

群馬大学医学部附属病院の保有する診療関連個人情報管理規程

平成21. 1. 13 制定

改正 平成24. 4. 10 平成27. 12. 8

平成30. 4. 1 平成30. 11. 16

令和 4. 4. 1

目次

- 第1章 総則（第1条・第2条）
- 第2章 管理体制（第3条―第6条）
- 第3章 教育研修（第7条）
- 第4章 職員等の責務（第8条）
- 第5章 診療関連個人情報の取扱い（第9条―第14条）
- 第6章 病院情報システムにおける安全の確保等（第15条―第29条）
- 第7章 情報システム室等の安全管理（第30条・第31条）
- 第8章 診療関連個人情報の提供及び業務の委託等（第32条・第33条）
- 第9章 安全確保上の問題への対応（第34条・第35条）
- 第10章 点検の実施等（第36条・第37条）
- 第11章 雑則（第38条・第39条）
- 附則

第1章 総則

（趣旨）

第1条 この規程は、国立大学法人群馬大学個人情報管理規程（平成17年4月1日制定。以下「管理規程」という。）第39条の規定に基づき、群馬大学医学部附属病院（以下「本院」という。）の保有する、診療関連の個人情報（以下「診療関連個人情報」という。）の管理に関し必要な事項を定める。

（定義）

第2条 この規程における用語の意義は、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。）第2条、第16条及び第60条の定めるところによる。

第2章 管理体制

（保護管理者）

第3条 本院に、保護管理者を置き、病院長をもって充てる。

2 保護管理者は、本院における診療関連個人情報の適切な管理を確保する。診療関連個人情報を情報システムで取り扱う場合、保護管理者は、当該情報システムの管理者と連携する。

（統括副保護管理者）

第4条 本院に、統括副保護管理者を置き、副病院長をもって充てる。

2 統括副保護管理者は、保護管理者の命を受け、診療関連個人情報を適切に管理する。

(副保護管理者)

第5条 診療科、中央診療施設等、薬剤部及び看護部（以下「診療科等」という。）に、副保護管理者を置き、当該診療科等の長をもって充てる。

2 副保護管理者は、保護管理者の職務を分任し、各診療科等の診療関連個人情報を適切に管理する。

(保護担当者)

第6条 本院に保護担当者を置き、各診療科等の教員等をもって充てる。

2 保護担当者は、保護管理者、統括副保護管理者及び副保護管理者を補佐し、当該診療科等における診療関連個人情報の保護に関する業務を担当する。

第3章 教育研修

(教育研修)

第7条 保護管理者は、職員等（診療関連個人情報を取り扱うことのある学生及び派遣労働者を含む。以下同じ。）に対し、診療関連個人情報の適切な管理のために、管理規程第3条に規定する総括保護管理者（以下「総括保護管理者」という。）の実施する教育研修又は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ものとする。

第4章 職員等の責務

(職員等の責務)

第8条 職員等は、法の趣旨に則り、関連する法令、規程等の定め並びに総括保護管理者、保護管理者、統括副保護管理者、副保護管理者及び保護担当者の指示に従い、診療関連個人情報を取り扱わなければならない。

第5章 診療関連個人情報の取扱い

(アクセス制限)

第9条 保護管理者は、診療関連個人情報の秘匿性等その内容に応じて、当該診療関連個人情報にアクセスする権限を有する職員等とその権限の内容を、当該職員等が業務を行う上で必要最小限の範囲に限るものとする。

2 アクセス権限を有しない職員等は、診療関連個人情報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診療関連個人情報にアクセスしてはならない。

(複製等の制限)

第10条 職員等が、業務上の目的で診療関連個人情報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、当該診療関連個人情報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限定し、職員等は、副保護管理者の指示に従い行うものとする。

- (1) 診療関連個人情報の複製
- (2) 診療関連個人情報の送信
- (3) 診療関連個人情報が記録されている媒体の外部への送付又は持出し
- (4) その他診療関連個人情報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11条 職員等は、診療関連個人情報の内容に誤り等を発見した場合には、副保護管理者の指示に従い、訂正等を行うものとする。

(媒体の管理等)

第12条 職員等は、副保護管理者の指示に従い、診療関連個人情報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、施錠等を行うものとする。

(廃棄等)

第13条 職員等は、診療関連個人情報又は診療関連個人情報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、副保護管理者の指示に従い、復元又は判読が不可能となる方法により当該情報の消去又は当該媒体の廃棄を行うものとする。

(診療関連個人情報の取扱状況の記録)

第14条 副保護管理者は、診療関連個人情報の秘匿性等その内容に応じて、台帳等を整備して、診療関連個人情報の利用、保管等の取扱いの状況について記録するものとする。

第6章 病院情報システムにおける安全の確保等

(アクセス制御)

第15条 保護管理者は、診療関連個人情報（病院情報システムで取り扱うものに限る。以下本章（第23条を除く。）において同じ。）の秘匿性等その内容に応じて、パスワード等（パスワード、ICカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずるものとする。

- 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（その定期又は随時の見直しを含む。）するとともに、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

(アクセス記録)

第16条 保護管理者は、診療関連個人情報の秘匿性等その内容に応じて、診療関連個人情報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

録を定期的に分析するために必要な措置を講ずるものとする。

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ものとする。

(アクセス状況の監視)

第17条 保護管理者は、診療関連個人情報の秘匿性等その内容及びその量に応じて、当該診療関連個人情報への不適切なアクセスの監視のため、診療関連個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認等の必要な措置を講ずる。

(管理者権限の設定)

第18条 保護管理者は、診療関連個人情報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等の防止のため、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19条 保護管理者は、診療関連個人情報を取り扱う病院情報システムへの外部からの不正アクセスを防止するため、経路制御等の必要な措置を講ずるものとする。

(不正プログラムによる漏えい等の防止)

第20条 保護管理者は、不正プログラムによる診療関連個人情報の漏えい、滅失又は毀損の防止のため、ソフトウェア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(導入したソフトウェアを常に最新の状態に保つことを含む。)を講ずるものとする。

(情報システムにおける診療関連個人情報の処理)

第21条 職員等は、診療関連個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、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。保護管理者は、当該診療関連個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認する。

(暗号化)

第22条 保護管理者は、診療関連個人情報が二次利用される場合においては、暗号化のために必要な措置を講ずるものとする。

職員等は、これを踏まえ、その処理する診療関連個人情報について、当該診療関連個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。

(入力情報の照合等)

第23条 職員等は、病院情報システムで取り扱う診療関連個人情報を入力するときは、入力原票と入力後の当該診療関連個人情報の内容との照合等を行うものとする。

(バックアップ)

第24条 保護管理者は、診療関連個人情報のバックアップを作成し、分散保管するために必要な措置を講ずるものとする。

(情報システム設計書等の管理)

第25条 保護管理者は、診療関連個人情報に係る情報システムの設計書、構成図等の文書について外部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。

(端末の限定)

第26条 保護管理者は、診療関連個人情報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ものとする。

(端末の盗難防止等)

第27条 保護管理者は、端末の盗難又は紛失の防止のため、24時間職員が常駐する場所を除き端末の固定、執務室の施錠等の必要な措置を講ずるものとする。

2 職員等は、保護管理者が必要が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28条 職員等は、端末の使用に当たっては、診療関連個人情報が第三者に閲覧されることがないように、使用状況に応じて病院情報システムからログオフを行うことを徹底する等の必要な措置を講ずるものとする。

(記録機能を有する機器・媒体の接続制限)

第29条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、スマートフォン、USBメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。

第7章 情報システム室等の安全管理

(入退管理)

第30条 保護管理者は、診療関連個人情報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「情報システム室等」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ものとする。また、診療関連個人情報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、同様とする。

2 保護管理者は、情報システム室等の出入口の特定化による入退の管理の容易化、所在表示の制限等の措置を講ずるものとする。

3 保護管理者は、情報システム室等及び保管施設の入退の管理について、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（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

（情報システム室等の管理）

第31条 保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置及び監視設備の設置等の措置を講ずるものとする。

2 保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、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ものとする。

第8章 診療関連個人情報の提供及び業務の委託等

（診療関連個人情報の提供）

第32条 保護管理者は、法第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に診療関連個人情報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ものとする。

2 保護管理者は、法第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に診療関連個人情報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、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、改善要求等の措置を講ずるものとする。

3 保護管理者は、法第9条第2項第3号の規定に基づき行政機関又は独立行政法人等に診療関連個人情報を提供する場合において、前2項に規定する措置を講ずるものとする。

（業務の委託等）

第33条 診療関連個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないように、必要な措置を講ずるものとする。また、契約書に、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ものとする。

- (1) 個人情報に関する秘密保持、目的外利用の禁止等の義務
- (2) 再委託の制限又は事前承認等再委託に係る条件に関する事項
- (3) 個人情報の複製等の制限に関する事項
- (4) 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
- (5) 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
- (6) 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

2 診療関連個人情報の取扱いに係る業務を外部に委託する場合には、委託する診療関連個人情報の秘匿性等その内容に応じて、委託先における診療関連個人情報の管理の状況について、年1回以上の定期的検査等により確認する。

3 委託先において、診療関連個人情報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項の措置を講じさせるとともに、再委託される業務に係る診療関連個人情報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第2項の措置を実施する。診療関連個人情報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。

- 4 診療関連個人情報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ものとする。

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34条 診療関連個人情報の漏えい等安全確保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、直ちに保護管理者に報告するものとする。

- 2 保護管理者は、被害の拡大防止、復旧等のために必要な措置を速やかに講ずるものとする。ただし、外部からの不正アクセスや不正プログラムの感染が疑われる当該端末等のLANケーブルを抜くなど、被害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(職員等に行わせることを含む)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ものとする。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ものとする。
- 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ものとする。

(公表等)

第35条 保護管理者は、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、当該事案に係る診療関連個人情報の本人への対応等の措置を総括保護管理者と協議の上、講ずるものとする。

第10章 点検の実施等

(点検)

第36条 保護管理者は、各診療科等における診療関連個人情報の記録媒体、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ものとする。

(評価及び見直し)

第37条 保護管理者等は、点検又は管理規程第35条に定める監査の結果等を踏まえ、実効性等の観点から診療関連個人情報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じ、総括保護管理者に報告するものとする。

第11章 雑則

(雑則)

第38条 この規程に定めるもののほか、本院の診療関連個人情報の管理について必要な事項は、別に定

めるところによる。

(規程の改廃)

第39条 この規程の改廃は、病院運営会議の議を経て、病院長が行う。ただし、法令等に基づく条文の整備又は所掌事務を遂行するために必要な改正、その他軽微な改正に関しては、会議への付議を省略することができる。

附 則

この規程は、平成21年1月13日から施行する。

附 則

この規程は、平成24年4月10日から施行する。

附 則

この規程は、平成27年12月8日から施行する。

附 則

この規程は、平成30年4月1日から施行する。

附 則

この規程は、平成30年11月16日から施行する。

附 則

この規程は、令和4年4月1日から施行する。