*それぞれ項目について、医療情報システムの安全管理に関するガイドライン第5.2版（以下、「ガイドライン」という）のどこの部分が対応するかを項目に追記しました。*

病院における医療情報システムのバックアップデータ及び
リモートゲートウェイ装置に係る調査に係る回答要領

依頼事項

- 本回答要領に基づき、病院における医療情報システムのバックアップデータ及びリモートゲートウェイ装置に係る調査（以下「本調査」という。）の設問に回答してください。
- 回答に当たっては、提出後の修正等作業をできるだけ防ぐだめ、必ず本回答要領を確認してください。
- 技術的な質問・用語等については、院内担当者だけでなく、システム設置事業者や保守事業者への照会等も活用して回答してください。

【電子カルテシステムのバックアップに係る質問関係】

**１．回答者の情報**

回答者の氏名、所属、連絡先を記載してください。なお、後日内容の確認のため、厚生労働省より回答者に対し連絡をさせていただく可能性があります。

**２．セキュリティ責任者を設置しているか**

システム障害時の対応や、問題発生の原因調査、セキュリティ対策訓練に関して責任がある、セキュリティ責任者を職員として配置しているか。また、セキュリティ責任者を医療情報システムの責任者とは、別に、配置しているか。回答を選択してください。

*【ガイドラインにおける該当箇所と概要】*
*本項目における「セキュリティ責任者」とは、ガイドライン本編6.10章（P.37）おける「情報セキュリティ責任者（CISO）」を指します。現状、すべての医療機関において設置の義務はありませんが、一定規模以上の病院や、地域で重要な機能を果たしている医療機関等においては、CISOの設置が強く求められています。*

**３．医療情報システムの安全管理に関するガイドライン及びそれを基としたチェックリスト等を活用しているか。**

厚生労働省が定めている、

- 医療情報システムの安全管理に関するガイドライン
- 同ガイドラインを基にした「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」

を活用しているか回答を選択してください。

（参考）

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）https://www.mhlw.go.jp/stf/shingi/0000516275.html

*【ガイドラインにおける該当箇所と概要】*

*ガイドライン本編３章（P.5）において、「本ガイドラインは医療情報を保存するシステムだけでなく、医療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、保守及び廃棄に関わる人及び組織を対象としている」と記載されています。*

**４．システム障害発生時等において詳細な緊急対応手順を整備し、定期的に訓練しているか**

システム障害時や不正アクセスが顕在化した際に、速やかに連絡するべき者（※）を院内に平時から確認・周知することが必須です。障害や不正の発生個所特定のための分析や切り分けの具体的な技術手順、代替措置のための機器や環境整備、緊急対応のための技術的措置に必要な設計資料やマニュアル、認証等の情報を常時最新化し、緊急対応が発生した際に対応が可能な状態であるか、また、それらの情報を医療情報システムの担当者と導入事業者が一体となって定期的に点検しているか、回答を選択してください。

（※）具体的には、医療情報システムの完全管理に関するガイドラインに記載されている

医政局研究機発振興課医療情報技術推進室　03-3595-2430

情報処理推進機構　情報セキュリティ安心相談窓口　03-5978-7509

の他、必要に応じて事業者、捜査機関等にも適切に情報提供すること。

*【ガイドラインにおける該当箇所と概要】*

*ガイドライン本編6.10章（P.37）において、システム障害発生時等の“非常時”における対応について、あらかじめ手順を定め、職員に対し教育・訓練を行うことを求めています。*

## ５．電子カルテシステムを使用しているか

診療録の記載・保存を電子カルテシステムで行っているか回答を選択してください。なお、本問でいう電子カルテシステムとは、

- オーダリングシステム
- オーダリング機能、画像管理等の部門システム及び診療録を電子的に記録する機能を備えた統合的な医療情報システム

を指します。なお、電子カルテシステムを使用していない場合は、９．までは回答不要となります。

## ６．電子カルテシステムのバックアップデータは作成しているか

サイバー攻撃や災害等で電子カルテシステムのデータが消失又は使用不可能な状態（暗号化等）になった場合でも、バックアップデータを作成し、診療におおきな支障がないように復旧が可能となるように定期的にテストを行っているか回答を選択してください。

*【ガイドラインにおける該当箇所と概要】*

*ガイドライン本編 7.2 章（P.60）、7.3 章（P.62）において、診療録等に記載された患者情報を確認できるよう、定期的なバックアップの実施を求めています。*

## ７．バックアップデータは世代管理しているか

電子カルテシステムのバックアップデータについて、世代管理をしているか回答を選択してください。ただし、具体的な管理方法までを問うものではありません。

なお、世代管理とは最新のバックアップデータだけでなく、それ以前のバックアップデータも管理することを指します。例えば、１日１回バックアップデータを作成している環境で「３世代管理」といえば、３日前までのデータまでさかのぼれることが可能となります。

*【ガイドラインにおける該当箇所と概要】*

*ガイドライン本編 6.10 章（P.37）において、「例えば、日次でバックアップを行う場合、数世代（少なくとも３世代）確保し、遅くとも３世代目以降はネットワーク的あるいは論理的に書き込み不可の状態にする等の対策が必要となる。」と具体例を示し、C.最低限のガイドラインにて重要なファイルは数世代バックアップを複数の方式で取得することを求めています。*

**８．バックアップデータについて、サイバー攻撃による汚損や破壊、火災や自然災害による消失等同時災害を回避する方法で管理しているか**

作成しているバックアップデータについて、例えば遠隔地のサーバに保管、世代ごとにオフラインで保存するなど、不測の事態に備えた保管方法をとっているか回答を選択してください。ただし、具体的な管理方法まで問うものではありません。

*【ガイドラインにおける該当箇所と概要】*

*上記同様に、「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して対策を講じることが強く求められる」と具体を記載しています。*

**９．バックアップデータの漏洩対策を講じているか**

作成しているバックアップデータが仮にサイバー攻撃等を受け漏洩する事態が起こった場合等においても、解読できないような対策（暗号化や秘密分散管理等）を講じているか回答を選択してください。ただし、具体的な管理方法まで問うものではありません。

*【ガイドラインにおける該当箇所と概要】*

*ガイドラインにおいては、バックアップデータの暗号化等を具体的には定めていませんが、令和４年４月施行となる改正個人情報保護法において、個人情報の流出事案については、報告の義務化・罰金の増額（最大１億円）等の措置が取られるようになるため、漏洩対策についても検討を行う必要があります。*

別紙

【リモートゲートウェイ装置に係る質問関係】

**本項目については、回答に当たり院内のサーバ室等を確認し、リモートゲートウェイ装置（以下、「VPN 装置」という）が存在するか確認してください。**

**１０．VPN 装置が存在するか。**

医療情報システム（※）の保守点検等を目的とし、事業者とシステムを接続するために VPN 装置を設置している場合が多々あります。

システム設置業者や保守業者などに照会し、当該機器が設置されているか回答を選択してください。設置されていない場合は、以降の設問は回答不要となります。

（※）医療情報システムとは、オーダリングシステム、電子カルテシステム、レセプト電算システム（審査請求受付も含む）、画像・検査等の各部門システム、地域医療ネットワークシステム、PHR 等、病院における診療を補助するためのシステム全般を指します。

**１１．VPN 装置のメーカー名、型番、台数を全て記載すること**

上記で確認した VPN 装置について記載してください。（記述方式）

**１２．内閣サイバーセキュリティセンター（NISC）や厚生労働省の注意喚起を基に VPN 装置のアップデートを適切に行っているか**

NISC や厚生労働省では、医療セプターや都道府県・地方厚生局宛にサイバーセキュリティ対策に係る情報を提供しています。それらの情報を基に、VPN 装置のアップデートを適切に行っているか、回答を選択してください。

（参考）

内閣サイバーセキュリティセンターランサムウェア特設ページ

https://security-portal.nisc.go.jp/stopransomware/

*【ガイドラインにおける該当箇所と概要】*

*ガイドライン本編 6.10 章（P.37）において、サイバー攻撃への対策については、PC や VPN 機器等の脆弱性対策をはじめとする 6.5 章及び 6.6 章に記載されている内容や、NISC から示されている「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）」、2021 年 4 月 30 日の「ランサムウェアによるサイバー攻撃に関する注意喚起について」も参照することを求めています。*

## １３．VPN 装置へのアクセス元 IP アドレスを保守業者等に制限しているか

VPN 装置への不正アクセスを防ぐため、アクセス元 IP アドレスを制限しているか、回答を選択してください。保守業者がアクセスするだけで機能を果たせると考えられ、それ以外のアクセスについては制限されるのが一般的です。保守事業者に照会し、現状を確認してください。

*【ガイドラインにおける該当箇所と概要】*

*ガイドライン 6.11 章（P.42）C.最低限のガイドラインにて、リモートメンテナンスを実施する場合は、必要に応じて、適切なアクセスポイントの設定、プロトコルの限定、アクセス権限管理等、不必要なログインを防止するための対策を実施すること、と求めています。*

## １４．VPN 装置へのアクセス記録を定期的に分析・監査しているか

不正アクセス防止の観点から VPN 装置へのアクセスをログ等に記録し、かつ、記録に不正な傾向がないか定期的に（例えば年１回）分析・監査をしているか回答を選択してください。

サイバー攻撃を受けた医療機関においても、不正アクセスの記録が残っていることがあり、それらを把握することができていれば被害を防げていた可能性もあります。

*【ガイドラインにおける該当箇所と概要】*

*ガイドライン 6.5 章（P.21）においては、VPN 装置のみならず医療情報システム全般について、アクセスログを記録するとともに、定期的にログを確認すること。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及びログイン中に操作した医療情報が特定できるように記録することを求めています。*