国立研究開発法人国立国際医療研究センターの保有する個人情報の保護に関する規程

平成２２年４月１日規程第４１号

国立研究開発法人国立国際医療研究センターの保有する個人情報の保護に関する規程

第１章　総則

（目的）

第１条　この規程は、国立研究開発法人国立国際医療研究センター（以下「センター」という。）において個人情報の利用が拡大していることにかんがみ、センターにおける個人情報の取扱いに関する基本的事項を定めることにより、センターの事務及び事業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。

２　センターにおける個人情報の取扱いについては、法令に定めるもののほか、この規程に定めるところによる。

（定義）

第２条　この規程において、次の各号に掲げる用語の意義については、それぞれ各号に定めるところによる。

一　個人情報　生存する個人に関する情報であって、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む。）をいう。

二　保有個人情報　センターの役員及び職員（派遣労働者を含む。以下「役職員」という。）が職務上作成し、又は取得した個人情報であって、役職員が組織的に利用するものとして、センターが保有しているものをいう。ただし、国立研究開発法人国立国際医療研究センター文書管理規程（平成２２年規程第３７号。以下「文書管理規程」という。）第２条第３項に規定する文書（以下「法人文書」という。）に記録されているものに限る。

（総括個人情報保護管理者）

第３条　センターに総括個人情報保護管理者を置くこととし、企画戦略局長をもって充てる。

２　総括個人情報保護管理者は、センターにおける保有個人情報の管理に関する事務を総括する。

３　総括個人情報保護管理者は、前項に規定する事務のうち、それぞれの部署に関するものについては、次の副総括個人情報保護管理者に行わせることができる。

部　　署	副総括個人情報保護管理者

研究所	研究所長
臨床研究センター	臨床研究センター長
センター病院	病院長
国府台病院	国府台病院長
国際医療協力局	国際医療協力局長
国立看護大学校	国立看護大学校長
事務部門	統括事務部長

（個人情報保護管理者）

第４条　研究所、臨床研究センター、センター病院、国府台病院、国際医療協力局、　国立看護大学校及び事務部門（以下、「研究所等」という。）に主任個人情報保護管理者を置くこととし、次のとおりそれぞれの役職者をもって充てる。

部　　署	主任個人情報保護管理者
研究所	副所長、糖尿病研究センター長、肝炎・免疫研究センター長
臨床研究センター	臨床研究センター各部長
センター病院	センター病院副院長、エイズ治療・研究開発センター長、国際感染症センター長
国府台病院	国府台病院副院長
国際医療協力局	運営企画部長
国立看護大学校	事務部長
事務部門	総務部長、人事部長、企画経営部長、財務経理部長、事務部長

２　主任個人情報保護管理者は、研究所等における保有個人情報の管理に関する事務をつかさどる。

３　保有個人情報を取り扱う部、課、室（以下、「課等」という。）の長は、個人情報保護管理者として、各課等における保有個人情報の適切な管理を確保するものとする。保有個人情報を情報システムで取り扱う場合、個人情報保護管理者は、当該情報システムを管理する者と連携して、その適切な管理に当たるものとする。

４　副総括個人情報保護管理者が指名する者に、第２項に規定する主任個人情報保護管理者が行う事務を代行させることができる。

（保護担当者）

第５条　個人情報保護管理者は、当該課等の職員のうちから個人情報保護担当者を指名することができる。

２　個人情報保護担当者は個人情報保護管理者を補佐し、当該課における保有個人情報を管理する事務を担当する。

第６条　個人情報保護管理者は、事務取扱担当者がこの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を整備する。

（個人情報管理委員会）

第７条　総括個人情報保護管理者は、センターにおける保有個人情報の管理に係る重要事項の決定、連絡調整等を行うため必要があると認めるときは、個人情報管理委員会を（以下「委員会」という。）を設け、随時に開催するものとする。

２　委員会の委員長は、総括個人情報保護管理者とする。

３　委員会の委員は、主任個人情報保護管理者及び個人情報保護管理者のうち総括個人情報保護管理者が必要と認める者とする。

４　委員会の庶務は、総務部総務課において行う。

５　前各項に規定するほか、委員会に関し必要な事項は、総括個人情報保護管理者が別に定める。

（役職員の責務）

第８条　役職員は、関連する法令、この規程その他の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、主任個人情報保護管理者、個人情報保護管理者及び個人情報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２章　　保有個人情報の取扱い

（アクセス制限）

第９条　個人情報保護管理者は、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（以下「アクセス権限」という。）を有する役職員とその権限の内容を、当該役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役職員は、保有個人情報にアクセスをしてはならない。

３　役職員は、アクセス権限を有する場合であっても表無上の目的以外の目的で保有個人情報にアクセスをしてはならない。

（複製等の制限）
第１０条　個人情報保護管理者は、保有個人情報の複製、送信、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等の業務について、当該保有個人情報の秘匿性等その内容に応じて、当該業務を行うことができる場合を限定するものとする。
２　役職員は、前項の業務を行うときは、個人情報保護管理者の指示に従い、当該保有個人情報の秘匿性等その内容に応じて、必要最小限の範囲においてこれらを行うとともに、漏えい等が行われないよう取扱いに注意するものとする。

（誤りの訂正等）
第１１条　役職員は、保有個人情報の内容に誤り等を発見した場合には、個人情報保護管理者の指示に従い、訂正等を行うものとする。

（媒体の管理等）
第１２条　役職員は、個人情報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、必要に応じ、耐火金庫等への保管、施錠等を行うものとする。

（廃棄等）
第１３条　役職員は、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、個人情報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る当該情報の消去又は当該媒体の廃棄を行うものとする。

（保有個人情報の取扱状況の記録）
第１４条　個人情報保護管理者は、必要に応じて保有個人情報の秘匿性等その内容に応じた台帳等を整備して、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ものとする。

第３章　　情報システムの安全確保等

（アクセス制御）
第１５条　個人情報保護管理者（情報システムを取り扱う個人情報保護管理者に限る。以下この章及び次章において同じ。）は、保有個人情報（情報システムで取り扱うものに限る。以下この章（第２４条を除く。）及び次章において同じ。）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ものとする。この場合の措置内容は、第９条により設定した必要最小限のアクセス権限を具体化するものとする。

第１６条　個人情報保護管理者は、前条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ものとする。
２　役職員は、自己の利用する保有個人情報に関して認証機能が設定されている場合、その認証機能の適切な運用を行うものとする。

（アクセス記録）
第１７条　個人情報保護管理者は、保有個人情報（特定個人情報を除く。）の秘匿性等その内容に応じて、当該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的に分析するために必要な措置を講ずるものとする。
２　個人情報保護管理者は、特定個人情報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ものとする。
３　個人情報保護管理者は、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ものとする。

（アクセス状況の監視）
第１８条　個人情報保護管理者は、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ものとする。

（管理者権限の設定）
第１９条　個人情報保護管理者は、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、当該特権を最小限とする等の必要な措置を講ずるものとする。

（外部からの不正アクセスの防止）
第２０条　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ネットワーク経路制御等の必要な措置を講ずるものとする。

（不正プログラムによる漏えい等の防止）
第２１条　個人情報保護管理者は、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、ソフトウエ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（導入したソフトウエアを常に最新の状態に保つことを含む。）を講ずるものとする。

（情報システムにおける保有個人情報の処理）
第２２条　役職員は、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ものとする。
２　個人情報保護管理者は、前項の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ものとする。

（暗号化）
第２３条　個人情報保護管理者は、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ものとする。
２　役職員は、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（適切なパスワードの選択、パスワードの漏えい防止の措置等を含む。）を行うものとする。

（入力情報の照合等）
第２４条　役職員は、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ものとする。

（バックアップ）
第２５条　個人情報保護管理者は、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ものとする。

（情報システム設計書等の管理）
第２６条　個人情報保護管理者は、保有個人情報に係る情報システムの設計書、仕様書、ネットワーク構成図等の文書について漏えい等が行われないよう、その保管、複製、廃棄等について必要な措置を講ずるものとする。

（端末の限定）
第２７条　個人情報保護管理者は、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ものとする。

（端末の盗難防止等）
第２８条　個人情報保護管理者は、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ものとする。
２　役員は、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。ただし、個人情報保護管理者の指示に従い、業務の必要最小限の範囲において行うときはこの限りではない。

３　役職員は、前項の規定に基づき、端末を外部へ持ち出したときは、紛失による漏えい等が行われないよう取扱いに注意するものとする。

（第三者の閲覧防止）

第２９条　役職員は、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ものとする。

（記録機能を有する機器・媒体の接続制限）

第３０条　個人情報保護管理者は、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ものとする。

第４章　情報システム室等の安全管理

（入退管理）

第３１条　個人情報保護管理者は、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、部外者の識別、部外者が立ち入る場合の役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ものとする。

２　個人情報保護管理者は、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ものとする。

３　個人情報保護管理者は、情報システム室等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。）、パスワードの読取防止等を行うために必要な措置を講ずるものとする。

（情報システム室等の管理）

第３２条　個人情報保護管理者は、外部からの不正な侵入に備え、情報システム室等への施錠装置、警報装置、監視設備等の設置等の措置を講ずるものとする。

２　個人情報保護管理者は、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ものとする。

（保管施設の管理）

第３３条　個人情報保護管理者は、保有個人情報を記録する電磁的記録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、前２条に規定す

る措置に準じて、所要の措置を講ずるものとする。

（執務室等に設置する場合の特例）
第３４条　個人情報保護管理者は、情報システム室等について、専用の部屋を確保するのが困難である等の理由により執務室内にサーバ等を設置する場合において、必要があると認めるときは、第３１条及び第３２条に規定する措置に準じて、所要の措置を講ずるものとする。

第５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３５条　個人情報保護管理者は、法令に基づき他の行政機関及び独立行政法人等以外の者に保有個人情報（特定個人情報を除く。第３６条及び第３７条において同じ。）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。

第３６条　個人情報保護管理者は、法令に基づき他の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ものとする。

第３７条　個人情報保護管理者は、法令に基づき他の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条に規定する措置を講ずるものとする。

（特定個人情報の提供）
第３８条　個人情報保護管理者は、番号法で限定的に明記された場合を除き、特定個人情報を提供してはならない。

（業務の委託等）
第３９条　個人情報保護管理者は、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ものとする。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。
一　個人情報に関する秘密保持、目的外利用の禁止等の義務
二　再委託の制限又は事前承認等再委託に係る条件に関する事項

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、損害賠償責任に関する事項
七　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ものとする。
３　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、委託先において、センター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う。
４　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第２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。
５　個人情報保護管理者は、個人番号利用事務等の全部又は一部の委託先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。

第４０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とともに、労働者派遣契約が、保有個人情報の適切な取扱いを行うことに配慮されたものとする。

第６章　安全確保上の問題への対応

（安全確保上の問題への対応）
第４１条　保有個人情報の漏えい等の事案が発生又は兆候等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役職員は、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報告しなければならない。この場合において、役職員は、時間を要する事実確認を行う前にまず個人情報保護管理者に報告するものとする。
２　前項の報告を受けた個人情報保護管理者は、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う得る措置については、直ちに行う（役職員に行わせることを含む。）ものとする。
３　第１項の報告を受けた個人情報保護管理者は、事案の発生した経緯、被害状況を調

査し、総括個人情報保護管理者及び主任個人情報保護管理者に報告しなければならない。ただし、特に重大と認める事案が発生した場合には、直ちに総括個人情報管理者及び主任個人情報保護管理者に当該事案の内容等について報告しなければならない。

4　第１項の報告を受けた個人情報保護管理者は、事案の内容等に応じ、総括個人情報保護管理者の指示に基づき、当該事案の内容、経緯、被害状況等を理事長に速やかに報告しなければならない。

5　個人情報保護管理者は、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じなければならない。

（公表等）

第４２条　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連絡の対応等の措置を講じなければならない。

2　個人情報保護管理者は、公表を行う事案については、その事案の内容、経緯、被害状況等について、速やかに総括個人情報保護管理者に情報提供を行うものとする。

3　個人情報保護管理者は、公表を行う事案について、統括事務部総務部総務課広報係長を経由して、速やかに厚生労働省に情報提供を行うものとする。

第７章　雑則

（教育研修）

第４３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役職員に対し、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ものとする。

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役職員に対し、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ものとする。

3　総括個人情報保護管理者は、個人情報保護管理者及び保有個人情報の取扱いに従事する役職員に対し、現場における保有個人情報の適切な管理のための教育研修を実施するものとする。

4　個人情報保護管理者は、当該課等の役職員に対し、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ものとする。

（監査）

第４４条　監査室長は、保有個人情報の適切な管理を検証するため、本規定に係る措置の状況を含む保有個人情報の管理の状況について、定期に又は必要に応じ随時に監査（外部監査を含む。以下同じ。）を行い、その結果を総括個人情報保護管理者に報告する。

（点検）
第４５条　主任個人情報保護管理者は、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、その結果を総括個人情報保護管理者に報告するものとする。

（評価及び見直し）
第４６条　総括個人情報保護管理者及び主任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、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じるものとする。

（行政機関との連携）
第４７条　センターは、「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、厚生労働省と緊密に連携して、保有個人情報等の適切な管理を行う。

第４８条　この規程に定めるもののほか、開示及び訂正等その他個人情報の取扱いに関し必要な事項は、別に定める

附　則

（施行期日）
この規程は、平成２２年４月１日から施行する。

附　則（平成２３年規程第９号）

（施行期日）
この規程は、平成２３年１１月１日から施行する。

附　則（平成２４年４月１日規程第８号）

（施行期日）
この規程は、平成２４年４月１日から施行する。

附　則（平成２７年３月３１日規程第９号）

（施行期日）
この規程は、平成２７年４月１日から施行する。

附　則（平成２７年３月３１日規程第１９号）

（施行期日）
この規程は、平成２７年４月１日から施行する。

附　則（平成２８年４月２８日規程第１１号）

（施行期日）
この規程は、平成２８年４月２９日から施行する。