

国立大学法人浜松医科大学個人情報管理規程

(平成 17 年 3 月 28 日規程第 54 号)

改正 平成 18 年 3 月 9 日規程第 10 号 平成 18 年 7 月 13 日規程第 43 号
平成 19 年 3 月 15 日規程第 18 号 平成 21 年 3 月 12 日規程第 61 号
平成 26 年 3 月 4 日規程第 30 号 平成 26 年 5 月 26 日規程第 56 号
平成 27 年 4 月 6 日規程第 60 号 平成 27 年 10 月 1 日規程第 71 号
平成 28 年 5 月 26 日規程第 54 号 平成 29 年 10 月 10 日規程第 51 号
平成 31 年 2 月 4 日規程第 8 号

目次

- 第 1 章 総則(第 1 条・第 2 条)
- 第 2 章 個人情報管理体制(第 3 条 - 第 12 条)
- 第 3 章 保有個人情報の取扱い(第 13 条 - 第 31 条の 3)
- 第 4 章 情報システムにおける安全確保等(第 32 条 - 第 48 条)
- 第 5 章 問題となる事案への対応等(第 49 条 - 第 55 条)
- 附則

第 1 章 総則

(趣旨)

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 条第 1 項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。)第 1 条の規定に基づき、国立大学法人浜松医科大学(以下「本法人」という。)が保有する個人情報の適切な管理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 この規程において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

- (1) 当該情報に含まれる氏名、生年月日その他の記述等(文書、図画若しくは電磁的記録(電磁的方式(電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。)で作られる記録をいう。以下同じ。)に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項(個人識別符号を除く。)をいう。以下同じ。)により特定の個人を識別することができるもの(他の情報と照合することができ、それにより特定の個人を識別することができることとなるものを含む。)
- (2) 個人識別符号が含まれるもの

- 2 この規程において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、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施行令（平成 15 年政令第 549 号。以下「保護法施行令」という。）第 1 条で定めるものをいう。
 - (1) 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの
 - (2) 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの
- 3 この規程において「要配慮個人情報」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして保護法施行令第 2 条で定める記述等が含まれる個人情報をいう。
- 4 この規程において「保有個人情報」とは、本法人の職員(役員を含む。以下同じ。)が職務上作成し、又は取得した個人情報であって、本法人の職員が組織的に利用するものとして、本法人が保有しているものをいう。ただし、独立行政法人等の保有する情報の公開に関する法律(平成 13 年法律第 140 号)第 2 条第 2 項に規定する法人文書に記載されているものに限る。
- 5 この規程において「個人情報ファイル」とは、保有個人情報を含む情報の集合物であって、次に掲げるものをいう。
 - (1) 一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
 - (2) 前号に掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有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
- 6 この規程において「非識別加工情報」とは、次の各号に掲げる個人情報（他の情報と照合することができ、それにより特定の個人を識別することができることとなるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを除く。）を除く。以下この項において同じ。）の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができない（個人に関する情報について、当該個人に関する情報に含まれる記述等により、又は当該個人に関する情報が他の情報と照合することができる個人に関する情報である場合にあっては他の情報（当該個人に関する情報の全部又は一部を含む個人情報その他の個人情報保護

委員会規則（第2号）第2条で定める情報を除く。）と照合することにより、特定の個人を識別することができないことをいう。）ように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。

(1) 第1項第1号に該当する個人情報 当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

(2) 第1項第2号に該当する個人情報 当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）

7 この規程において「独立行政法人等非識別加工情報」とは、次の各号のいずれにも該当する個人情報ファイルを構成する保有個人情報（他の情報と照合することができ、それにより特定の個人を識別することができることとなるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを除く。）を除く。以下この項及び第9項において同じ。）の全部又は一部（これらの一部に独立行政法人等情報公開法第5条に規定する不開示情報（同条第1号に掲げる情報を除く。以下この項において同じ。）が含まれているときは、当該不開示情報に該当する部分を除く。）を加工して得られる非識別加工情報をいう。

(1) 第21条の規定に基づき、法第11条に規定する帳簿（以下「個人情報ファイル簿」という。）に掲載するものであること。

(2) 本学に対し、当該個人情報ファイルを構成する保有個人情報が記録されている法人文書の独立行政法人等情報公開法第3条の規定による開示の請求があったとしたならば、本学が次のいずれかを行うこととなるものであること。

ア 当該法人文書に記録されている保有個人情報の全部又は一部を開示する旨の決定をすること。

イ 国立大学法人浜松医科大学情報公開取扱規程（平成16年5月24日規程第13号）第7条第1項又は第2項の規定により意見書の提出の機会を与えること。

(3) 本学の事務及び事業の適正かつ円滑な運営に支障のない範囲内で、法第四十四条の十第一項の基準に従い、当該個人情報ファイルを構成する保有個人情報を加工して非識別加工情報を作成することができるものであること。

8 この規程において「独立行政法人等非識別加工情報ファイル」とは、独立行政法人等非識別加工情報を含む情報の集合体であって、次に掲げるものをいう。

(1) 特定の独立行政法人等非識別加工情報を電子計算機を用いて検索することができるように体系的に構成したもの

(2) 前号に掲げるもののほか、特定の独立行政法人等非識別加工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として政令で定めるもの

- 9 この規程において「削除情報」とは、独立行政法人等非識別加工情報の作成に用いた保有個人情報から削除した記述等及び個人識別符号をいう。
- 10 この規程において「個人番号」とは、住民票コード（住民基本台帳法（昭和42年法律第81号）第7条第13号に規定する住民票コードをいう。）を変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。
- 11 この規程において「本人」とは、個人情報によって識別される特定の個人又は個人番号によって識別される特定の個人をいう。
- 12 この規程において「個人番号カード」とは、氏名、住所、生年月日、性別、個人番号その他政令で定める事項が記載され、本人の写真が表示され、かつ、これらの事項その他総務省令で定める事項（以下「カード記録事項」という。）が電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識できない方法をいう。）により記録されたカードであって、番号法又は番号法に基づく命令で定めるところによりカード記録事項を閲覧し、又は改変する権限を有する者以外の者による閲覧又は改変を防止するために必要なものとして総務省令で定める措置が講じられたものをいう。
- 13 この規程において「特定個人情報」とは、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報をいう。
- 14 この規程において「特定個人情報ファイル」とは、個人番号をその内容に含む個人情報ファイルをいう。
- 15 この規程において「課等」とは、国立大学法人浜松医科大学事務組織規程（平成16年規程第8号）第2条に規定する事務局の課及び国立大学法人浜松医科大学組織規則（平成16年規則第1号）第19条に規定する監査室をいう。

第2章 個人情報管理体制

（保有個人情報等の管理体制）

第3条 本法人における保有個人情報及び個人番号（以下「保有個人情報等」という。）を適切に管理するため、総括保護管理者、保護管理者及び保護担当者を置く。

（総括保護管理者）

第4条 総括保護管理者は、保有個人情報等の管理に関する事務を総括する。

2 総括保護管理者は、副学長（情報・広報担当）をもって充てる。

（保護管理者）

第5条 保護管理者は、保有個人情報等の適切な管理を確保するため、次に掲げる業務を行う。保有個人情報等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して、その任に当たる。

(1) 個人情報ファイル簿の作成に関すること。

(2) 保有個人情報等の取扱状況の記録に関すること。

- (3) 情報システムにおける安全の確保等に関すること。
- (4) 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。）の安全管理に関すること。
- (5) 保有個人情報等の提供に関すること。
- (6) 保有個人情報等の点検に関すること。
- (7) 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「事務取扱担当者」という。）並びにその役割を指定すること。
- (8) 各事務取扱担当者が取り扱う特定個人情報等の範囲を指定すること。
- (9) 次に掲げる組織体制を整備すること。

ア 事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合の責任者への報告連絡体制

イ 特定個人情報等の漏えい、滅失又は毀損等（以下「情報漏えい等」という。）事案の発生又は兆候を把握した場合の職員から責任者等への報告連絡体制

ウ 特定個人情報等を複数の部署で取り扱う場合の各部署の任務分担及び責任の明確化

エ 特定個人情報等の情報漏えい等の事案の発生又は兆候を把握した場合の対応体制

- (10) その他保有個人情報等の管理に関すること。

(保護担当者)

第6条 保護担当者は、保護管理者を補佐し、保有個人情報等の管理に関する事務を担当する。

- 2 保護担当者は、保護管理者の下に若干人を置き、当該保護管理者が指名する者をもって充てる。

(課等が保有する個人情報及び個人番号の管理体制)

第7条 課等が保有する個人情報及び個人番号（以下「個人情報等」という。）の管理については、当該個人情報等を保有する課等の長を保護管理者とし、当該係長を保護担当者とする。

(教員が保有する個人情報の管理体制)

第8条 教員が保有する個人情報の管理については、当該個人情報を保有する教員の所属する講座等の教授(教授が欠員の場合は准教授)を保護管理者とし、当該教員を保護担当者とする。

(医学部附属病院が保有する個人情報の管理体制)

第9条 医学部附属病院が保有する個人情報の管理については、病院長を保護管理者とし、医療情報部長及び事務局次長（病院担当）を保護担当者とする。

- 2 医学部附属病院が保有する個人情報については、この規程によるほか「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（平成16年12月厚

生労働省。)及び「国立大学附属病院における個人情報の適切な取扱いのためのガイドライン」(平成17年2月国立大学附属病院長会議)に基づいて、病院長が必要な措置を講じなければならない。

(監査責任者)

第10条 本法人に、監査責任者を1人置き、監査室長をもって充てる。

2 監査責任者は、保有個人情報等の管理状況について監査する。

(情報公開・個人情報保護委員会)

第11条 本法人における保有個人情報の管理に係る重要事項の決定、連絡・調整等について検討するため、情報公開・個人情報保護委員会(以下「委員会」という。)を置く。

2 委員会に関する必要な事項は、学長が別に定める。

(教育研修)

第12条 総括保護管理者は、保有個人情報等の取扱いに従事する職員(派遣労働者を含む。以下同じ。)に対して、次に掲げる事項の教育研修を実施するものとする。

(1) 保有個人情報等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事項

(2) 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、運用及びセキュリティ対策に関して必要な事項

2 保護管理者は、当該課等及び講座等の職員に対し、前項に規定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。

3 総括保護管理者は、保護管理者及び保護担当者に対し、課室等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。

第3章 保有個人情報の取扱い

(職員の責務)

第13条 職員は、法及び番号法の趣旨に則り、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、保有個人情報等を取り扱わなければならない。

2 職員(これらの職にあった者を含む。)は、その業務に関して知り得た個人情報(独立行政法人等非識別加工情報及び削除情報に該当するものを除く。)の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。

3 職員は、情報漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合は、速やかに保護管理者に報告しなければならない。

(保有の制限)

第14条 職員は、個人情報等を保有するに当たっては、業務を遂行するため必要な場合に限るものとし、かつ、その利用の目的をできる限り特定しなければならない。

- 2 職員は、前項の規定により特定された利用の目的(以下「利用目的」という。)の達成に必要な範囲を超えて、個人情報等を保有してはならない。
- 3 職員は、利用目的を変更するに当たっては、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

(利用目的の明示)

第 15 条 職員は、本人から直接書面(電磁的記録を含む。)に記録された当該本人の個人情報等を取得するときは、次に掲げる場合を除き、あらかじめ、本人に対し、その利用目的を明示しなければならない。

- (1) 人の生命、身体又は財産の保護のために緊急に必要があるとき。
- (2) 利用目的を本人に明示することにより、本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがあるとき。
- (3) 利用目的を本人に明示することにより、国の機関、独立行政法人等、地方公共団体又は地方独立行政法人(地方独立行政法人法(平成 15 年法律第 118 号)第 2 条第 1 項に規定する地方独立行政法人をいう。以下同じ。)が行う事務又は事業の適正な遂行に支障を及ぼすおそれがあるとき。
- (4) 取得の状況からみて利用目的が明らかであると認められるとき。

(適正な取得)

第 16 条 職員は、偽りその他不正の手段により個人情報等を取得してはならない。

(正確性の確保)

第 17 条 職員は、利用目的の達成に必要な範囲内で、保有個人情報(独立行政法人等非識別加工情報(独立行政法人等非識別加工情報ファイルを構成するものに限る。))及び削除情報に該当するものを除く。以下同じ。)が過去又は現在の事実と合致するよう努めなければならない。

- 2 職員は、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、訂正等を行わなければならない。

(利用及び提供の制限)

第 18 条 職員は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

- 2 前項の規定にかかわらず、職員は、保護管理者が次の各号のいずれかに該当すると認めるときは、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供することができる。ただし、保有個人情報を利用目的以外の目的のために自ら利用し、又は提供することによって、本人又は第三者の権利利益を不当に侵害するおそれがあると認められるときは、この限りでない。

- (1) 本人の同意があるとき、又は本人に提供するとき。
- (2) 本法人が法令の定める業務の遂行に必要な限度で保有個人情報を内部で利用する場合であって、当該保有個人情報を利用することについて相当な理由のあるとき。

(3) 行政機関(行政機関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58号。以下「行政機関個人情報保護法」という。)第2条第1項に規定する行政機関をいう。以下同じ。)、他の独立行政法人等、地方公共団体又は地方独立行政法人に保有個人情報を提供する場合において、保有個人情報の提供を受ける者が、法令の定める事務又は業務の遂行に必要な限度で提供に係る個人情報を利用し、かつ、当該個人情報を利用することについて相当な理由のあるとき。

(4) 前3号に掲げる場合のほか、専ら統計の作成又は学術研究の目的のために保有個人情報を提供するとき、本人以外の者に提供することが明らかに本人の利益になるとき、その他保有個人情報を提供することについて特別の理由のあるとき。

3 前項の規定は、保有個人情報の利用又は提供を制限する他の法令の規定の適用を妨げるものではない。

4 総括保護管理者は、個人の権利利益を保護するため特に必要があると認めるときは、保有個人情報の利用目的以外の目的のため、本法人の内部における利用を特定の職員に限るものとする。

第19条 保護管理者は、利用目的以外の目的のために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ものとする。

2 保護管理者は、利用目的以外の目的のために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、必要な安全確保の措置を要求し、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じなければならない。

3 保護管理者は、利用目的以外の目的のために行政機関、独立行政法人等、地方公共団体又は地方独立行政法人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項に規定する手続き又は措置を講じなければならない。

4 保護管理者は、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20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に、必要な措置を講じなければならない。

2 前項の規定により外部に委託する場合には、契約者又は当該契約の委任を受けた者が、保護管理者の協力を得て、当該契約書に、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（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。第6項において同じ。）の制限又は事前承認等再委託に係る条件に関する事項（再委託に際して再委託先に求める事項は、再委託先が子会社である場合も同様に求めるものとするを明記しなければならない。）
- (3) 個人情報の複製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
- 3 個人番号利用事務等の全部又は一部を委託する場合には、委託先において、番号法に基づき本法人が果たすべき安全管理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。
- 4 保有個人情報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保有個人情報等の秘匿性等その内容やその量等に応じて、委託先における管理体制及び実施体制や個人情報の管理の状況について、少なくとも年1回以上、原則として実地検査により確認する。
- 5 個人番号利用事務等の全部又は一部の委託をする際には、「委託を受けた者」において、本法人が果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。
- 6 委託先において、保有個人情報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2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。
- 7 個人番号利用事務等の全部又は一部の「委託を受けた者」が再委託をする際には、委託をする個人番号利用事務等において取り扱う特定個人情報の適切な安全管理が図られることを確認した上で再委託の諾否を判断する。
- 8 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ものとする。
- 9 保有個人情報を提供又は業務委託する場合には、漏えい等による被害発生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、保有個人情報の秘匿性等その内容などを考慮し、必要に応じ、氏名を番号に置き換える等の匿名化措置を講ずる。

(個人情報ファイル簿)

第 21 条 総括保護管理者は、個人情報ファイルを保有するに至ったときは、直ちに法第 11 条に規定する帳簿(以下「個人情報ファイル簿」という。)を作成し、公表するものとする。

2 個人情報ファイル簿は、本法人が保有する個人情報ファイルを通じて一の帳簿とする。

3 総括保護管理者は、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するものとする。

4 総括保護管理者は、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しなくなったとき、又はその個人情報ファイルに含まれる個人情報によって識別される特定の個人の数が 1000 人未満となったときは、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ものとする。

5 総括保護管理者は、個人情報ファイル簿を作成したときは、遅滞なく、これを本法人の適当な場所に備えて置き一般の閲覧に供するとともに、本法人のホームページに掲載するなどの方法により公表するものとする。

(アクセス制限)

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(個人識別の容易性(匿名化の程度等)、要配慮個人情報の有無、漏えい等が発生した場合に生じ得る被害の性質・程度などを考慮する。以下同じ。)に応じて、当該保有個人情報等にアクセスする権限を付与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ものとする。

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

(複製等の制限)

第 23 条 職員が、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、次に掲げる行為については、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限定し、職員は、保護管理者の指示に従うものとする。

(1) 保有個人情報等の複製

(2) 保有個人情報等の送信

(3) 保有個人情報等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等の適切な管理に支障を及ぼす恐れのある行為

(媒体の管理等)

第 24 条 職員は、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、耐火金庫へ保管、施錠しなければならない。

(廃棄等)

第 25 条 職員は、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わなければならない。

(保有個人情報の取扱状況の記録)

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、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しなければならない。

2 保護管理者は、特定個人情報ファイルの取扱状況を確認する手段を整備して、当該特定個人情報等の利用及び保管等の取扱状況について記録する。

(個人番号の利用の制限)

第 27 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。

(特定個人情報の提供の求めの制限)

第 28 条 個人番号利用事務又は個人番号関係事務(以下「個人番号利用事務等」という。)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。

(特定個人情報ファイルの作成の制限)

第 29 条 個人番号利用事務等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。

(特定個人情報等の収集・保管の制限)

第 30 条 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又は保管してはならない。

(取扱区域)

第 31 条 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(以下「取扱区域」という。)を明確にし、物理的な安全管理措置を講ずる。

(独立行政法人等非識別加工情報等の作成及び提供等)

第 31 条の 2 本学は、法の規定に従い、独立行政法人等非識別加工情報(独立行政法人等非識別加工情報ファイルを構成するものに限る。以下同じ。)を作成し、及び提供することができる。

2 職員は、法令に基づく場合を除き、利用目的以外の目的のために独立行政法人等非識別加工情報及び削除情報(保有個人情報に該当するものに限る。)を自ら利用し、又は提供してはならない。

3 独立行政法人等非識別加工情報の作成及び提供等に関し、必要な事項は、別に定める。

(独立行政法人等非識別加工情報等の従事者の義務)

第 31 条の 3 職員（これらの職にあった者を含む。）は、その業務に関して知り得た独立行政法人等非識別加工情報、独立行政法人等非識別加工情報の作成に用いた保有個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報の内容のみだりに他人に知らせ、又は不当な目的に利用してはならない。

第 4 章 情報システムにおける安全確保等

(アクセス制御)

第 32 条 保護管理者は、情報システムで取り扱う保有個人情報等の秘匿性等その内容に応じて、アクセスに係るパスワード等(パスワード、IC カード、生体情報等を使用して権限を識別する機能をいう。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じなければならない。

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じなければならない。

(アクセス記録)

第 33 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、当該保有個人情報が記録される各種媒体へのアクセス状況の記録(以下「アクセス記録」という。)を一定の期間保存するとともに、アクセス記録を定期的かつ必要に応じて随時に分析するために必要な措置を講じなければならない。

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じなければならない。

3 保護管理者は、特定個人情報等へのアクセス状況を記録し、その記録を一定の期間保存し、定期に又は随時に分析するために必要な措置を講ずる。また、アクセス記録の改ざん、窃取又は不正な削除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 34 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、保有個人情報等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 35 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、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、当該特権を付与する者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 36 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じなければならない。

(不正プログラムによる漏えい等の防止)

第 37 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、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。）を講じなければならない。

(情報システムにおける保有個人情報の処理)

第 38 条 職員は、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。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 39 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じなければならない。

2 職員は、これを踏まえ、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 40 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わなければならない。

(バックアップ)

第 41 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じなければならない。

(情報システム設計書等の管理)

第 42 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じなければならない。

(端末の限定)

第 43 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(機、機器、装置)を限定するために必要な措置を講じなければならない。

(端末の盗難防止等)

第 44 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じなければならない。

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서는ならない。

(第三者の閲覧防止)

第 45 条 職員は、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じなければならない。

(記録機能を有する機器・媒体の接続制限)

第 46 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情報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・媒体の保有個人情報にアクセスできる端末等への接続の制限(可能な範囲においての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。

(入退管理)

第 47 条 保護管理者は、情報システム室等に立ち入る権限を有する者(以下「権限者」という。)を定めるとともに、用件の確認、入退の記録、権限者以外の者についての識別化、権限者以外の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じなければならない。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、同様の措置を講じなければならない。

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ことができる。

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するとともに、パスワード等の取扱いに関する定め整備及びその定期又は随時の見直しの実施、読取防止等の措置を講じなければならない。

(情報システム室等の管理)

第 48 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、監視装置の設置等の措置を講じなければならない。

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じなければならない。

第 5 章 問題となる事案への対応等

(事案の報告及び再発防止措置)

第 49 条 職員は、情報漏えい等の事案の発生又は兆候を把握した場合及び事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合等、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

した場合には、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ものとする。

- 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じなければならない。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について報告しなければならない。
- 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しなければならない。
- 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、本法人を所管する行政機関に対し、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構じなければならない。
- 7 学長は、事案の発生した内容、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等の本人への対応等の措置を講じなければならない。
- 8 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。

（監査）

第50条 監査責任者は、保有個人情報等の適切な管理を検証するため、第3条から第49条に規定する措置の状況を含む本法人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ものとする。

（点検）

第51条 保護管理者は、各所属（第7条における課等、第8条における講座等、第9条における医学部附属病院を指す。）における保有個人情報等の記録媒体、処理経路、保管方法等について、定期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には、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52条 総括保護管理者、保護管理者等は、保有個人情報等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保有個人情報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には、その見直し等の措置を講じなければならない。

（行政機関との連携）

第53条 本法人は、「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、本法人を所管する行政機関と緊密に連携して、その保有する個人情報の適切な管理を行う。

(庶務)

第54条 保有個人情報等の管理事務の総括の庶務は、総務課において処理する。

(雑則)

第55条 この規程に定めるもののほか、本法人の保有個人情報等の取扱いに関する必要な事項は、学長が別に定める。

附 則

この規程は、平成17年4月1日から施行する。

附 則(平成18年3月9日規程第10号)

この規程は、平成18年4月1日から施行する。

附 則(平成18年7月13日規程第43号)

この規程は、平成18年7月13日から施行する。

附 則(平成19年3月15日規程第18号)

この規程は、平成19年4月1日から施行する。

附 則(平成21年3月12日規程第61号)

この規程は、平成21年4月1日から施行する。

附 則(平成26年3月4日規程第30号)

この規程は、平成26年4月1日から施行する。

附 則(平成26年5月26日規程第56号)

この規程は、平成26年5月26日から施行し、平成26年4月1日から適用する。

附 則(平成27年4月6日規程第60号)

この規程は、平成27年4月6日から施行する。

附 則(平成27年10月1日規程第71号)

この規程は、平成27年10月5日から施行する。

附 則(平成28年5月26日規程第54号)

この規程は、平成28年5月26日から施行し、平成28年4月1日から適用する。

附 則(平成 29 年 10 月 10 日規程第 51 号)

この規程は、平成 29 年 10 月 10 日から施行し、平成 29 年 5 月 30 日から適用する。

附 則(平成 31 年 2 月 4 日規程第 8 号)

この規程は、平成 31 年 2 月 4 日から施行する。