○　山梨大学医学部附属病院の保有する個人情報の適切な管理のための措置に関する規程

制定　平成２９年　８月　２日
改正　令和　３年　９月２９日

第１章　趣旨

第１条　この規程は、山梨大学医学部附属病院（以下「病院」という。）の保有する個人情報の適切な管理のために必要な事項を定める。

第２章　定義

第２条　この規程における用語の定義は、国立大学法人山梨大学個人情報保護規則第２条の定めるところによる。

第３章 管理体制

（保護管理者）
第３条　国立大学法人山梨大学保有個人情報管理細則（以下「管理細則」という。）第４条の規定に基づき、病院に、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、保有個人情報（病院が保有するものに限る。以下同じ。）を適切に管理する任に当たる。

（保護担当者）
第４条　管理細則第５条第１項の規定に基づき、保護担当者を置き、医療情報部長をもって充てる。

２　保護担当者は、保護管理者を補佐し、保有個人情報の管理に関する事務を担当する。

（監査責任者）

第５条　病院に、監査責任者を置き、保護管理者が指名する。

２　監査責任者は、保有個人情報の管理の状況について監査する。

（保有個人情報の適切な管理のための委員会）

第６条　保護管理者は、保有個人情報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、関係職員で構成する山梨大学医学部附属病院医療情報委員会を定期に又は随時に開催する。

第４章　職員等の責務

第７条　職員等（保有個人情報を取り扱うことのある大学院生、学生、委託職員等を含む。以下同じ。）は、独立行政法人等の保有する個人情報の保護に関する法律（平成１５年法律第５９号。以下「法」という。）の趣旨に則り、関連する法令及び規則等の定め並びに管理細則第３条に規定する総括保護管理者、保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱わなければならない。

第５章　教育研修

第８条　保護管理者は、保有個人情報の取扱いに従事する職員等に対し、保有個人情報の取扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。

２　保護管理者は、保有個人情報を取り扱う病院情報管理システムの管理に関する事務に従事する職員等に対し、保有個人情報の適切な管理のために、病院情報管理システムの管理、運用及びセキュリティ対策に関して必要な教育研修を行う。

３　保護管理者は、医学域等の職員等に対し、保有個人情報の適切な管理のために、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６章　保有個人情報の取扱い

（アクセス制限）

第９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、当該保有個人情報にアクセスする権限を有する者をその利用目的を達成するために必要最小限の職員等に制限する。

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

４　保護管理者は、各職種等のアクセス権限を別に定める。

（複製等の制限）

第１０条　職員等は、業務上の目的で保有個人情報を取り扱う場合であっても、次に掲げる行為については、保護管理者の指示に従い行う。

(1) 保有個人情報の複製

(2) 保有個人情報の送信

(3) 保有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) その他保有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、保有個人情報の内容に誤り等を発見した場合には、保護管理者の指示に従い、訂正等を行う。

（媒体の管理等）

第１２条　職員等は、保護管理者の指示に従い、保有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。

（廃棄等）

第１３条　職員等は、保有個人情報又は保有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、保護管理者の指示に従い、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。

（保有個人情報の取扱状況の記録）

第１４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、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録する。

第７章　病院情報管理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、保有個人情報（病院情報管理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。

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の整備（その定期又は随時の見直しを含む。）、パスワード等の窃取防止等を行うために必要な措置を講ずる。

（アクセス記録）

第１６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、保有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に又は随時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１７条　保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセスの監視のため、保有個人情報を含む又は含むおそれがある一定量以上の情報が病院情報管理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、保有個人情報の秘匿性等その内容に応じて、病院情報管理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、保有個人情報を取り扱う病院情報管理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。

（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保有個人情報の漏えい、滅失又は毀損の防止のため、導入ベンダーの検証のとれた脆弱性の解消、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。

（病院情報管理システムにおける保有個人情報の処理）

第２１条　職員等は、保有個人情報について、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。

２　保護管理者は、当該保有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、保有個人情報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、その処理する保有個人情報について、当該保有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、病院情報管理システムで取り扱う保有個人情報の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報の内容の確認、既存の保有個人情報との照合等を行う。

（バックアップ）

第２４条　保護管理者は、保有個人情報の重要度に応じて、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。

（病院情報管理システム設計書等の管理）

第２５条　保護管理者は、保有個人情報に係る病院情報管理システムの設計書、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、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、保有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。

（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、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、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて病院情報管理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。

（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・媒体の病院情報管理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８章 電算機室等の安全管理

（入退の管理）

第３０条　保護管理者は、保有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等（以下「電算機室等」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。また、保有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、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、電算機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。

３　保護管理者は、電算機室等及び保管施設の入退の管理について、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の整備（その定期又は随時の見直しを含む。）、パスワード等の窃取防止等を行うために必要な措置を講ずる。

（電算機室等の管理）

第３１条　保護管理者は、外部からの不正な侵入に備え、電算機室等に施錠装置、警報装置、監視設備の設置等の措置を講ずる。

２　保護管理者は、災害等に備え、電算機室等に、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。

第９章　保有個人情報の提供及び業務の委託等

（保有個人情報の提供）

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保有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。

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保有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、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、改善要求等の措置を講ずる。

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保有個人情報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。

（業務の委託等）

第３３条　保有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、必要な措置を講ずる。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並びに実施体制、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、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等に関する事項
(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　保有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、委託する保有個人情報の秘匿性等その内容に応じて、委託先における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、保有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保有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前項の措置を実施する。保有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　保有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。

第１０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　保有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。

２　保護管理者は、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。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　総括保護管理者は、前項の規定に基づく報告を受けた場合には、事案の内容等に応じて、当該事案の内容、経緯、被害状況等を学長に速やかに報告する。

５　総括保護管理者は、事案の内容等に応じて、事案の内容、経緯、被害状況等について、文部科学省に対し、速やかに情報提供を行う。

６　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。

（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、当該事案に係る保有個人情報の本人への対応等の措置を講ずる。

２　前項の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、速やかに総務省（行政管理局）に情報提供を行う。

第１１章　監査及び点検の実施

（監査）

第３６条　監査責任者は、保有個人情報の適切な管理を検証するため、第３条から前条までに規定する措置の状況を含む病院における保有個人情報の管理の状況について、定期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３７条　保護管理者は、病院における保有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。

（評価及び見直し）

第３８条　保護管理者は、保有個人情報の適切な管理のための措置について、前条の点検又は管理細則第３６条，第３７条及び第３８条に規定する監査及び点検の結果等を踏まえ、実効性等の観点から保有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ずるものとする。

第１２章　行政機関との連携

第３９条　病院は、「個人情報の保護に関する基本方針」（平成１６年４月２日閣議決定）４を踏まえ、

文部科学省と緊密に連携して、その保有する個人情報の適切な管理を行う。

第１３章　雑則

（雑則）

第４０条　この規程に定めるもののほか、病院が保有する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。

附　則

この規程は、平成２９年８月２日から施行し、平成２９年４月１日から適用する。

附　則

この規程は、令和３年１０月１日から施行し、令和３年６月１日から適用する。