○　地方独立行政法人筑後市立病院個人情報安全管理要領

令和８年３月27日
要領等第32号

（目的）

第１条　この要領は、「地方独立行政法人筑後市立病院個人情報取扱要綱」（令和８年要綱第36号。以下「要綱」という。）第９条第２項の規定に基づき、地方独立行政法人筑後市立病院（以下「法人」という。）における個人情報の漏えい、滅失又は毀損の防止その他の安全管理のために講ずべき措置の具体的な事項を定めることを目的とする。

（組織的安全管理措置）

第２条　法人における組織的な安全管理措置として、次の事項を実施する。

(1)　管理体制の構築　要綱第４条に基づき最高情報責任者（CIO）を置き、各部署に情報管理責任者（各部署の長）を配置して、報告連絡体制を整備する。

(2)　規程等の運用　安全管理措置に関する内部規範を遵守し、運用の状況を記録する。

(3)　点検及び監査　情報システム管理部会は、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き、定期的に自己点検及び監査を実施する。

(4)　漏えい等事案への対応　役職員等は、漏えい等の事案又はその兆候を把握したときは、要綱第13条に基づき直ちに部署責任者に報告し、CIOの指示を受けなければならない。

（人的安全管理措置）

第３条　法人における人的な安全管理措置として、次の事項を実施する。

(1)　役職員等の義務　役職員等は、職務上知り得た個人情報をみだりに他人に知らせ、又は不当な目的に使用してはならない。その職を退いた

後も同様とする。

(2)　教育及び啓発　CIO及び情報システム管理部会は、役職員等に対し、個人情報の保護及びサイバーセキュリティに関する教育を定期的に実施する。

（物理的安全管理措置）

第４条　個人情報を取り扱う区域及び情報資産の物理的な保護のため、次の措置を講じる。

(1)　入退室管理　サーバー室等の重要区域については、入退室の制限及び記録を行う。

(2)　盗難防止　個人情報を取り扱う機器、電子媒体及び書類等の盗難又は紛失を防止するため、施錠管理等の措置を講じる。

(3)　廃棄　個人情報が記録された書類や媒体を廃棄する場合は、復元不可能な方法で裁断、溶解又は消去を行う。

（技術的安全管理措置）

第５条　情報システムにおける個人情報の保護のため、次の措置を講じる。

(1)　アクセス制御　業務上の必要性に応じ、情報システムへのアクセス権限を最小限に制限する。

(2)　識別と認証　ユーザーID、パスワード等により、情報システムを利用する者の識別と認証を行う。

(3)　真正性の確保　電子カルテ等の記載にあたっては、修正履歴を適切に保持し、確定した原記録を不当に消去しない。

(4)　外部攻撃対策　コンピュータウイルス対策ソフトの導入及び最新化、不正アクセス監視等のサイバー攻撃対策を講じる。

(5)　利用履歴の記録　情報システムへのアクセスログ及び個人情報の処理履歴を一定期間保存し、不適切なアクセスの有無を定期的に確認する。

（外部委託の管理）

第６条　個人情報の取扱いの全部又は一部を外部に委託するときは、要綱第10条の規定に基づき、再委託の制限、安全管理、情報の返還又は廃棄、事故時の報告義務等を契約書に明記し、委託先を適切に監督する。

（事業継続計画の策定）

第７条　CIOは、サイバー攻撃、大規模災害又はシステム障害の発生時に備え、診療機能への影響を最小限に留めるための事業継続計画（BCP）を策定し、定期的な訓練を行う。

（委任）

第８条　この要領に定めるもののほか、個人情報の安全管理に関し必要な事項は、CIOが別に定める。

付　則（令和８年３月27日決裁）

この要領は、決裁の日から施行し、令和８年４月１日から適用する。