

「一般社団法人山梨健康DNA情報バンク」個人情報保護管理規程

目次

第1章 総則

第1節 通則

第2節 保有個人情報の管理体制等

第2章 個人情報の管理

第1節 個人情報の取得、利用等

第2節 個人情報を保有する課等において行う安全確保の措置

第3節 システム管理班等において行う安全確保の措置

第3章 個人情報ファイルの保有等に関する通知等

第4章 事故の報告及び再発防止措置

第5章 点検及び監査

第6章 補則

第1章 総則

第1節 通則

(目的)

第1条 この規程は、一般社団法人山梨健康DNA情報バンク（以下、「当法人」とします。）の保有する個人情報について、その適切な管理に必要な事項を定めることにより、当法人の業務の適正かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

(適用の範囲)

第2条 当法人の保有する個人情報及び個人情報ファイルの取扱いは、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「法」という。）及びこの規程の定めるところによる。

(定義)

第3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つて、当該情報に含まれる氏名、生年月日その他の記述等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み、法の規定の適用を受けるものに限る。）をいう。

- 2 この規程において「保有個人情報」とは、当法人の会員が職務上作成し、又は取得した個人情報であって、職員が組織的に利用するものとして、当法人が保有しているものをいう。
- 3 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
- 4 この規程において個人情報について「本人」とは、個人情報によって識別される特定の個人をいう。

(職員の責務)

第4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個人情報保護管理者、副総括個人情報保護管理者、個人情報保護管理者及び副個人情報保護管理者の指示に従い、保有個人情報を取り扱わなければならない。

第2節 保有個人情報の管理体制等

(総括個人情報保護管理者等)

第5条 当法人に、総括個人情報保護管理者1人を置き、理事長をもって充てる。

- 2 当法人に、副総括個人情報保護管理者1人を置き、専務理事をもって充てる。
- 3 各班等に、個人情報保護管理者1人を置き、各班等の長をもって充てる。
- 4 個人情報保護管理者は、あらかじめ、その所属する班等に属する職員のうちから、副個人情報保護管理者を指名することができる。
- 5 当法人に、個人情報保護監査責任者1人を置き、理事の中より理事長が指名した理事をもって充てる。

(総括個人情報保護管理者等の任務)

第6条 総括個人情報保護管理者は、当法人における保有個人情報の管理に関する事務を総括する。

- 2 副総括個人情報保護管理者は、総括個人情報保護管理者の命を受けて、総括個人情報保護管理者を補佐する。
- 3 個人情報保護管理者は、各班等における保有個人情報を適切に管理する任に当たる。
- 4 副個人情報保護管理者は、個人情報保護管理者の命を受けて、個人情報保護管理者を補佐する。
- 5 個人情報保護監査責任者は、保有個人情報の管理の状況について監査する任に当たる。

(保有個人情報の適切な管理のための連絡及び調整)

第7条 総括個人情報保護管理者は、当法人の保有する個人情報の管理に係る重要事項の決定のためその他必要があると認めるときは、当法人における理事会等において、調整を行う。

(教育研修)

第8条 総括個人情報保護管理者は、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 総括個人情報保護管理者は、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 個人情報保護管理者は、その所属する班等の職員に対し、保有個人情報の適切な管理のために、総括個人情報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2章 個人情報の管理

第1節 個人情報の取得、利用等

(利用目的の特定)

第9条 課等は、個人情報を保有するに当たっては、法令の定める所掌事務を遂行するため必要な場合に限り、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 班等は、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、個人情報を保有してはならない。

3 班等は、利用目的を変更する場合には、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10条 班等は、本人から直接文書等（文書、図画及び電磁的記録（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で作られた記録をいう。）をいう。）に記録された当該本人の個人情報を取得するときは、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（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）第2条第1項に規定する独立行政法人等をいう。）、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。）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。

（利用目的以外の目的のための利用及び提供の制限）

第11条 個人情報保護管理者は、法第8条第1項又は第2項の規定により保有個人情報を利用目的以外の目的のために利用し、又は提供しようとする場合は、原則として、あらかじめ、副総括個人情報保護管理者に通知しなければならない。

（保有個人情報を提供する場合の措置）

第12条 個人情報保護管理者は、法第8条第1項又は第2項第2号から第4号までの規定により保有個人情報を提供しようとする場合は、当該保有個人情報の提供を受ける者に対し、原則として、その利用しようとする保有個人情報に関する次に掲げる事項について、書面で確認するものとする。

- （1）記録範囲及び記録項目
- （2）利用の目的
- （3）利用の形態
- （4）その他必要と認める事項

2 個人情報保護管理者は、前項の場合において必要があると認めるときは、同項の規定により確認した利用の形態等について実地の調査等を行い、又は改善を要求する等必要な措置を講ずる。

（業務を委託する場合の措置）

第13条 保有個人情報の取扱いに係る業務を外部に委託（請負契約のための発注を含む。以下この条において同じ。）をする者は、個人情報の適切な管理を行う能力を有すると認める者と契約しなければならない。

2 委託に関する契約書には、次に掲げる事項を記載する。

- （1）個人情報に関する秘密保持等の義務
- （2）再委託の制限又は条件に関する事項
- （3）個人情報の複製等の制限に関する事項
- （4）個人情報の安全確保に関する事項
- （5）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
- （6）個人情報の管理の状況についての調査に関する事項
- （7）契約終了時における個人情報が記録された媒体の返却に関する事項
- （8）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

3 保有個人情報の取扱いに係る業務を外部に委託をする者は、契約を締結した後、委託先における管理体制について確認する。

(派遣労働者の派遣を受ける場合の措置)

第14条 保有個人情報の取扱いに係る業務を派遣労働者に行わせる者は、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しなければならない。

第2節 個人情報を保有する班等において行う安全確保の措置

(保有個人情報の管理区分)

第15条 個人情報保護管理者は、保有個人情報の漏えい、滅失又はき損の防止その他の保有個人情報の適切な管理のために、次の表の左欄に掲げる区分に応じ、同表の右欄に掲げる管理区分に管理する。

秘匿性を有し、漏えいした場合、重大な支障が生じるおそれがあるため、厳重に管理することが適当と判断される保有個人情報	管理A
管理Aに区分されるもの以外の保有個人情報であって、本人の数が千人以上のもの及びこれに準ずる管理が適当と判断されるもの	管理B
管理A又は管理Bに区分されるもの以外の保有個人情報	管理C

2 個人情報保護管理者は、保有個人情報について、前項の管理区分に応じて、経済産業省個人情報保護管理マニュアル（20120904 シ第2号。以下「マニュアル」という。）で定める保有個人情報の取扱方法に準拠し、次に掲げる事項を定めるものとする。

- (1) 保有個人情報のアクセス制限に関すること。
- (2) 保有個人情報の暗号化に関すること。
- (3) 保有個人情報の複製等の制限に関すること。
- (4) 保有個人情報が記録された媒体の保管等に関すること。
- (5) 保有個人情報の廃棄等に関すること。
- (6) 保有個人情報のバックアップに関すること。

3 個人情報保護管理者は、前項の規定により定めた保有個人情報の取扱方法について、必要があると認めるときは、その見直し等を行う。

(アクセス制限)

第16条 個人情報を保有する班等の職員（以下この節において「班員」という。）は、前条第2項の規定により個人情報保護管理者が定めた方法に従い、保有個人情報のアクセス制限を行わなければならない。

2 班員は、アクセス権限を有しない保有個人情報にアクセスしてはならない。

3 班員は、アクセス権限を有する保有個人情報であっても、業務上の目的以外の目的でこれにアクセスしてはならない。

(暗号化)

第17条 班員は、次に掲げる行為については、第15条第2項の規定により個人情報保護管理者が定めた方法に従い、保有個人情報（情報システムに係るものに限る。）の暗号化を行わなければならない。

- (1) 保有個人情報の共有ドライブ（当該保有個人情報に係るアクセス権限を有する課員のみがアクセスすることが可能な共有ドライブを除く。）への保存
- (2) 保有個人情報が記録されている媒体の外部への持出し
- (3) 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

(複製等の制限)

第18条 班員は、次に掲げる行為については、第15条第2項の規定により個人情報保護管理者が定めた方法によりこれを行わなければならない。

- (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

(媒体の保管等)

第19条 班員は、第15条第2項の規定により個人情報保護管理者が定めた方法に従い、保有個人情報が記録されている媒体を保管しなければならない。

(廃棄等)

第20条 班員は、保有個人情報又は保有個人情報が記録されている媒体（端末及びサーバ内に内蔵されているものを含む。）が不要となった場合には、第15条第2項の規定により個人情報保護管理者が定めた方法に従い、当該保有個人情報の確実な消去又は当該媒体の廃棄を行わなければならない。

(バックアップ)

第21条 班員は、第15条第2項の規定により個人情報保護管理者が定めた方法により、保有個人情報（情報システムに係るものに限る。）のバックアップを行わなければならない。

(誤り等の訂正等)

第22条 班員は、保有個人情報の内容に誤り等を発見した場合には、当該誤り等が明らかに軽微であると認められる場合を除き、個人情報保護管理者の指示に従い、当該誤り等の

訂正等を行わなければならない。

(第三者の閲覧防止)

第23条 班員は、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ることがないように、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じなければならない。

(アクセス記録)

第24条 個人情報保護管理者は、保有個人情報（情報システムに係るものに限る。）について、必要に応じて当該保有個人情報へのアクセス状況を分析しなければならない。

(情報システム設計書等の管理)

第25条 保有個人情報に係る情報システムの設計書及び構成図等の文書を保有している課等の長は、当該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、複製等及び廃棄について必要な措置を講じなければならない。

第3節 システム管理班等において行う安全確保の措置

(アクセス制御の措置)

第26条 システム管理班等の長は、保有個人情報に係る情報システムについて、第15条第1項の管理区分に応じてマニュアルで定める保有個人情報の取扱方法に従い、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など、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。

(アクセス記録の措置)

第27条 システム管理班等の長は、個人情報保護管理者から申請があった場合には、保有個人情報（情報システムに係るものに限る。）へのアクセス状況を記録し、並びにその記録を一定の期間保存し、及び分析するために必要な措置を講じなければならない。

2 システム管理班等の長は、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。

(暗号化の措置)

第28条 システム管理班等の長は、保有個人情報に係る情報システムについて、第15条第1項の管理区分に応じてマニュアルで定める保有個人情報の取扱方法に従い、暗号化のために必要な措置を講じなければならない。

(バックアップの措置)

第29条 システム管理班等の長は、保有個人情報について、第15条第1項の管理区分に

応じてマニュアルで定める保有個人情報の取扱い方法に従い、バックアップを行うための必要な措置を講じなければならない。

(外部からの不正アクセスの防止)

第30条 システム管理班等の長は、保有個人情報に係る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等の必要な措置を講じなければならない。

(コンピュータウイルスによる漏えいの防止)

第31条 システム管理班等の長は、コンピュータウイルスによる保有個人情報（情報システムに係るものに限る。）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じなければならない。

(管理区域の立入り等)

第32条 機器管理班等（別表の情報システム欄に掲げる情報システムに応じ、同表の乙欄に掲げる班等をいう。以下この条及び次条において同じ。）の長は、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区域（以下この条及び次条において「管理区域」という。）に立ち入ることのできる権限を有する者を定めるとともに、用件の確認、立入りの記録、部外者についての識別化及び部外者が立ち入る場合の必要に応じた職員の立会い等の措置を講じなければならない。

2 機器管理班等の長は、必要があると認めるときは、管理区域の出入口の特定化及び所在表示の制限等の措置を講じなければならない。

3 機器管理班等の長は、管理区域の立入りの管理について、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、認証カ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等の措置を講じなければならない。

(管理区域に関する措置)

第33条 機器管理班等の長は、外部からの不正な侵入に備え、管理区域に施錠装置、警報装置及び監視設備を設置する等必要な措置を講じなければならない。

2 機器管理班等の長は、災害等に備え、管理区域に、耐震、防火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3章 個人情報ファイルの保有等に関する通知等

(個人情報ファイルの保有等に関する通知)

第34条 個人情報ファイル（法第10条第2項第1号から第10号までに掲げるものを除く。）を保有しようとする個人情報保護管理者は、あらかじめ、マニュアルで定める事項

を副総括個人情報保護管理者に通知しなければならない。通知した事項を変更しようとするときも、同様とする。

- 2 個人情報保護管理者は、管理A及び管理Bに区分される保有個人情報（法第10条第2項第1号から第8号まで及び第10号に掲げるもの並びに前項の規定により通知を行ったものを除く。）を保有したときは、遅滞なく、マニュアルで定める事項を副総括個人情報保護管理者に通知しなければならない。通知した事項を変更したときも、同様とする。

（個人情報ファイル簿の整備）

第35条 総括個人情報保護管理者は、法第11条の規定に従い、当法人の個人情報ファイル簿を整備しなければならない。

- 2 総括個人情報保護管理者は、個人情報ファイル簿の整備に当たっては、秘密保全の必要について十分留意するものとする。
- 3 個人情報ファイル簿は、整備上必要な場合を除き、閲覧所に備え置き、一般の閲覧に供するものとする。

（保有個人情報の取扱いの状況の記録）

第36条 副総括個人情報保護管理者は、第34条の規定により通知を受けた保有個人情報について、台帳を整備し、当該保有個人情報の利用及び保管等の取扱いについて記録しなければならない。

第4章 事故の報告及び再発防止措置

（事故の報告）

第37条 保有個人情報の漏えいその他個人情報の管理に関して問題となる事案が発生したことを知った職員は、直ちに、当該保有個人情報を管理する個人情報保護管理者にその旨を報告しなければならない。

- 2 個人情報保護管理者は、前項の規定により職員から報告を受けたときは、速やかに副総括個人情報保護管理者に報告するとともに、被害の拡大防止又は復旧等のために必要な措置を講じなければならない。
- 3 個人情報保護管理者は、前項の措置を講じた後、速やかに、事案の発生した経緯、被害状況等を調査し、その調査結果を総括個人情報保護管理者及び副総括個人情報保護管理者に報告しなければならない。ただし、軽易な事案としてマニュアルで定めるものについては総括個人情報保護管理者への報告は要しない。
- 4 個人情報保護管理者は、事案の内容、影響等に応じて、事実関係の公表、当該事案に係る本人への対応等の措置を講じなければならない。

（再発防止措置）

第38条 個人情報保護管理者は、保有個人情報の漏えいその他個人情報の管理に関して問

題となる事案が発生した場合には、前条第3項の調査結果に基づき、当該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じなければならない。

- 2 個人情報保護管理者は、事案の内容、影響等に応じて、前項の規定により講じた措置を公表しなければならない。

第5章 点検及び監査

(点検)

第39条 個人情報保護管理者は、保有個人情報について、毎年、点検を行い、その結果を副総括個人情報保護管理者に報告する。

- 2 副総括個人情報保護管理者は、必要があると認めるときは、前項の点検の結果を総括個人情報保護管理者に報告する。

(監査)

第40条 個人情報保護監査責任者は、保有個人情報の管理及び利用の状況について、定期に又は随時に監査を行い、その結果を総括個人情報保護管理者に報告する。

- 2 個人情報保護監査責任者は、被監査部門から独立した者（次項において「監査事務実施者」という。）をもって、前項の監査に必要な事務を行わせることができる。
- 3 監査事務実施者は、前項の規定により監査を行った場合には、その結果を個人情報保護監査責任者に報告する。

(評価及び見直し)

第41条 副総括個人情報保護管理者は、保有個人情報の適切な管理のための措置について、点検又は監査の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等を行う。

- 2 副総括個人情報保護管理者は、前項の見直し等の結果を総括個人情報保護管理者に報告する。

第6章 補則

(細則の策定)

第42条 総括個人情報保護管理者は、この規程の実施に必要な細則を定めることができる。

この規定は、平成27年1月10日から施行する。

別表

情報システム
1 当法人のネットワークに接続された情報システム
2 専ら調査統計グループにおける統計調査に関する事務の処理のために使用される情報システムであって、当法人のネットワークに接続されたもの
3 公開するホームページの運用を行うために使用される情報システム、専ら電子申請の受付等に関する事務の処理のために使用される情報システム、専ら入会申込に関する事務の処理のために使用される情報システムであって、当法人のネットワークに接続されたもの
4 個別業務に関する事務のために使用される情報システムであって、当法人のネットワークに接続されたもの
5 上記以外の情報システム