、保存国・処理国、アクセス可能地域、再委託先、外国政府からの開示要求、暗号鍵管理及び終了時のデータ回収を具体的に評価し、記録する必要がある。

## 10　医療機関等において必要となる対応

第 7.0 版への対応として、少なくとも次の事項を確認する必要がある。

| 区分 | 主な確認事項 |
|---|---|
| 経営・体制 | 経営層が計画・予算・EOS 対応・残存リスクを承認しているか。責任者、代行者及び報告経路が明確か。 |
| 資産・契約 | 構成図、資産台帳、EOS 一覧、委託先・再委託先一覧が最新か。アップデート、脆弱性、ログ、バックアップ、インシデント通知、返却・削除の責任を契約等で明確にしているか。 |
| 認証・技術 | クライアントとサーバの二要素認証を更改計画に反映しているか。VPN、管理画面、特権 ID、ログ監視及びバックアップの実効性を確認しているか。 |
| インシデント・BCP | 初報、法定報告、厚生労働省・警察等への連絡、患者等への説明及び医療継続の手順があるか。復旧訓練を実施しているか。 |
| 新規リスク | 生成 AI・海外クラウドについて、入力情報、学習利用、保存場所、国外法、再委託及び出力確認を別途評価しているか。 |

**【契約見直しの優先順位】**

直ちに全契約を全面改定することが困難な場合は、①インシデント通知・緊急連絡、②VPN・ネットワーク機器を含む脆弱性対応、③ログ提供、④バックアップ・復旧、⑤再委託・保存場所、⑥終了時のデータ返却・削除、の順に確認することが考えられる。既存契約に条項がない場合は、覚書、運用合意書、SLA 又はチェックシートで補完し、次回更新時に契約本文へ統合する方法もある。

## 11 おわりに

第 7.0 版は、医療情報システムの安全管理を、技術担当者だけの問題から、**経営層が予算、人材、EOS 機器、残存リスク、BCP 及び訓練について判断するサイバーガバナンスへと転換する改訂**である。同時に、特に小規模医療機関等についてクラウド・SaaS・保守委託を有力な選択肢とし、その前提として責任分界と契約管理を重視している。

実務上は、二要素認証の新規導入・更改時対応、漏えいのおそれ段階からの初動、EOS・VPN 機器等の脆弱性管理、ログ監視及び委託先管理が特に重要である。生成 AI 及びデータ保存場所については課題が残されており、今後の Q&A 及び次期改訂を継続的に確認しつつ、経営判断、規程、契約、技術対策、訓練及び監査を一つの管理サイクルとして運用する必要がある。

## 12 理解度チェック（〇×問題 10 問）

第 7.0 版の理解度を確認するため、〇×問題を 10 問用意した。院内研修等にご活用いただきたい。まず【問題】に解答した上で、【解答・解説】をご確認いただきたい。

**【問題】次の記述は正しいか（〇×）。**

**第 1 問** 本ガイドラインは、意見募集時には第 6.1 版（案）とされていたが、改訂内容が多岐にわたることを踏まえ、第 7.0 版として公表された。

**第 2 問** 本ガイドラインの対象となる医療情報システムは、医療情報を「保存する」システムに限られ、医療情報を一時的に処理するにとどまるシステムは対象とならない。

**第 3 問** 第 7.0 版は、安全管理対策を、質の高い医療の提供等に不可欠な「投資」ではなく、可能な限り抑制すべき「コスト」と位置付けている。

**第 4 問** 概説編の判定フローにおいて、保守委託機関編で対応する（「YES」を選択する）ためには、すべてのサーバのセキュリティアップデート責任を事業者に委託していることが、契約書・約款・SLA 等に記載されている必要がある。

**第 5 問** 第 7.0 版は、施錠された診察室やサーバ室に端末が設置されていること（入退室管理）をもって、システム上の二要素認証の代替として認めている。

**第 6 問** 第 7.0 版は、既存のすべての医療情報システムについて、令和9年4月 1 日までに二要素認証への一律の改修を完了することを求めている。

**第 7 問** 個人情報を含む資源については、収集したすべてのアクセスログを、担当者が目視で確認することが求められている。

**第 8 問** ランサムウェアに感染したものの、情報の持出しの事実が確定していない場合には、フォレンジック調査が完了するまで、個人情報保護委員会への速報の要否を判断する必要はない。

**第 9 問** 第 7.0 版は、生成 AI に関する固有の規律を本文に追加し、プロンプトへの医療情報の入力や学習利用等について具体的な遵守事項を定めた。

**第 10 問** 第 7.0 版は、外部保存の委託先について、保存する情報機器を国内に設置すること又は国内事業者を利用することを一律の要件とした。

**【解答・解説】**

| 問 | 解答 | 解説（根拠） |
|---|---|---|
| 第 1 問 | 〇 | 意見募集時の名称は第 6.1 版（案）であったが、改訂内容が多岐にわたることを踏まえ、版数は第 7.0 版に変更された（パブコメ回答項番 3。本文 1）。 |
| 第 2 問 | × | 対象となる医療情報システムは、医療情報を「保存する」システムに限られず、医療情報を入力、送信、解析又は一時的に処理する情報システム全般である。電子カルテ等だけでなく、医療情報を扱う AI・画像解析サービス、クラウド型サービス等も利用実態に応じて対象となり得る（概説編 2 頁。本文 3(1)）。 |
| 第 3 問 | × | 経営管理編は、安全管理対策を「コスト」ではなく、質の高い医療の提供等に不可欠な「投資」と捉え、必要な予算・人材を確保することが重要であるとする（経営管理編 1 頁、パブコメ回答項番 42。本文 2(2)）。 |
| 第 4 問 | 〇 | 事業者がアップデート責任を負うことが契約書、約款又は SLA 等に記載されている場合にのみ、判定フローで「YES」を選択できる。記載がない場合又は不明確な場合には、事業者に直接確認し、責任の所在を明確にしなければならない（概説編 3～4 頁。本文 3(3)）。 |
| 第 5 問 | × | 入退室時の認証と端末利用時の認証を組み合わせて二要素認証相当と扱う考え方は、第 7.0 版では維持されなかった。施錠された診察室・サーバ室に端末があることは物理的安全管理として重要であるが、システム上の当人認証を代替しない（パブコメ回答項番 181 ほか。本文 7(1)）。 |
| 第 6 問 | × | 第 7.0 版が求めるのは、令和9年4月 1 日時点で稼働が想定されるシステムについて、今後の新規 |

| 問 | 解答 | 解説（根拠） |
|---|---|---|
| | | 導入又は更改の際に二要素認証等を採用することであり、既存のすべてのシステムについて同日までの一律改修を求める趣旨ではない。技術的理由等により間に合わない場合は、令和9年度以降の直近の更改・新規導入までが経過措置とされる（システム運用編 35～37 頁。本文 7(2)）。 |
| 第 7 問 | × | 全ログを人が目視確認することまでは求められていない。システム監視又は適切な閾値によるスクリーニング後のログを確認する運用が想定されている（パブコメ回答項番 217、システム運用編 42 頁。本文 7(3)）。 |
| 第 8 問 | × | 持出しの事実が未確定であっても、漏えいのおそれを否定できない場合には、フォレンジック調査の完了を待たず、速報の要否を判断する必要がある（経営管理編 13 頁、パブコメ回答項番 55・242。本文 5(3)）。 |
| 第 9 問 | × | 厚生労働省は、生成 AI に関する意見を今後の参考とするにとどめ、第 7.0 版に生成 AI 固有の規律を追加しなかった（パブコメ回答項番 16）。もっとも、一般原則は適用され、学習利用・出力確認等を利用規程・契約で補完する必要がある（本文 9(1)）。 |
| 第 10 問 | × | 企画管理編は、外部保存先が国内法の適用及び執行の及ぶ範囲にあることを確実にするよう求める一方、国内保存・国内事業者の利用を一律の要件とはしなかった。委託先選定時に、設置場所（地域・国）及び国外法の適用可能性を確認する必要がある（パブコメ回答項番 17・72・77・169、企画管理編 26～27 頁。本文 9(2)）。 |

## 主な参照資料

① 厚生労働省「医療情報システムの安全管理に関するガイドライン第 7.0 版」（令和8年7月）――概説編、経営管理編、企画管理編、システム運用編及び保守委託機関編

② 厚生労働省「「医療情報システムの安全管理に関するガイドライン第 6.1 版（案）」に関する意見募集の結果について」――提出された意見に対する厚生労働省の考え方（本文中の「パブコメ回答項番」は同資料の項番を指す。）

③ 医療法施行規則 14 条 2 項、医薬品医療機器等法施行規則 11 条 2 項 1 号

④ 個人情報の保護に関する法律及び同法施行規則（報告対象事態に関する規定）

⑤ サイバーセキュリティ基本法、重要インフラのサイバーセキュリティに係る安全基準等策定指針

なお、本ニュースレターは一般的な情報提供を目的とするものであり、個別の医療機関等における対応については別途ご相談ください。各編の詳細及び今後公表される Q&A 等の最新情報につきましては、適宜ご確認ください。

以上