東京医科大学の各病院における医療情報の管理に関する規程

平成19年11月13日制定

（目的）

第1条　この規程は、学校法人東京医科大学個人情報保護に関する規程により、適正な取扱いが図られるよう定められているが、東京医科大学病院・霞ヶ浦病院・八王子医療センター（以下「各病院」という。）における診療、教育、研究については、患者の個人の情報そのものであることから、個人情報について、分類を定義し、管理の原則を具体的に定めるものである。

この規程の目的は、本学の運営のために各病院が保持する医療情報に係る情報セキュリティー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ーに対する加害行為を阻止することであり、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、適正な取扱いを図らなければならない。

（定義）

第2条　この規程における用語の定義は以下のとおりとする。

(1)　個人情報

各病院において診療・研究・教育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・医学に係る情報をいう。

(2)　院内ＬＡＮネットワーク

各病院の診療業務を目的として病院敷地内に敷設されたプライベートネットワークをいう。

(3)　学内ＬＡＮネットワーク

各キャンパス間をネットワークで結び、さらに外部とインターネット網を通じて接続され、広く情報共有・交換を目的としたネットワークをいう。

(4)　閉じたネットワーク

第2条第1項第2号、第3号に該当しないネットワークであって、利用目的、利用範囲等の規則が定められ、適正に管理されたネットワークをいう。

(5)　ＰＣ等

一般に使用されているパーソナルコンピュータ（ＰＣ:Personal Computer）が、その代表であり、用途（例：サーバー）、形状（例：ＰＤＡ）を問わず、データを保管・加工・表示できる情報機器をいう。

(6)　記憶メディア等

ＵＳＢメモリー等可搬型記憶メディアをいう。

（対象者）

第３条　この規程の対象者は、前条第１項第１号に示す医療情報を取扱う者すべてとし、学校法人東京医科大学に所属するか否か、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。

（情報の分類）

第４条　この実施手順における情報の分類については、次のとおりとする。

(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（個人識別不能）

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、第４条第１項第４号として取扱うものとする。

(3)　連結可能匿名化個人情報（個人識別可能）

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持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)　特別な取扱いが必要な情報

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、特別な取扱いが求められている情報。

２　「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）でもあるので、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、この規程においては、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。

（情報の取扱い）

第5条　情報は次のとおり取扱う。

(1)　情報の分類化と見直し

情報の取扱いに際しては、まず当該情報を前条第1項に掲げる分類に慎重に分類し、第5条第1項第3号から第8号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、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）及び「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）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

一般的な医療情報として取扱うものとする。必要に応じて作成・保存・公開が可能であるが、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

一般的な医療情報としての取扱いが可能であるが、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、第5条第1項第6号に準じて取扱うこと。必要に応じて作成・保存・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、一般的な医療情報としての取扱いが可能であるが、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、第5条第1項第6号に準じて取扱うものとし、作成・保存は可能だが公開は原則不可とする。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、ＰＣ等、ネットワーク又は各種メディア等の物理的に別れているか否か、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。

(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、速やかに廃棄を行うこと。

(7)　特別な取扱いが必要な情報

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い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。

(8)　データの型式による具体的な取扱い

第５条第１項第４号、第５号に該当する情報の具体的な取扱いは以下のとおりとする。

ａ．テキストデータ

- 患者名・ＩＤ番号は削除する。
- ＩＤ等の数値に一定の関数で変換させたものでは、削除したことにならない。
- 年齢については、〇〇年代とする。
- 日付は平成〇年〇月〇日という、期日が確定されるものは削除し、なるべく日数、たとえば症状出現後〇日や入院後〇病日という表現を用いる。

ｂ．画像データ

- 個人が特定できないような手段を講じる。
- 必要以外の部位は削除する。
- 顔では、目の部分にマスキングをかけるなどし、個人が特定されないようにする（マスキングでは削除部分が容易に元に戻せないように、対応した画像を一度別ファイルに保存しなおしてから再度貼り付ける等の対応が必要）。
- ＣＴ等では、画像周辺の患者病院情報を削除する。

（ＰＣ等・記憶メディア等の取扱い）

第６条　ＰＣ等・記憶メディア等の取扱いについては、次のとおりとする。

(1)　ＰＣ等のセキュリティー

ａ．リアルタイム検索が可能なウイルス対策ソフトが導入され、常に最新のウイルス定

義ファイルに更新されていること。

b．ファイル交換ソフトがインストールされていないこと。

c．盗難防止チェーンがついていること。

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ーレベル化

① ノートＰＣ

・第６条第１項第１号に準じること。

・ログイン時のパスワードが設定されていること。

・（内蔵）ハードディスクに個人情報を保存する場合はデータを暗号化すること。

② 連結不能匿名化情報

学内ＬＡＮネットワークに接続されたＰＣ等に作成・保存が可能だが以下の対策を講じること。

・ＯＳ及びアプリケーションプログラムセキュリティーの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。

・保存するデータについては暗号化すること。

③ 連結可能匿名化個人情報

スタンドアロン又は閉じたネットワークに接続されたＰＣ等に作成・保存が可能だが以下の対策を講じること。

・ログイン中のＰＣを第三者に使用されないよう、スクリーンセイバーを解除するパスワードを設定する。若しくは同等以上の機能を有する保安対策を講じること。

・画像の保存を除いて暗号化すること。

・画像を保存し、サムネイル参照が必要な場合は、暗号化をすることで機能が制限されることから、物理的な保安対策を講じること。

・例）施錠できる閉鎖区域に設置

(2) 記憶メディア等

・個人情報は、一時的な情報の移動を目的として保存する場合を除き記憶メディア等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、記憶メディア等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。

(3)　電子メール

・連結不能匿名化情報のみ取扱い可能とし、第6条第1項第1号②に準拠すること。

(4)　ＰＣ等・記憶メディア等の破棄

・ＰＣ等内のハードディスクについては完全消去を行うソフトウェアにて消去を行うこと。また起動が困難な場合はハードディスクの物理的破壊を行うこと。

・記憶メディア等についてはメディアシュレッダー等で完全廃棄すること。

（外部への持出し）

第7条　個人情報の施設外への持出しは、紛失・盗難のリスクが格段に高くなることから以下の対策を講じること。

・持出し可能なデータは連結不能匿名化情報のみとし、ＰＣは第6条第1項第1号②、各種メディアは第6条第1項第2号に準拠すること。

・持出しデータは必要最低限の範囲に留めること。

・運搬・保管については最善の注意を払うこと。

・作業が終了したなど不要になった時点で速やかに処分するか施設内の所定の場所に保管すること。

（実施手順の運用と監査）

第8条　この規程の適正な運用のため、所属長は、この規程にそって業務マニュアル等を整備し、教職員採用時研修、教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よう努めなければならない。

附　則

この規程は、平成19年11月13日から施行する。