滋賀医科大学医学部附属病院個人情報保護規程

令和４年４月１日制定

（趣旨）

第１条　この規程は，国立大学法人滋賀医科大学個人情報保護規程（以下「大学規程」という。）に基づき，滋賀医科大学医学部附属病院（以下「本院」という。）における個人情報の保護について，必要な事項を定めるものとする。

（定義）

第２条　この規程における用語の意義は，大学規程第２条の定めるところによる。

（管理体制）

第３条　本院に，総括保護管理者のもとに保護管理者を置き，病院長をもって充てる。

２　本院に保護管理者，保護担当者及び部署担当者（以下「保護管理者等」という。）を別表のとおり置く。

３　保護管理者は，本院における個人情報の取り扱いを監督し，本院が保有する個人データ及び保有個人情報（以下「保有個人情報等」という。）の漏えい，滅失又は毀損（以下「漏えい等」という。）の防止及び個人情報の取扱いにおいて問題となる事案の発生又は事案の発生のおそれを把握のための報告連絡体制の整備その他保有個人情報等の適切な管理のための必要な措置を講じる。また，保有個人情報等を情報システムで取り扱う場合，当該情報システムの管理者と連携する。

４　保護担当者は，保護管理者を補佐するとともに，所掌する部署においては保護管理者と同等の権限を持って保有個人情報等の管理に関する事務を担当する。

５　部署担当者は，保護担当者を補佐し，所掌する部署においては保護担当者と同等の権限を持って保有個人情報等の事務を担当する。

（職員等の責務）

第４条　本院の役員及び職員（派遣労働者を含む。）（以下「職員等」という。）は，法の趣旨に則り，個人情報関係法令等及び本規程の定め並びに総括保護管理者及び保護管理者等の指示に従い，個人情報を取り扱わなければならない。

２　職員等が個人情報を取り扱うに当たっては，本学の業務を遂行するため必要な場合に限るものとする。

３　職員等は，保有個人情報等の漏えい等その他個人情報の取扱いにおいて問題となる事案の発生又は事案の発生のおそれを認識した場合は，速やかに保護管理者等に報告しなければならない。

（教育研修）

第５条　総括保護管理者は，職員等に対し，個人情報の保護に関する意識の高揚を図り，その取扱いについて理解を深めるための啓発その他必要な教育研修を行う。

２　総括保護管理者は，保有個人情報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等に対し，保有個人情報等の適切な管理のために，情報システムの管理及び運用並びにセキュリティ対策に関して必要な教育研修を行う。

３　総括保護管理者は，保護管理者等に対し，担当する組織区分の現場における保有個人情報等の適切な管理のための教育研修を実施する。

４　保護管理者は，担当する組織区分の職員等に対し，保有個人情報等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。

（アクセス制限）

第６条　保護管理者は，保有個人情報等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職員の範囲と権限の内容を，当該職員が業務を行う上で必要最小限の範囲に限る。

２　アクセス権限を有しない職員等は，保有個人情報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保有個人情報にアクセスしてはならず，アクセスは必要最小限としなければならない。

（複製等の制限）

第７条　職員等が業務上の目的で保有個人情報等を取り扱う場合であっても，保護管理者は，次の行為については，当該保有個人情報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，職員等は，保護管理者の指示に従い行う。

⑴　保有個人情報等の複製

⑵　保有個人情報等の送信

⑶　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ち出し

⑷　その他保有個人情報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８条　職員等は，保有個人情報等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９条　職員等は，保護管理者の指示に従い，保有個人情報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，施錠等を行う。また，保有個人情報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。

（誤送付等の防止）

第10条　職員等は，保有個人情報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・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，複数の職員による確認やチェックリストの活用等の必要な措置を講ずる。

２　職員等は，前項の措置に際しては，文書の内容だけでなく，付加情報（ＰＤＦファイルの「しおり機能表示」やプロパティ情報等）に個人情報が含まれている場合があることに注意する。

（廃棄等）

第11条　職員等は，保有個人情報等又は保有個人情報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，保護管理者の指示に従い，当該保有個人情報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　保有個人情報等の消去や保有個人情報等が記録されている媒体の廃棄を委託する場合（二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，又は写真等を付した消去及び廃棄を証明する書類を受け取るなど，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。

（保有個人情報等の取扱状況の記録）

第12条　保護管理者は，保有個人情報等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。

（外的環境の把握）

第13条　保護管理者等は，保有個人情報等が，外国（クラウドサービス提供事業者が所在する外国及び個人データが保存されるサーバが所在する外国等。）において取り扱われる場合，当該外国の個人情報の保護に関する制度等を把握した上で，保有個人情報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。

（アクセス制御）

第14条　保護管理者は，保有個人情報等の秘匿性等その内容に応じて，必要最小限のアクセス権限を具体化するため，認証機能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。

（アクセス記録）

第15条　保護管理者は，保有個人情報等の秘匿性等その内容に応じて，当該保有個人情報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定期的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16条　保護管理者は，保有個人情報等の秘匿性等その内容及びその量に応じて，当該保有個人情報等への不適切なアクセスの監視のため，保有個人情報等を含む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17条　保護管理者は，保有個人情報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18条　保護管理者は，保有個人情報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を防止するため，ファイアウォール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19条　保護管理者は，不正プログラムによる保有個人情報等の漏えい等の防止のため，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。

（情報システムにおける保有個人情報等の処理）

第20条　職員等は，保有個人情報等について，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，当該保有個人情報等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21条　保護管理者は，保有個人情報等の秘匿性等その内容に応じて，暗号化のために必要な措置を講ずる。

２　職員等は，前項を踏まえ，その処理する保有個人情報等について，当該保有個人情報等の秘匿

性等その内容に応じて，適切に暗号化（適切なパスワードの選択，その漏えい等防止の措置等を含む。）を行う。

（記録機能を有する機器・媒体の接続制限）

第22条　保護管理者は，保有個人情報等の秘匿性等その内容に応じて，当該保有個人情報等の情報の漏えい等の防止のため，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。

２　職員等は，暗号化機能を有し，パスワード等による認証を要するＵＳＢメモリを除き，ＵＳＢメモリを使用しないものとする。

（端末の限定）

第23条　保護管理者は，保有個人情報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24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25条　職員等は，端末の使用に当たっては，保有個人情報等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。

（入力情報の照合等）

第26条　職員等は，情報システムで取り扱う保有個人情報等の重要度に応じて，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等の内容の確認，既存の保有個人情報等との照合等を行う。

（バックアップ）

第27条　保護管理者は，保有個人情報等の重要度に応じて，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。

（情報システム設計書等の管理）

第28条　保護管理者は，保有個人情報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

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。

（入退管理）

第29条　保護管理者は，保有個人情報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「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。また，保有個人情報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，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。

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，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。），パスワード等の読取防止等を行うために必要な措置を講ずる。

（情報システム室等の管理）

第30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。

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。

（漏えい等の報告等及び再発防止措置）

第31条　職員等は，保有個人情報等の漏えい等その他個人情報の取扱いにおいて問題となる事案の発生又は事案の発生のおそれを認識した場合は，直ちに保護管理者等に報告するものとする。

２　保護管理者等は，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ものとし，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，事案の概要等を調査し，総括保護管理者に報告する。

４　保護管理者等は，前項の規定にかかわらず，次に掲げる事態である場合には，事態を知った時点において直ちに総括保護管理者に当該事態の内容等について報告しなければならない。

⑴　要配慮個人情報が含まれる個人データの漏えい等が発生し，又は発生したおそれがある事態

⑵　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し，又は発生したおそれがある事態

⑶　不正の目的をもって行われたおそれがある個人データの漏えい等が発生し，又は発生したおそれがある事態

(4)　個人データに係る本人の数が千人を超える漏えい等が発生し，又は発生したおそれがある事態

5　第１項の報告は，次に掲げる事項とする。ただし，前項の事態を知った時点での報告の場合は，当該時点で把握しているものとする。

(1)　概要

(2)　漏えい等が発生し，又は発生したおそれがある個人データの項目

(3)　漏えい等が発生し，又は発生したおそれがある個人データに係る本人の数

(4)　原因

(5)　二次被害又はそのおそれの有無及びその内容

(6)　本人への対応の実施状況

(7)　公表の実施状況

(8)　再発防止のための措置

(9)　その他参考となる事項

6　総括保護管理者は，前３項による報告を受けた場合は，当該内容に応じて，直ちに学長に報告するものとする。

7　学長は，第４項に掲げる事態の場合は，速やかに（この場合，３日から５日以内とする。）個人情報保護委員会に報告し，総括保護管理者及び保護管理者に対して，引き続き調査及び復旧等の対応を行わせるとともに，事態を知った日から30日以内（第３号の事態の場合は60日以内。）に個人情報保護委員会に報告しなければならない。

8　学長は，第４項に掲げる事態の場合は，当該事態の状況に応じて速やかに，当該本人の権利利益を保護するために必要な範囲において，第５項第１号，第２号，第４号，第５号及び第９号に定める事項を通知しなければならない。ただし，本人への通知が困難な場合であって，本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは，この限りでない。

9　学長は，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を行うものとする。

（苦情の処理）

第32条　職員等は，個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

2　保護管理者は，個人情報の取扱いに関する苦情について，迅速かつ適切に対応できるよう体制整備を行う。

（点検）

第33条　保護管理者は，担当する組織区分における個人情報の取り扱いの状況並びに保有個人情報等，仮名加工情報，行政機関等匿名加工情報及び匿名加工情報の適切な管理について，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34条　保護管理者は，個人情報の取り扱いの状況並びに保有個人情報等，仮名加工情報，行政機関等匿名加工情報及び匿名加工情報の適切な管理のための措置について，監査又は点検の結果等を踏まえ，実効性等の観点から当該状況及び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。

（雑則）

第35条　この規程に定めるもののほか，本院における個人情報の保護に関し必要な事項は，別に定める。

附　則

１　この規程は，令和４年４月１日から施行する。

２　滋賀医科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（平成17年４月１日制定）は廃止する。

別表

保護管理者，保護担当者及び部署担当者

組織区分	保護管理者	保護担当者	部署担当者
医学部附属病院	病院長	医療情報部長 事務部長 （病院担当）	医療安全管理部長
			感染制御部長
			各診療科長
			中央診療部門の各部長
			中央手術部門の各部長
			診療・教育・研究支援部門の各部長
			薬剤部長
			看護部長
			病院経営戦略課，クオリティマネジメント課，医療サービス課及び医務課の課長