

地方独立行政法人長崎市立病院機構個人データ等安全管理措置規程

令和5年10月4日

規程第25号

目次

- 第1章 総則（第1条・第2条）
- 第2章 管理体制（第3条—第8条）
- 第3章 教育研修（第9条）
- 第4章 職員等の責務（第10条）
- 第5章 個人データ等の取扱い（第11条—第19条）
- 第6章 情報システムにおける安全の確保等（第20条—第34条）
- 第7章 サーバ室等の安全管理（第35条・第36条）
- 第8章 個人データ等の提供及び業務の委託等（第37条・第38条）
- 第9章 安全確保上の問題への対応（第39条—第41条）
- 第10章 監査及び点検の実施（第42条—第44条）
- 第11章 雑則（第45条・第46条）

附則

第1章 総則

（目的）

第1条 この規程は、地方独立行政法人長崎市立病院機構（以下「本機構」という。）
が取り扱う個人データ、個人番号及び特定個人情報（以下「個人データ等」とい
う。）の適切な管理に関し必要な事項を定めることを目的とする。

（定義）

第2条 この規程における用語の定義は、個人情報の保護に関する法律（平成15
年法律第57号。以下「法」という。）及び行政手続における特定の個人を識別す
るための番号の利用等に関する法律（平成25年法律第27号。以下「番号法」
という。）の定めるところによる。

第2章 管理体制

（総括保護管理者）

第3条 個人データ等の管理に関する事務を総括するため、総括保護管理者を置き、理事長が任命する者をもって充てる。

(副総括保護管理者)

第4条 総括保護管理者が行う個人データ等の管理に関する事務を補佐するため、副総括保護管理者を置き、理事長補佐、副院長、看護部長及び事務部長をもって充てる。

(保護管理者)

第5条 部署（地方独立行政法人長崎市立病院機構組織規程（平成25年地方独立行政法人長崎市立病院機構規程第6号）第3条第3項の表の中欄に規定する課及び同規程第4条の左欄に規定する室、科、部（事務部を除く。）及びセンターをいう。以下同じ。）における個人データ等の適切な管理を確保するため、保護管理者を置き、各部署の長をもって充てる。ただし、看護部の保護管理者にあつては、看護副部長をもって充てる。

2 前項に定めるもののほか、保護管理者は、個人データ等を情報システムで取り扱う場合は、当該情報システムの情報システム管理者と連携し、その任に当たる。

3 保護管理者は、次に掲げる事項を指定する。

(1) 個人番号及び特定個人情報（以下「特定個人情報等」という。）を取り扱う職員（以下「特定個人情報等取扱者」という。）並びにその役割

(2) 特定個人情報等取扱者が取り扱う特定個人情報等の範囲

(保護担当者)

第6条 各部署に保護担当者を置き、当該各部署の保護管理者が指名する職員をもって充てる。

2 前項の保護担当者は、保護管理者を補佐し、各部署における個人データ等の管理に関する事務を行う。

(監査責任者)

第7条 個人データ等の管理の状況について監査するため、監査責任者を置き、総括保護管理者が任命する者をもって充てる。

(個人データ等の適切な管理のための会議)

第8条 総括保護管理者は、個人データ等の管理に係る重要事項の決定、連絡、調整等を行うため必要があると認めるときは、関係職員を構成員とする会議を定期的に又は随時に開催する。

2 総括保護管理者は、必要に応じて前項の会議に情報セキュリティ等について専門的な知識及び経験を有する者の参加を求めることができる。

第3章 教育研修

第9条 総括保護管理者は、個人データ等の取扱いに従事する職員等（地方独立行政法人長崎市立病院機構再任用職員就業規程（平成24年地方独立行政法人長崎市立病院機構規程第12号）第2条第1号に規定する再任用職員、地方独立行政法人長崎市立病院機構任期付職員就業規程（平成24年地方独立行政法人長崎市立病院機構規程第13号）第1条に規定する任期付職員、地方独立行政法人長崎市立病院機構非常勤職員就業規程（平成24年地方独立行政法人長崎市立病院機構規程第14号）第2条に規定する非常勤職員及び労働者派遣事業の適正な運営の確保及び派遣労働者の保護等に関する法律（昭和60年法律第88号）第2条第2号に規定する派遣労働者（以下第37条第7項において単に「派遣労働者」という。）を含む。以下同じ。）に対し、個人データ等の取扱いについて理解を深め、個人データ等の保護に関する意識の高揚を図るための啓発その他を目的として必要な教育研修を実施する。

2 総括保護管理者は、個人データ等を取り扱う情報システムの管理に関する事務に従事する職員に対し、個人データ等の適切な管理のために、情報システムの管理、運用及びセキュリティ対策に関し必要な教育研修を実施する。

3 総括保護管理者は、副総括保護管理者、保護管理者及び保護担当者に対し、各部署における個人データ等の適切な管理のための教育研修を定期的実施する。

4 保護管理者は、各部署の職員等に対し、個人データ等の適切な管理のため、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。

第4章 職員等の責務

第10条 職員等は、法及び番号法の趣旨にのっとり、関連する法令、規則等並びに

総括保護管理者、副総括保護管理者、保護管理者及び保護担当者（以下「総括保護管理者等」という。）の指示に従い、個人データ等を取り扱わなければならない。

第5章 個人データ等の取扱い

（アクセス制限）

第11条 保護管理者は、個人データ等の秘匿性等その内容に応じ、当該個人データ等にアクセス（紙に記録されている個人データ等に接する行為を含む。以下同じ。）

権限を有する職員等の範囲及び権限の内容を、当該職員等が業務を行う上で必要最小限の範囲に限る。

2 前項のアクセス権限を有しない職員等は、個人データ等にアクセスしてはならない。

3 職員等は、アクセス権限を有する場合であっても、業務上の目的以外の目的で個人データ等にアクセスしてはならず、必要最小限としなければならない。

（複製等の制限）

第12条 職員等が、業務上の目的で個人データ等を取り扱う場合であっても、保護管理者は、次に掲げる行為については、当該個人データ等の秘匿性等その内容に応じて、当該行為を行うことができる場合を必要最小限に限定し、当該職員等は、当該保護管理者の指示に従い行う。

(1) 個人データ等の複製又は送信

(2) 個人データ等が記録されている媒体の外部への送付又は持ち出し

(3) その他個人データ等の適切な管理に支障を及ぼすおそれのある行為

（誤りの訂正等）

第13条 職員等は、個人データ等の内容に誤りを発見した場合には、保護管理者の指示に従い、訂正、追加又は削除を行う。

（媒体の管理等）

第14条 職員等は、保護管理者の指示に従い、個人データ等が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管及び施錠を行う。

2 個人データ等が記録されている媒体を外部へ送付し、又は持ち出す場合には、原

則として、パスワード（情報システムに接続する際に入力する暗証番号をいう。）、ICカード、生体情報（以下「パスワード等」という。）を使用して権限を識別する機能（以下「認証機能」という。）を設定し、必要な措置を講ずる。

（誤送付等の防止）

第15条 職員等は、個人データ等を含む電磁的記録又は媒体の誤送信、誤送付、誤交付又はウェブサイト等への誤掲載を防止するため、個別の事務又は事業において取り扱う個人情報の秘匿性等その内容に応じ、複数の職員等で確認できるよう必要な措置を講ずる。

（廃棄等）

第16条 職員等は、個人データ等又は個人データ等が記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者又は情報システム責任者の指示に従い、当該個人データ等の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。

2 個人データ等の消去又は個人データ等が記録されている媒体の廃棄を委託する場合（2以上の段階にわたる委託を含む。）には、必要に応じて職員が消去及び廃棄に立ち会い、又は写真を付した消去及び廃棄を証明する書類を受け取り、委託先において消去及び廃棄が確実に行われていることを確認する。

（個人データ等の取扱状況の記録）

第17条 保護管理者は、個人データ等の秘匿性等その内容に応じて、台帳等を整備して、当該個人データ等の利用及び保管等の取扱いの状況について記録する。

（外的環境の把握）

第18条 個人データ等が、外国において取り扱われる場合、当該外国の個人情報等の保護に関する制度等を把握した上で、個人データ等の安全管理のために必要かつ適切な措置を講じなければならない。

（個人番号の利用の制限等）

第19条 保護管理者は、個人番号の利用に当たり、番号法があらかじめ限定的に定めた事務に限定する。

2 特定個人情報等取扱者は、個人番号関係事務を処理するために必要な場合その他

番号法で定める場合を除き、個人番号の提供を求めてはならない。

- 3 特定個人情報等取扱者は、個人番号関係事務を処理するために必要な場合その他番号法で定める場合を除き、特定個人情報ファイルを作成してはならない。
- 4 特定個人情報等取扱者は、番号法第19条各号のいずれかに該当する場合を除き、他人の個人番号を含む個人情報を収集し、及び保管してはならない。
- 5 保護管理者は、特定個人情報等を取り扱う事務を実施する区域を明確にし、物理的な安全管理措置を講ずる。

第6章 情報システムにおける安全の確保等

(アクセス制御)

第20条 保護管理者は、個人データ等（情報システムで取り扱うものに限る。以下この章（第32条を除く。）において同じ。）の秘匿性等その内容に応じて、認証機能を設定し、アクセス制御のために必要な措置を講ずる。

- 2 保護管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めを整備するとともに、パスワード等の読取防止を行うために必要な措置を講ずる。

(アクセス記録)

第21条 保護管理者は、個人データ等の秘匿性等その内容に応じて、当該個人データ等へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を効率的かつ確実に分析するために必要な措置を講ずる。

- 2 保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。

(アクセス状況の監視)

第22条 保護管理者は、個人データ等の秘匿性等その内容に応じて、当該個人データ等への不適切なアクセスの監視のため、アクセス記録又は操作記録の定期的な点検又は分析を実施する。

(管理者権限の設定)

第23条 保護管理者は、個人データ等の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操

作の防止のため、当該特権を最小限とする等の必要な措置を講ずる。

(外部からの不正アクセスの防止)

第24条 保護管理者は、個人データ等を取り扱う情報システムへの外部からの不正アクセス（アクセス権限を有しない者が情報システムの内部へ侵入を行う行為をいう。以下同じ。）を防止するため、ファイアウォール（外部の通信回線（以下「ネットワーク」という。）からの不正なアクセスを防御する仕組みをいう。）の設定による経路制御等の必要な措置を講ずる。

(不正プログラムによる漏えい等の防止)

第25条 保護管理者は、不正プログラム（情報システムに害悪な動作をさせるデータをいう。以下同じ。）による個人データ等の漏えい、滅失又は毀損の防止のため、ソフトウェア（情報システムを動作させるためのデータをいう。以下同じ。）に関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置を講ずる。

(情報システムにおける個人データ等の処理)

第26条 職員等は、個人データ等について、一時的に加工の処理を行うため複製を行う場合には、その対象を必要最小限に限り、処理終了後は不要となった情報を速やかに消去する。この場合において、保護管理者は、当該個人データ等の秘匿性等その内容に応じて、随時、消去の実施状況を重点的に確認する。

(暗号化等)

第27条 保護管理者は、個人データ等の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずる。

2 職員等は、前項の措置を踏まえ、その処理する個人データ等について、当該個人データ等の秘匿性等その内容に応じて、適切に暗号化又はパスワードの付与を行う。

(記録機能を有する外部電磁的記録媒体の接続制限)

第28条 保護管理者は、個人データ等の秘匿性等その内容に応じて、当該個人データ等の漏えい等の防止のため、記録機能を有する外部の電磁的記録媒体の情報システム端末への接続を制限（当該機器の更新への対応を含む。）する。

(端末の限定)

第29条 保護管理者は、個人データ等の秘匿性等その内容に応じて、その処理を行う端末を限定するために必要な措置を講ずる。

(端末の盗難防止等)

第30条 保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講ずる。

2 職員等は、保護管理者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

(第三者の閲覧防止)

第31条 職員等は、端末の使用に当たっては、個人データ等が第三者に閲覧されることがないように、使用状況に応じて情報システムからログオフ（情報システムの利用を終了することをいう。）を行うことを徹底する等の必要な措置を講ずる。

(入力情報の照合等)

第32条 職員等は、情報システムで取り扱う個人データ等について、当該情報システムに入力する元となる申請書等と当該情報システムに入力する内容との照合、処理前後の当該個人データ等の内容の確認、既存の個人データ等との照合等を行う。

(バックアップ)

第33条 保護管理者は、個人データ等について、他の電磁的記録媒体に複製を作成し、分散保管するために必要な措置を講ずる。

(情報システム設計書等の管理)

第34条 保護管理者は、個人データ等に係る情報システムの設計書、構成図等の文書について関係部署以外に知られることがないように、その保管、複製、廃棄等について必要な措置を講ずる。

第7章 サーバ室等の安全管理

(入退管理)

第35条 保護管理者は、個人データ等を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「サーバ室等」という。）に立ち入る権限を有する者を定めるとともに、用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員等の立会い又は監視設備による監視、外部電磁的記録媒体等の持ち込

み、利用及び持ち出しの制限又は検査等の措置を講ずる。個人データ等を記録する媒体を保管するための施設を設けている場合においても、必要があると認めるときは、同様の措置を講ずる。

2 保護管理者は、必要があると認めるときは、サーバ室等の出入口の特定による入退管理の容易化、所在表示の制限等の措置を講ずる。

3 保護管理者は、サーバ室等の保管施設の入退管理について、必要があると認めるときは、立入りに係る認証機能を設定し、及びパスワード等の管理に関する定めを整備及びパスワード等の読取防止を行うために必要な措置を講ずる。

(サーバ室等の管理)

第36条 保護管理者は、外部からの不正な侵入に備え、サーバ室等に施錠装置の設置等の措置を講ずる。

2 保護管理者は、災害等に備え、サーバ室等に、耐震、防火、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずる。

第8章 個人データ等の提供及び業務の委託等

(個人データ等の提供)

第37条 保護管理者は、法第27条第1項各号の規定により、行政機関等以外の者に本機構が取り扱う個人データを提供する場合には、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わす。

2 保護管理者は、法第27条第1項各号の規定により、行政機関等以外のものに本機構が取り扱う個人データを提供する場合には、安全確保の措置を要求するとともに、必要があると認めるときは、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求の措置を講ずる。

3 保護管理者は、法第27条第1項第4号の規定により、行政機関等に本機構が取り扱う個人データを提供する場合において、必要があると認めるときは、前2項に規定する措置を講ずる。

4 職員等は、番号法で限定的に明記された場合を除き、特定個人情報等を提供して

はならない。

(業務の委託等)

第38条 個人データ等の取扱いに係る業務を外部に委託する場合には、個人情報(特定個人情報等を含む。以下この条において同じ。)の適切な管理を行う能力を有しないものを選定することがないよう、必要な措置を講ずる。この場合において、契約書、仕様書等に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者の管理体制及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。

- (1) 個人情報に関する秘密保持、利用目的以外の目的のための利用の禁止等の義務
- (2) 再委託(再委託先が委託先の子会社(会社法(平成17年法律第86号)第2条第1項第3号に規定する子会社をいう。)である場合も含む。以下この項及び第4項において同じ。)の制限又は事前承認等の条件に関する事項
- (3) 個人情報の複製に関する事項
- (4) 個人情報の安全管理措置に関する事項
- (5) 個人情報の漏えい等の事案の発生時における対応に関する事項
- (6) 委託終了時における個人情報の消去及び媒体の返却に関する事項
- (7) 違反した場合における契約解除、損害賠償責任その他必要な事項
- (8) 契約内容の遵守状況についての定期的報告に関する事項及び委託先における委託された個人情報の取扱状況を把握するための監査等に関する事項(再委託先の監査等に関する事項を含む。)

2 個人番号利用事務等の取扱いに係る業務を外部に委託する場合には、委託先において、番号法に基づき行政機関が果たすべき措置と同等の措置が講じられるか否かについて、あらかじめ確認するものとする。この場合において、契約書、仕様書等に、前項各号に掲げる事項及び次に掲げる事項を明記する。

- (1) 事務所等内からの個人番号及び特定個人情報の持ち出しの禁止に関する事項
- (2) 個人番号及び特定個人情報を取り扱う従事者の明確化及び従事者の監督・教育に関する事項
- (3) 契約内容の遵守状況の報告に関する事項

- (4) 必要に応じて実施可能とする委託先に対する実地の調査に関する事項
- 3 個人データ等の取扱いに係る業務を外部に委託する場合には、取扱いを委託する個人情報の範囲は、委託する業務内容に照らして必要最小限でなければならない。
- 4 個人データ等の取扱いに係る業務を外部に委託する場合には、委託する業務に係る個人データ等の秘匿性等その内容に応じて、委託先における管理体制及び実施体制又は個人情報の管理の状況について、実地検査又は書面による報告により確認することができる。
- 5 委託先において、個人データ等の取扱いに係る業務が再委託される場合には、委託先に第1項に規定する措置を講じさせるとともに、再委託される業務に係る個人データ等の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項に規定する措置を実施する。個人データ等の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。
- 6 個人データ等を提供し、又は業務委託する場合には、漏えい等による被害発生のリスクを低減する観点から、提供先の利用目的、委託する業務の内容、個人データ等の秘匿性等その内容などを考慮し、必要に応じ、特定の個人を識別することができる記載の全部又は一部を削除し、又は別の記号等に置き換える等の措置を講ずる。
- 7 個人データ等の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記する。

第9章 安全確保上の問題への対応

(事案の報告及び再発防止措置)

第39条 個人データ等の漏えい等安全管理の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合に、その事案等を認識した職員等は、理事長が別に定める方法に基づき、直ちに当該保有個人情報を管理する保護管理者に報告する。

- 2 保護管理者は、前項の認識をした場合は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセス、不正プログラムの感染が疑われる当該端末等のネットワークの切断等の被害の拡大防止のため直ちに行い得る措置については、直ちに行うものとする。

3 保護管理者は、事案の発生した経緯、被害状況等を調査し、総括保護管理者に報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。

4 保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずるとともに、同種の業務を実施している部署に再発防止措置を共有する。

(法に基づく報告及び通知)

第40条 個人データ等の漏えい等が生じた場合であって法第26条第1項の規定による個人情報保護委員会への報告及び同条第2項の規定による本人への通知を要する場合には、前条第1項から第4項までの規定によるものと並行して、速やかに所定の手続を行うとともに、個人情報保護委員会による事案の把握等に協力する。

(公表等)

第41条 保護管理者は、法第26条第1項の規定による報告及び同条第2項の規定による本人への通知を要しない場合であっても、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る個人データ等の本人への対応等の措置を講ずる。

2 患者等の不安を招きかねない事案（公表を行う漏えい等が発生したとき、個人情報保護に関連する法令、規則等の違反があったとき、委託先において個人情報の適切な管理に関する契約条項等に対する違反があったとき等をいう。）については、公表を行う事案については、当該事案の内容、経緯、被害状況等について、速やかに個人情報保護委員会に情報提供を行う。

第10章 監査及び点検の実施

(監査)

第42条 監査責任者は、個人データ等の適切な管理を検証するため、第2章から前章までに規定する措置の状況を含む各部署等における個人データ等の管理の状況について、定期的に及び必要に応じ随時に監査（外部監査を含む。以下同じ。）を行い、その結果を総括保護管理者に報告する。

(点検)

第43条 保護管理者は、各部署における個人データ等の記録媒体、処理経路、保管

方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告する。

(評価及び見直し)

第44条 総括保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から個人データ等の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講ずる。

第11章 雑則

(サイバーセキュリティに関する対策の基準等)

第45条 個人情報を取り扱い、又は情報システムを構築し、若しくは利用するに当たっては、サイバーセキュリティ基本法（平成26年法律第104号）第26条第1項第2号に掲げられたサイバーセキュリティに関する対策の基準を参考として、取り扱う個人データ等の性質等に照らして適正なサイバーセキュリティ（情報の機密性、完全性及び可用性を確保することをいう。）の水準を確保する。

(委任)

第46条 この規程に定めるもののほか、必要な事項は、理事長が別に定める。

附 則

この規程は、公布の日から施行する。