医学部附属病院における医療情報の管理に係る実施手順

平成 19 年 2 月 9 日制定

１．目的

本実施手順は、神戸大学情報セキュリティポリシー（以下「情報セキュリティポリシー」という。） 1.3.3 「実施手順等」及び同 3.6 「入試情報・医療情報・図書館情報・附属学校における情報における実施手順等」により、医学部附属病院における研究については、患者の個人の情報そのものが研究資料となることを考慮する必要があることから、研究に係る医療情報について、分類を定義し、管理の原則を定めるものである。

本実施手順の目的は、本学の運営のために医学部附属病院が保持する医療情報に係る情報セキュリティに対する侵害を阻止するとともに、本学内外の情報に係る情報セキュリティに対する加害行為を阻止することであり、情報セキュリティポリシーの対象者が必ず遵守すべき最低限のルールを定めるものである。医学研究分野における情報については、さらに各種関連法令・通知・指針等（以下「関連法令等」という。）を遵守し、適正な取扱を図らなければならない。

なお、診療・医療に関わる医療情報の取扱については、関連法令等に定めるもののほか、「神戸大学医学部附属病院の保有する医療に係る個人情報の適切な管理のための措置等に関する内規」（平成 17 年 3 月 30 日制定）及び「全教職員等が守るべき具体的事項」（平成 17 年 3 月 30 日医学部附属病院長通知）によるものとする。

２．定義

本実施手順における用語の定義は以下のとおりとし、その他の用語の定義については、情報セキュリティポリシーによるものとする。

（１）医療研究情報

医学部附属病院において診療・研究に従事する者が作成し、又は取得した診療情報・健康情報（他の医療機関等から提供された情報を含む。）等の個人の医学的・身体的情報を基盤とした、医療・医学に関わる研究情報（作成時又は取得時において電磁的記録でないものであって、将来的に電磁的記録となり得るもの及び電磁的記録をプリント出力したものを含む。）をいい、病院診療に係る情報を含まない。

（２）病院情報ネットワーク

医学部附属病院の診療業務を目的として楠地区内に敷設されたプライベートネットワークをいう。

（３）公開用セグメント

本学情報ネットワーク上において、医学部附属病院が情報公開を目的として

利用する 133.30.188.0/24 の IP アドレスのネットワークをいう。

（４）研究系ネットワーク

本学情報ネットワーク上において、医学部附属病院職員が利用する公開用セグメントを除く 133.30.176.0/20 の IP アドレスのネットワークをいう。

３．対象者

本実施手順の対象は、上記２．定義（１）に示す医療情報を取扱う者すべてとし、医学部附属病院に所属するか否か、勤務態様が常勤であるか否か及び教職員であるか否かを問わない。

４．本実施手順における医療研究情報の分類

（１）個人に関連する情報を含まない情報

個人に関連する情報を一切含まない情報（統計情報等）

（２）連結不能匿名化情報

個人に関連する情報から、姓名、住所、電話番号、病院患者 ID など個人の特定に結び付く情報をすべて除去し、又は再連結可能な情報を持たせずに分離したもの。

なお、直接的に個人の特定に結び付く情報を含まない場合であっても、組合せにより個人を絞り込める可能性がある場合は、「（４）非匿名化個人情報」として取扱うものとする。

（３）連結可能匿名化個人情報

個人に関連する情報から、姓名、住所、電話番号、病院患者 ID 等個人の特定に結び付く情報のすべてを、再連結可能な情報をもたせて分離したもの。（病院患者 ID を連結キーの目的で残した場合は、匿名化に該当しないことに注意すること。）

（４）非匿名化個人情報

個人に関連する情報に、姓名、住所、電話番号、病院患者 ID など個人の特定に結び付く情報が含まれるもの。

（５）特別な取扱が必要な情報

ヒトゲノム・遺伝子解析研究等、関連法令等によって、個人情報管理責任者を置くなど、特別な取扱が求められている情報。

なお、「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「個人情報保護法」という。）では、死亡した者に係る個人情報については法の対象とされていないが、その場合であっても、死亡した個人の情報を保存している場合には、漏えい、滅失又はき損等の防止を図るなど適正に取り扱われることが期待されており、また、死亡した個人に関する情報が、同時に、遺族等の生存する個人に関係する情報（ゲノム情報、遺伝情報等）でもある場合には、当該生存する個人に関する情報として個人情報保護法の対象となることから、本実施手順においては、原則として、死亡した者に

係る個人情報は、生存している者の個人情報と同等に取扱うものとする。

５．情報の取扱

（１）情報の分類化と見直し

情報の取扱に際しては、まず当該情報を上記４に掲げる分類に慎重に分類し、下記（３）～（７）に従い適切に取扱うこと。

また、分類後も、情報の構成を変更するごとに、分類区分が変更されないか検討し、常に適切な分類により情報が管理されるように留意するものとする。

（２）遵守すべきガイドライン等

個人に関連する情報を含まない情報については、本学の「研究情報管理ガイドライン（研究情報の管理に関する事項）（平成 16 年 9 月 29 日制定（平成 17 年 3 月 25 日改正））」を遵守するものとし、それ以外の情報（上記４に掲げる分類（２）～（４）に該当する情報）については、併せて個人情報保護法、「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 24 日厚生労働省通知、平成 18 年 4 月 21 日改正）、「医療情報システムの安全管理に関するガイドライン」（平成 17 年 3 月厚生労働省作成）及び「全教職員等が守るべき具体的事項」（平成 17 年 3 月 30 日医学部附属病院長通知）を遵守するものとする。

また、以下の指針に該当する研究において取扱う情報については、当該指針を遵守すること。

・ヒトゲノム・遺伝子解析研究に関する倫理指針（平成 16 年 12 月 28 日告示改定）
・疫学研究に関する倫理指針（平成 16 年 12 月 28 日告示改定）
・遺伝子治療臨床研究に関する指針（平成 16 年 12 月 28 日告示改定）
・臨床研究に関する倫理指針（平成 16 年 12 月 28 日告示改定）
・ヒト幹細胞を用いる臨床研究に関する指針（平成 18 年 9 月 1 日施行）

（３）個人に関連する情報を含まない情報

一般的な研究情報として取扱うものとする。必要に応じて公開可能であるが、公開前に個人に関連する情報が含まれていないことを慎重に確認するものとする。

（４）連結不能匿名化情報

一般的な研究情報としての取扱が可能であるが、匿名化の個人に由来する情報の組合せにより、個人を絞り込める可能性がある場合は、「（６）非匿名化個人情報」に準じて取扱うこと。必要に応じて公開可能であるが、公開前に個人の特定に関連する情報が含まれていないことを慎重に確認するものとする。

（５）連結可能匿名化個人情報

・原則として、一般的な研究情報としての取扱が可能であるが、連結不能匿

名化情報の場合と同様に個人に由来する情報の組合せにより、個人を絞り込める可能性がある場合は、「（６）非匿名化個人情報」に準じて取扱うものとし、非公開とする。

ただし、特別の理由により公開する必要がある場合は、連結用の情報を除去するものとする。

・連結可能な相互の情報は、その存在場所が、単独の情報機器、ネットワーク上又は USB メモリ等の物理的な別メディアであるか否か及び暗号化の有無にかかわらず、単独の資格情報、同一のパスワードによって参照できるものであってはならない。

・分離された情報は、異なるアカウント・パスワードによりアクセスを制御し、若しくは暗号化し、又は明示的に再連結を企図する場合を除いて、個人を識別する情報を、別の管理者の管理下等に置き、物理的な認証が必要な状態で管理すること。

（６）非匿名化個人情報

・関連法令等に定めのある場合を除き、公開してはならない。取扱う情報の非匿名化の必要性を十分検討し、可能な限り匿名化等の対応を考慮すること。

・情報の作成者又は取得者は、当該情報の廃棄まで責任を持って一貫した管理を行い、不要となった情報については、速やかに、「パソコン、サーバ及び外部記憶メディアの廃棄時における取扱い」（平成１８年１１月１６日情報管理室長通知）に基づいて適切な廃棄を行うこと。

（７）特別な取扱が必要な情報

ヒトゲノム・遺伝子解析研究等、各種ガイドラインによって、再連結匿名化に際して個人情報管理責任者を置く等の特別な取扱が求められているものについては、それによるものとする。

６．情報ネットワーク上における取扱

（１）研究公開用サーバ

研究公開用サーバは、公開用セグメントに設置し、学内・学外等必要な範囲に対して、必要な通信ポートのみ開放するものとする。

（２）利用者端末

医療研究情報を取扱う端末では、必ず個人認証を行い、取扱う情報に応じて適宜、生体認証を含む複数要素認証を行うものとする。医療研究情報は、病院情報ネットワークに設置された診療用端末上で取扱うことを原則とし、特別な理由により、やむを得ず研究系ネットワーク上に設置された端末で取扱う場合は、最低限、以下の管理が行われた端末を使用するものとする。

ａ．ＯＳ及びインストール済みアプリケーションのセキュリティアップデートを常に行い、最新の状態に保たれていること。

ｂ．常時、オンアクセス検出が可能なウィルス対策ソフトが導入さ

れ、常に最新のウィルス定義ファイルに更新されていること。

ｃ．ファイル交換ソフトがインストールされていないこと。

ｄ．ファイアーウォール機能等で必要なポート以外をすべて閉じて外部からのアクセスができない状態であること。

また、可能な限り、以下の対策を行うこと。

・ファイルシステム又はアプリケーションによる暗号化

・フォルダ又はファイル単位での限定的な読取りアクセス権の設定

・通常用いるシステム利用アカウントの非特権ユーザレベル化

・セキュリティ対策ソフトウェア又はハードウェアによる、通常の外部アクセスで用いられるポート以外に向けられた外部へのアクセスの遮断

（３）限定された対象に対する情報共有サーバ

・研究上の必要により、サーバ又は利用者端末（以下「サーバ等」という。）において、楠地区内の限定された対象に対して情報を共有する場合、当該サーバ等は、原則として病院情報ネットワーク上に設置し、必要なポートのみを開放し、必要な範囲に対して、必要な情報のみが、適切な認証の後にのみ利用できるようにするものとする。

・当該サーバ等のファイアーウォール機能又はネットワーク機器等により、利用可能対象 IP アドレス制限及びポート制限を行い、利用者ごとにアカウントを発行・管理し、共有するフォルダ等にのみアクセス許可を設定するものとする。

（４）可搬型記憶メディア

・医療研究情報は、一時的な情報の移動を目的として保存する場合を除き可搬型記憶メディアには保存しないものとする。

　また、一時的な情報の移動を目的として保存する場合にあっても、メディア自体の暗号化又はファイル単位での暗号化を行うものとする。

・情報の消去に当たっては、通常のファイル削除による消去及びメディアの初期化による消去だけではなく、メディア上の情報断片がすべて消去される完全消去を行うソフトウェアを用いて消去すること。情報が不要となり廃棄する場合は、「パソコン、サーバ及び外部記憶メディアの廃棄時における取扱い」（平成１８年１１月１６日情報管理室長通知）に基づいて適切な廃棄を行うこと。

（５）電子メール

　電子メールにより情報を送信する場合、当該電子メールの受信者において、本実施手順による管理が及ばない範囲への自動転送設定がなされている可能性は否定できないことから、匿名性の低い医療情報を電子メールで発信する場合は、当該電子メールの受信者のメールアカウントが、病院情報ネットワークの個人メールアカウントのみであり、かつ、転送の可能性が完全に否定

される場合を除き、当該電子メールの内容の暗号化を行うものとする。

７．実施手順の運用と監査

本実施手順の適正な運用のため、情報の管理責任者は、本実施手順を業務マニュアル集等に整備し、教職員採用時研修、職員研修等において周知しなければならない。

また、必要に応じて、適宜、詳細な運用マニュアルを作成し、適正な運用を推進するとともに、定期的に監査を行うものとする。

８．責任

情報の管理責任については、情報を取扱う部署等において負うものとする。