社会福祉法人別府発達医療センター 医療情報システム運用管理規程

第１章　総　　則

（目的）

第１条　この規程は、社会福祉法人別府発達医療センター（以下「法人」という。）において、医療情報システム（以下「システム」という。）で使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取扱い及び管理に関する事項を定め、当法人において、診療情報を適正に保存するとともに、適正に利用することを目的とする。

（対象）

第２条　対象システムは、電子カルテシステム、オーダーリングシステム、医事会計システム、検体検査システム、リハビリ支援システム、栄養管理システム、その他電子カルテシステムと連動するシステムであり、対象情報は、すべての診療に関する情報とする。

第２章　管理体制

（管理者・責任者の任命）

第３条　法人に情報システム管理者（以下「システム管理者」という。）を置き、センター長をもってこれに充てる。また、センター長は必要な場合、システム管理者を別に指名することができる。

２　情報システムを円滑に運用するため、情報システムに関する運用を担当する責任者（以下「運用責任者」という。）を置き、センター長が指名する。

３　情報システムに関する取扱い及び管理に関し必要な事項を審議するため、センター長の下に医療情報システム委員会（以下「委員会」という。）を置き、委員会の運営については別途定める。

４　その他、この規程の実施に関し必要な事項がある場合は、委員会の審議を経て、センター長がこれを定める。

（マニュアル等の文書管理体制）

第４条　マニュアル等の文書の管理については別に定める。

（監査体制と監査責任者）

第５条　システムを円滑に運用するため、システムに関する監査を担当する責任者（以下「監査責任者」という。）を置き、センター長が指名する。

２　監査責任者の責務は本規程に定めるものの他、別に定める。

３　運用責任者は、監査責任者に毎年１回、システムの監査を実施させ、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じるものとする。

４　監査の内容については、委員会の審議を経て、センター長がこれを定める。

５　システム管理者は、必要な場合、臨時の監査を監査責任者に命ずることができる。

（患者及びシステム使用者からの苦情・質問の受付体制）

第６条　患者またはシステム使用者(以下「使用者」という。)からシステムについての苦情・質問を受け付ける窓口を設置し、苦情・質問受付後は、その内容を検討し、直やかに必要な措置を講じるものとする。

（事故対策）

第７条　システム管理者は、緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、使用者に周知の上、常に利用可能な状態にしておく。

（システム使用者への教育・訓練等の周知体制）

第８条　システム管理者は、システムの取扱いについてマニュアルを整備し、使用者に周知の上、常に利用可能な状態にしておく。また、システムを正しく利用させるため、使用者に対し、定期的にシステムの取扱い及びプライバシー保護に関する教育と訓練を実施する。

（退職後の守秘規程）

第９条　法人の職員は在職中のみならず、退職後においても業務中に知った個人情報に関する守秘義務を負うものとする。

第３章　管理者、責任者及び使用者の責務

（システム管理者及び運用責任者の責務）

第 10 条　システム管理者及び運用責任者は、システムに用いる機器及びソフトウェアを導入するにあたって、システムの機能を確認し、情報システムの機能要件に挙げられている機能が支障なく運用される環境を整備する。また、診療情報の安全性を確保し、常に利用可能な状態にしておく。

２　システム管理者及び運用責任者は、機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるように維持する。

３　システム管理者は、情報システムの使用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止する。

（システム使用者の責務）
第 11 条　使用者は、自身のＩＤやパスワードを管理し、これを他者に利用させてはならない。また、システムの情報の参照や入力（以下「アクセス」という。）に際して、ＩＤやパスワードによって、システムに自身を認識させなければならない。
２　パスワードの有効期限は 60 日とし、使用者は、有効期限が経過する前に、定期的にパスワードの変更を行わなければならない。
３　使用者は、システムへの情報入力に際して、確定操作を行って入力情報に対する責任を明示しなければならない。
４　使用者は、与えられたアクセス権限を越えた操作を行ってはならない。
５　使用者は、参照した情報の目的外利用や、患者等のプライバシーを侵害してはならない。
６　使用者は、離席する際は、必ずログアウトし、窃視防止を図らなければならない。
７　使用者は、システム管理者の許可なくシステム環境を改変してはならない。
８　使用者は、ウイルスへの感染等、システムの異常や不正アクセスを発見した場合は、速やかにシステム管理者に連絡し、その指示に従わなければならない。
９　使用者は、登録情報の内容に変更が生じた際は、その内容を速やかに運用責任者に届け出なければならない。

第４章　一般管理における運用管理事項

（システムへのアクセス制限の決定方法及び記録、点検等のアクセス管理）
第 12 条　運用責任者は、使用者の職務により定められた権限によるデータアクセス範囲を定め、必要に応じてハードウェア・ソフトウェアの設定を行うこと。また、その内容に沿って、アクセス状況の確認を行い、監査責任者に報告すること。
２　運用責任者は、使用者が入力した情報について、確定操作を行った情報の記録及び更新日時を確認すること。
３　運用責任者は、使用者が情報にアクセスした記録を保存し、これを追跡調査できるようにすること。

（個人情報を含む記録媒体の管理）
第 13 条　保管及びバックアップの作業にあたる者は、手順に従って行い、その作業の記録を残し、システム管理者の承認を得ること。

（個人情報を含む媒体の破棄）
第 14 条　個人情報を含む媒体の廃棄にあたっては、安全かつ確実に行われるこ

とを、運用責任者が作業前後に確認し、結果を記録に残すこと。

（リスクに対する予防及び発生時の対処法）
第15条　システム管理者は、業務上において情報漏えい等のリスクが予想される場合は、本規程の見直しを行う。また、事故発生に対しては、速やかに運用責任者に報告し、使用者に周知すること。

（無線LANに関する事項）
第16条　システム管理者は、無線LANアクセスポイントの設定状態を適宜確認すること。

（技術的・運用的対策の分担を定めた文書の管理）
第17条　システム管理者は、各システムの設計時及び運用開始時に、技術的対策と運用による対策を基準適合チェックリストに記載し、必要時には第三者への説明に使える状態で保存すること。
２　システム管理者は、システムの保守時には、基準適合チェックリストの記載に従っていることを確認すること。
３　システム管理者は、システム改造時に、最新の基準適合チェックリストに従って、技術的対策と運用による対策の分担を見直すこと。
４　技術的対策の内容は「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」別紙に示す「サービス仕様適合開示書」等で確認すること。

第５章　業務委託の安全管理措置

（委託契約における安全管理）
第18条　業務を外部の業者等に委託する場合は、秘密保持事項を含む業務委託契約を締結する。また、システム管理者は、委託作業内容が個人情報保護の観点から適正かつ安全に行われていることを確認すること。

（再委託の場合の安全管理措置）
第19条　業務委託契約書には、再委託での安全管理に関する事項を含むものとすること。

第６章　情報及び情報機器の持ち出しについて

（持ち出し対象となる情報及び情報機器）
第20条　システム管理者は、情報及び情報機器の持ち出しに関しリスク分析を行い、持ち出し対象となる情報及び情報機器を規定し、それ以外の情報及び情報機器の持ち出しを禁止すること。

２　持ち出し対象となる情報若しくは情報機器は別表としてまとめ、使用者に公開すること。

（持ち出した情報及び情報機器の運用管理）

第 21 条　使用者は、情報及び情報機器を持ち出す場合は、所属、氏名、連絡先、持ち出す情報の内容、格納する媒体、持ち出す目的、期間を別途定める書式でシステム管理者に届け出て、承認を得なければならない。

２　システム管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録するとともに、その内容を定期的にチェックし、所在状況を把握すること。

（持ち出した情報及び情報機器への安全管理措置）

第 22 条　運用責任者は、持ち出す情報機器について起動パスワード等を設定する。推定しやすいパスワード等の利用を避ける等、適切なパスワードの設定・運用を行うこと。

２　運用責任者は、持ち出す情報機器については、必要なセキュリティ対策を講じておくこと。

３　使用者は、公衆無線 LAN を使用してはならない。

４　使用者は、持ち出した情報機器には、別途定められている以外のアプリケーションをインストールしてはならない。また、承認されていないサービスを利用してはならない。

（盗難、紛失時の対応策）

第 23 条　使用者は、持ち出した情報及び情報機器の盗難、紛失時には、直ちにシステム管理者に届け出なければならない。

２　届出を受け付けたシステム管理者は、その情報及び情報機器の重要度にしたがって、必要な対応策を講じること。

第 7 章　外部の機関と医療情報を交換する場合

（技術的・運用的面からの安全の確認）

第 24 条　システム管理者は、外部の機関と医療情報を交換する場合、リスク分析を行い、安全に運用されるように別途定める技術的及び運用的対策を講じること。

２　監査責任者は、技術的対策が適切に実施され問題がないかを定期的に監査を行って確認すること。

（リモートメンテナンスの基本方針）

第 25 条　システム管理者は、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、相手の保守会社等、電気通信事業者、運用委託業者等との間で、責任分界点や責任の所在を契約書等で明確にすること。

２　監査責任者は、上記契約状態が適切に維持管理されているか定期的に監査を行って確認すること。

第８章　自然災害やサイバー攻撃等による非常時の対策

（災害等の非常時の運用）

第 26 条　システム管理者は、災害、サイバー攻撃等により、一部医療行為の停止等、医療サービス提供体制に支障が発生する非常時の場合、別途定める事業継続計画(BCP)に従って運用を行うこと。

（システムの縮退運用管理）

第 27 条　システム管理者は、システムの縮退運用時や非常時の運用に関して運用管理規程を作成し、使用者に周知の上、常に利用可能な状態にしておくこと。

（報告先と内容一覧）

第 28 条　システム管理者は、災害、 コンピュータウイルスの感染などによるサイバー攻撃を受けた（疑い含む）場合、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる、またはそのおそれがある事案であると判断した等の場合には、別途定める一覧の連絡先に連絡すること。

附　則

１　この規程は、令和３年１２月１日から施行する。