日薬情発第 133 号
令和 7 年 11 月 11 日

都道府県薬剤師会担当役員殿

日本薬剤師会
副会長　　原口　亨

医療情報システムの運用管理規程の薬局向け雛形について

平素より、本会会務に格別のご高配を賜り厚く御礼申し上げます。

近年、薬局においてサイバーセキュリティ対策や非常時における事業継続計画（BCP）の策定を含む、より厳格な安全管理措置が求められており、電子薬歴システムだけでなく、全ての医療情報システムについて、安全管理体制の整備が急務となっております。

そこで、薬局における情報セキュリティ管理体制を支援するため、本会において「医療情報システムの運用管理規程（雛形）」を作成いたしました。本規程は、薬局が求められる安全管理基準を遵守するための基本方針、管理体制、運用手順等を定める際の雛形であり、既に本会において公開しているサイバーインシデント発生時の事業継続計画（BCP）雛形と連携させ、平時からの体制整備と非常時の対応を一貫して行う基盤としてご活用いただけます。

なお、本規程は雛形であるため、各薬局のシステム構成や、各システムのベンダーとの契約内容等をご確認いただき、薬局の実態に合わせた内容に改変・反映していただくようお願い申し上げます。

つきましては、薬局での運用管理規程の策定にご活用いただきますよう、会務ご多用のところ恐縮ながら、貴会会員にご周知のほどお願い申し上げます。

日薬 HP＞薬局関連情報＞医療情報システムの安全管理について
https://www.nichiyaku.or.jp/yakuzaishi/pharmacy-info/cybersecurity

Ver.1.00（2025 年 11 月）

【ご確認ください】

本規程例は、各々の薬局が当該施設の医療情報システムの運用管理規程を作成する場合の参考とされるべきものであり、そのまま個々の薬局に適用できるものではありません。実際の運用管理規程は、導入されたシステムの機能や適用範囲、施設の管理体制によって異なります。このため、厚生労働省が公表している「医療情報システムの安全管理に関するガイドライン」に基づく運用を実現するには、機器やソフトウェア機能と運用手順を照らし合わせ、実態に最も合った方法を決定していただく必要があります。

医療情報システムの運用管理規程

〇〇〇薬局

Ⅰ　総則

1　目的

本規程は、○○○薬局（以下「当薬局」という。）において、医療情報を扱うシステムを安全に運用するために必要な事項を定め、患者情報等の個人情報を適正に管理し、医療情報システムの安全管理を確保することを目的とする。

2　理念

当薬局における医療情報システムの運用は、医療の質の向上と患者の安全確保を目的とするものであり、その運用に際しては、情報を取り扱う全ての職員が自己の責任において、正確かつ安全に情報を管理しなければならない。また、医療情報は、患者の人格とプライバシーに深く関わるものであることを認識し、法令および社会的規範を遵守し、機密保持と個人情報保護を徹底する。特に電子薬歴システムの利用にあたっては、その真正性（誰が・いつ・何を記録したかが明確であること）、見読性（必要な時に正確に閲覧できること）、保存性（長期間にわたり改ざんされず保持できること）を確保するよう留意しなければならない。また、電子薬歴は単なる記録媒体ではなく、患者の服薬状況や生活背景を理解し、チーム医療や地域連携に活用するための重要なツールである。管理者および職員は、その意義を理解し、システムを適切に運用しながら、患者中心の医療提供体制の実現に努める。

3　対象情報の範囲

本規程における対象範囲は次の通りとする。

種別	システム名称	提供メーカー
会計システム （レセコン）		
電子調剤録 電子薬歴		
オンライン資格端末		
オンライン服薬指導 システム		
電子お薬手帳 システム		

Ⅱ　一般管理

1　管理組織

当薬局に医療情報システム安全管理責任者（以下「システム管理者」という。）を置き、【薬局開設者／管理薬剤師】をもってこれに充てる。システム管理者は、必要に応じて運用責任者、監査責任者を指名する。

2　システム管理者の責務

システム管理者は、医療情報システムの導入・設定・運用・保守・教育・監査に関して統括的な責任を負う。利用者登録・アクセス権限設定・不正利用防止・技術的安全管理の実施・セキュリティパッチ更新・定期点検・障害対応・情報セキュリティインシデント対応を行う。

3　利用者の責務

利用者は、自身の ID とパスワードを適切に管理し、他人に貸与または共有してはならない。入力情報は正確に確認し、確定操作を行う。情報の目的外利用はせず、患者のプライバシー保護を常に意識して行動する。情報セキュリティインシデント又はそのおそれのある事象を発見した場合は、速やかにシステム管理者に連絡し、その指示に従う。

4　文書管理体制

マニュアル、契約書、報告書等の文書は電子媒体または紙媒体で適切に保管し、改訂履歴を管理する。常に最新版が参照できるようにする。

5　教育・訓練体制

全職員に対し、情報セキュリティおよびプライバシー保護に関する教育を必要に応じて随時実施する。新規採用者には初期教育を行う。

6　監査体制

システム管理者は、年 1 回以上、運用状況およびアクセス権限等を監査し、必要に応じて改善措置を講じる。監査結果は記録して保存する。

7　事故・非常時の対策

別途定めるサイバーインシデント発生時の事業継続計画（以下「BCP」という）に基づき、情報漏えい、改ざん、紛失、機器障害等が発生した場合は、速やかにシステム管理者へ報告し、初期対応と再発防止策を実施する。重大な事案は関係機関へ報告する。また、可能な範囲で代替手段を用いて業務を継続し、患者への影響を最小限に抑えるよう努める

8　入退管理

医療情報システム設置場所への来訪者は受付簿に記録し、入退室の際には職員の立会いを要する。サーバ設置場所等の重要区域への立ち入りは最小限に制限する。

9　アクセス管理

各職員に固有の ID を付与し、アクセス権限は職務に応じて最小限に設定する。アクセスログは定期的に確認・保存し、不審な行為を監視する。

10　記録媒体の管理

　個人情報を含む媒体（USB、外付 HDD 等）は外部への持ち出しができないよう鍵付きで管理し、持ち出しは禁止とする。記録媒体廃棄時は、物理破壊または完全データ消去を行い、廃棄記録を残す。

11　機器の管理

　サーバ、端末、ルーター等の機器はシステム管理者が管理する。定期点検を行い、故障時は速やかに交換・修理を行う。

12　ネットワークの安全管理

　システム運用担当者は、医療情報システムの構成に応じて、 安全性が確認できるネットワーク機器を利用し、不正な機器が接続したり、不正なデータやソフトウェアが混入したり、異常なデータ通信が発生したりしないよう、セキュアなネットワークを構築し、ネットワークに接続する機器の構成を適切に管理する。外部ネットワークとの接続点はファイアウォール等で保護し、不正な通信を遮断する。

13　無線 LAN の管理

　無線 LAN を利用する場合は、適切な暗号化及び認証方式を設定し、不正利用を防止する。

14　セキュリティパッチの適用

　OS やアプリケーションの脆弱性を定期的に確認し、セキュリティパッチを速やかに適用する。

15　システム保守

　システム保守作業はシステム管理者の承認を得て実施し、作業内容を記録して確認を受ける。外部の保守会社からリモートメンテナンスを受ける場合には、責任分界点や連絡体制を事前に明確にし、必要に応じて医療情報セキュリティ開示書（SDS）等で確認する。

16　資産管理および持ち出し管理

　情報機器の資産台帳を整備し、持ち出しは禁止とする。業務上必要な場合は書面で承認を得る。

17　その他

　システム管理者は、本規程の内容を定期的に見直し、必要に応じて改定を行う。本規程に定めのない事項については、システム管理者が別途定める。

Ⅲ　電子保存における運用管理

1　真正性

　利用者ごとに認証を行い、入力者および確定者を識別できるようにする。確定操作を行った情報の内容・日時・操作者を記録し、改ざんを防止する。

2　見読性

　保存された情報は必要に応じて画面または印刷により明確に表示できる状態を維持する。障害発生時は迅速に復旧する。

3　保存性

　データは定期的にバックアップを取得し、別媒体に保管する。媒体劣化時には複写保存を行い、継続利用を保証する。

4　相互運用性

　他システムとの連携に際しては、標準フォーマットを用い、整合性および安全性を確保する。

Ⅳ　外部保存における運用管理

　クラウドサービスまたは外部事業者にデータを保存する場合は、以下の項目を遵守する。

1. 委託先の安全管理体制を確認し、契約書に責任分界点を明記する。
2. クラウド事業者の保存・暗号化・バックアップ・障害対応体制を確認する。
3. 年 1 回を目安に、委託先の運用状況を監査し、結果を記録する。
4. 契約終了時にはデータを完全に消去し、消去証明書を受領して保管する。

附則

この規程は、20●●年●●月●●日より施行する。