

国立大学法人滋賀医科大学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

平成24年3月13日改正

(設置)

第1条 この規程は、「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。）第7条及び独立行政法人等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指針（平成16年9月14日総務省行政管理局長通知総管情第85号）に基づき、国立大学法人滋賀医科大学（以下「本学」という。）の保有する個人情報の適切な管理について、必要な事項を定める。

(定義)

第2条 この指針における用語の意義は、法第2条の定めるところによる。

(管理体制)

第3条 本学に、総括保護管理者を置き、総務担当理事をもって充てる。

- 2 総括保護管理者は、本学における保有個人情報の管理に関する事務を総括する任に当たる。
- 3 本学に保護管理者、保護担当者及び部署担当者を別表のとおり置く。
- 4 保護管理者は、各課室等における保有個人情報を適切に管理する。
- 5 保護担当者は、保護管理者を補佐し、保護管理者と同等の権限を持って保有個人情報の管理に関する事務を担当する。
- 6 部署担当者は、保護担当者を補佐し、保有個人情報の事務を担当する。
- 7 本学に、監査責任者を置き、常勤の監事をもって充てる。
- 8 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。

(教育研修)

第4条 総括保護管理者は、保有個人情報の取扱いに従事する職員に対し、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 総括保護管理者は、保有個人情報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、保有個人情報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て必要な教育研修を行う。
- 3 保護管理者は、当該課室等の職員に対し、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。

(職員の責務)

第5条 職員は、法の趣旨に則り、関連する法令及び規程等の定め並びに総括保護管理者、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

ない。

(アクセス制限)

第6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に限る。

2 アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。

3 職員は、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。

(複製等の制限)

第7条 職員は、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。

一 保有個人情報の複製

二 保有個人情報の送信

三 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

四 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8条 職員は、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9条 職員は、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10条 職員は、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、当該保有個人情報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。

(保有個人情報の取扱状況の記録)

第11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。

(アクセス制御)

第12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、パスワード等を使用して権限を識別する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。

(外部からの不正アクセスの防止)

第13条 保護管理者は、保有個人情報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。

(コンピュータウイルスによる漏えい等の防止)

第14条 保護管理者は、コンピュータウイルスによる保有個人情報の漏えい、滅失又はき損の防止のため、コンピュータウイルスの感染防止等に必要な措置を講ずる。

(暗号化)

第15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。

(入力情報の照合等)

第16条 職員は、情報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17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。

(情報システム設計書等の管理)

第18条 保護管理者は、保有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19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20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21条 職員は、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ないことがないように、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずる。

(入退室の管理)

第22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「情報システム室等」という。）に入室する権限を有する者を定めるとともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずる。

(情報システム室等の管理)

第23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。

(保有個人情報の提供)

第24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、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25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等の管理体制、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。

- 一 個人情報に関する秘密保持等の義務
- 二 再委託の制限又は条件に関する事項
- 三 個人情報の複製等の制限に関する事項
- 四 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
- 五 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
- 六 違反した場合における契約解除の措置その他必要な事項

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。

(事案の報告及び再発防止措置)

第26条 役職員は、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が発生した場合に、その事実を知った職員は、速やか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、被害の拡大防止又は復旧等のために必要な措置を講ずる。

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 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27条 総括保護管理者は、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、当該事案に係る本人への対応等の措置を講ずる。

(監査)

第28条 監査責任者は、保有個人情報の管理の状況について、定期に又は随時に監査（外部監査を含む。）を行い、その結果を総括保護管理者に報告する。

(点検)

第29条 保護管理者は、自ら管理責任を有す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、定期に又は随時に点検を行い、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30条 保有個人情報の適切な管理のための措置については、監査又は点検の結果等を踏まえ、実効性等の観点から評価し、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。

(個人情報ファイル簿)

第31条 保護管理者は、個人情報ファイル（法第11条第2項各号に掲げるもの及び同条第3項に規定により個人情報ファイル簿に記載しないものを除く。以下同じ。）を保有するに至ったときは、直ちに、別紙様式により個人情報ファイル簿を作成し、総括保護管理者に提出しなければならない。

- 2 保護管理者は、個人情報ファイル簿に記載すべき事項に変更があったときは、直ちに、当該個人情報ファイル簿を修正し、総括保護管理者に提出しなければならない。
- 3 保護管理者は、個人情報ファイル簿に掲載した個人情報ファイルの保有をやめたとき、又は本人の数が政令で定める数に満たない個人情報ファイルに至ったときは、遅滞なく、当該個人情報ファイルについての記載を削除するよう総括保護管理者に申し出なければならない。
- 4 個人情報ファイル簿は、一般の閲覧に供するとともに、法人のホームページにおいて公表する。

(雑則)

第32条 この規程に定めるもののほか、個人情報の適切な管理に関し、必要な事項は、別に定める。

附 則

この規程は、平成17年4月1日から施行する。

附 則

この規程は、平成23年4月1日から施行する。

附 則

この規程は、平成23年10月1日から施行する。

附 則

この規程は、平成24年4月1日から施行する。

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
事務部門		理事（総務等担当）	課長又は室長	課長補佐又は各所属職員
医学科	講座（大講座を除く）	医学科長	各講座の長	各講座の教員
	大講座		主任教授及び主任教授が指名する者	各講座の教員
看護学科	大講座	看護学科長	主任教授及び主任教授が指名する者	各講座の教員
附属図書館		図書館長	図書課長	所属職員
保健管理センター		センター所長	センター教員	所属職員
学内教育研究施設		各センター長	センター教員	所属職員

医学部附属病院	病院長	副病院長 (経営・業務改善・事務総括) 医療情報部長	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
			事務部門の課長又は室長

個人情報ファイル簿
(通番は総務課で記入)

通 番

--	--

個人情報ファイルの名称	
個人情報ファイルを使用する組織名称	
個人情報ファイルの種別 <input type="checkbox"/> にチェックしてください。	<input type="checkbox"/> 電算処理ファイル <input type="checkbox"/> マニュアルファイル (氏名、生年月日その他の記述等により特定の個人情報を容易に検索することができるように体系的に構成したもの)
記録件数	件 (概数)
ファイル保有目的	
ファイル記録項目	
ファイル記録範囲	
処理情報の収集方法	
処理情報の経常的提供先	
備考	