●●●●年●月●日

難病等データの利用に当たっての運用管理規程

●●大学●●部●●研究室

１．基本方針と管理目的

本運用管理規程は、●●大学における臨床研究の発展を推進するとともに研究成果の社会還元に寄与するため、●●大学●●部●●研究室の運用において、情報資産のセキュリティ対策に必要な事項を定める。特に本運用管理規程は、情報資産毎のリスク分析を踏まえたセキュリティ対策を担保するための運用管理規程である。本規程を基準にPDCAサイクルを回し、情報漏えい防止を適切に行う。厚生労働省から提供を受けた難病データの取扱者が、本学にて策定・公開している個人情報保護に関する基本方針、個人情報を取り扱う情報システムの安全管理に関する方針に基づき、個人情報保護と情報セキュリティの観点から遵守すべき事項を規定するものである。

２．適用範囲

厚生労働省から提供を受けた難病等データ、及びそれから派生する全ての生成物に携わる業務、部局、情報技術等に適用するものとする。

３．運用管理

（１）取扱者

* 提供申出者及び取扱者は、以下のいずれにも該当しないものである。
	1. 難病法、児童福祉法、統計法、個人情報の保護に関する法律に基づく命令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から起算して５年を経過しない者
	2. 難病等データや「指定難病患者データ及び小児慢性特定疾病児童等データの提供に関するガイドライン」に基づき提供されたデータ、高齢者の医療の確保に関する法律第 16 条の２第１項に規定する匿名医療保険等関連情報、高齢者の医療の確保に関する法律施行規則第５条の８に規定する匿名医療保険等関連情報と連結解析可能なデータ、統計法に基づくデータの利用の契約に違反し、データ提供禁止等の措置が講じられている者
	3. 暴力団員による不当な行為の防止等に関する法律（平成３年法律第 77 号）に規定する暴力団員又は暴力団員でなくなった日から５年を経過しない者（以下「暴力団員等」という。）
	4. 法人等であって、その役員のうちに上記ⅰ）からⅲ）までのいずれかに該当する者がある者
	5. 暴力団員等がその事業活動を支配する者又は当該業務の補助者として使用するおそれのある者
	6. その他、難病等データを利用して不適切な行為をしたことがある等で取扱者になることが不適切であると厚生労働省が認めた者
* 難病等データの取扱者は、予め厚生労働省に申出を行い厚生労働大臣に承諾された者のみに限られ、その他の者は難病等データにアクセスしてはならない。
* 難病等データの取扱者は、取扱者以外の者への難病等データ譲渡、貸与または他の情報との交換等をしてはならない。

（２）管理責任者

* 管理責任者は、取扱者のうち難病等データの運用管理を担う責任者である。日常的なシステムの安全管理や、安全管理に必要な資料の作成や報告を行い、これらの安全管理に係る業務に必要な承認権限等を有する。取扱者の●●●●がこれを担う。
* 難病等データを用いた研究・業務を外部委託するとき、管理責任者は当該委託を受けた者が講ずる安全管理措置について、適切に確認及び監督を行う。

（３）文書管理について

* 提供申出手続きの際に発生する文書等は、管理責任者が必要に応じて速やかに確認できる状態で管理する。
* 難病等データの安全管理のため、以下の管理台帳を作成、運用、整備を行う。改変防止のためボールペンによる記録とする。
	+ 保管場所入退室管理台帳
		- 毎月●●大学●●課より入退出記録を取得
	+ 利用場所入退室管理台帳（附表1）
	+ 解析端末利用管理台帳
		- 毎月、解析端末のアクセスログおよび操作ログを取得
	+ 公表物確認用PC利用管理台帳（附表2）
	+ 記憶媒体利用管理台帳（附表3）
	+ 作成帳票管理台帳（附表4）
* 各管理台帳は難病等データ利用終了後、１年間保管する。
* やむを得ない事情（プログラムの異常等で、保存データを救済する必要があるとき等）で外部の保守要員が難病等データを使用・保存する情報機器にアクセスする場合には、秘密保持の対策として罰則のある就業規則等で裏づけられた守秘契約を行い、厚生労働省に契約書等を提出する。

（４）利用・保管場所への立入り制限

* 利用場所は●●大学　XXX棟　X階 XXX号室　●●研究室（以下、研究室）
* 保管場所は●●大学　XXX棟　X階 XXX号室　●●サーバー室（以下、サーバ室）
* ●●大学　XXX棟については、●●大学が別途、定めているセキュリティ対策に則り、●●大学●●課による入退室管理を行い、権限のない者の入室を認めない。
* サーバ室については、●●大学が別途、定めているセキュリティ対策に則り、●●大学●●課による入退室管理を行い、権限のない者の入室を認めない。
* 研究室については、難病等データの取扱者のみが入室できることとする。
* 研究室は入退室管理を行い、入室した者の氏名、入退室した時刻、施錠・開錠時刻を利用場所入退室管理台帳に記録し、最後に退室する者が必ず研究室に施錠を行うこととする。
* 清掃等で一時的に取扱者以外の者が立ち入る必要がある場合には、難病等データを取り扱う端末からサインアウトし、取扱者の付き添いのもと、情報の漏洩や窃視の可能性を排除する。

（５）提供データの管理

* 提供データの利用、管理及び保管は、サーバ室でのみ行う。
* サーバは外部ネットワーク（インターネット、学内LAN、院内LAN等）へは接続しない閉域環境で使用する。
* サーバはラックに格納し、施錠管理する。
* サーバには取扱者のみがアクセス可能とし、Admin権限は取扱者の●●●●が保持する。
* 提供データは厚生労働省より提供を受けた難病等データ保存媒体からサーバに複写し、研究終了時までサーバ内で管理する。
* 難病等データ保存媒体の保管場所は、サーバ室の戸棚に保管し、施錠する。

（６）中間生成物の管理

* サーバ室から研究室へデータを運搬する場合を除き、中間生成物の利用、管理及び保管は、研究室でのみ行う。
* サーバから切出したデータを解析端末に複写し、研究終了時まで利用、管理および保管する。
* 研究中に生成した中間生成物は必要に応じて記憶媒体へ記録する。
* 研究中に生成した中間生成物は、ネットワークに繋がっていないローカル接続プリンターでのみ印刷する。

（７）最終生成物の管理

* 最終生成物の利用および管理は、研究室および公表物確認用PCでのみ行う。
* 最終生成物の保管は、研究室でのみ行う。
* 研究中に生成した最終生成物は必要に応じて記憶媒体へ記録する。
* 研究中に生成した最終生成物は必要に応じて印刷する。
* 作成した最終生成物は、公表審査依頼の時のみ利用保管場所より持ち出すことを認める。
* 公表審査依頼の完了後、速やかに公表物確認用PCから最終生成物を削除する。

（８）利用端末の管理

* 利用端末の利用、管理及び保管は、研究室でのみ行う。
* 利用端末へのアクセス時には、取扱者の識別と認証にIDおよびパスワードを設定する。
* IDおよびパスワードは取扱者個々人で管理し、他者への譲渡又は貸与は認めない。
* パスワードは８文字以上の英数字、記号を混在させた推定困難な文字列とする。
* パスワードは２ヶ月ごとに変更する。
* システム内のパスワードは暗号化された状態で管理・運用する。
* パスワード忘れ等で取扱者本人以外がパスワードを変更する場合には、当該取扱者の本人確認後に記録を残す。
* 設定ファイルにパスワードが記載される等、取扱者のパスワードを推定できる措置は認めない。
* 利用端末にはパスワード付のスクリーンセーバーを●●分以内に設定する。
* 利用端末にはウィルス対策ソフト(Kaspersky)を導入する。
* 初回データ利用開始前には、全ての利用端末で最新のパターンファイルにてウイルスチェックを実施する。
* ウイルス対策ソフトの保守(ウイルス定義ファイル更新、バージョンアップ等)の際は、公表物確認用PCから記憶媒体に保守ファイルを格納し、解析端末へ移行後に保守を実施する。
* 難病等データを利用中の画面を撮影、録画、スクリーンショットすることは認めない。
* 解析端末は外部ネットワーク（インターネット、学内LAN、院内LAN等）へは接続しない。
* 解析端末には盗難防止用チェーンを設置する。
* 解析端末はアクセス記録を備えたものを使用し、アクセスの記録及び定期的なログの確認を行う。
* 解析端末のログへは取扱者の●●●●のみがアクセスできるよう制限をかける。
* 公表物確認用PCは、利用時以外(離席時を含む)は研究室の戸棚に保管し、施錠する。
* 公表物確認用PCを利用する際は、利用前に最新のパターンファイルにてウィルスチェックを実施する。
* 公表物確認用PCは最終生成物のみ扱い、公表審査依頼の完了後速やかに最終生成物を削除する。
* 公表物確認用PCは、ボールペンによる手書きの操作端末利用管理台帳にてアクセスの記録及び定期的なログの確認を行う。
* 操作端末利用管理台帳には氏名、操作日時、作業内容を記録し、取扱者の●●●●が妥当性を確認する。

（９）記憶媒体および印刷物の管理

* 研究で使用する記憶媒体および印刷物は、利用・保管場所以外では使用しない。
* 研究で使用する記憶媒体および印刷物は、利用時以外(離席時を含む)は研究室の戸棚に保管し、施錠する。
* 研究で使用する全ての記憶媒体は、利用前に最新のパターンファイルにてウィルスチェックを実施する。
* 研究で使用する全ての記憶媒体は、暗号化とパスワード保護を設定する。
* 研究で使用する全ての記憶媒体は、利用後速やかにデータを削除する。
* 研究で使用する全ての記憶媒体は媒体利用管理台帳にて管理し、それ以外の記憶媒体の利用は認めない。
* 研究で使用する印刷物は１枚毎に番号を振り、作成帳票管理台帳にて管理する。

（１０）データ混同防止について

* 研究室は申出番号AXXXX-XX-XXと同じ利用場所である。
* 両研究の取扱者が混在しないよう、研究ごとに居室の利用時間帯を分ける。
* 利用データが取扱者以外の視野に入らないよう、パーティションを設置する(パーティション配置図は別途提出)
* 申出番号AXXXX-XX-XXの研究とは端末および記憶媒体を共有しない。
* 記憶媒体および印刷物を保管する棚は分別し、取扱者のみが利用できる状態とする。

（１１）データの持ち出しについて

* 公表審査を通過した成果物以外は、承諾された利用・保管場所から持ち出してはならない。
* 持ち出しが許可されるのは、サーバ室から研究室へのデータ移行、外部委託先へのデータ授受および公表審査依頼時のみとする。
* サーバ室から研究室へのデータを移行する際は、暗号化機能付き外付けHDDを使用しパスワードを設定する。
* サーバからのデータを解析端末へ移行した後、速やかに暗号化機能付き外付けHDDのデータを削除する。
* 外部委託先とのデータ授受はセキュリティ便および手渡しで実施する。
* 手渡しでデータ授受を行う場合は、暗号化機能付き外付けHDDを使用しパスワードを設定する。
* 手渡しでデータ授受を行う場合は、移行用データを格納した外付けHDD専用の施錠できるボディバッグを使用し、データ授受のみを目的とする。
* 公表審査依頼の際は、最終生成物をZIPファイル化し担当者が公表物確認用PCにてメールを送信する。
* 公表審査依頼後、速やかに公表物確認用PCおよび記憶媒体のデータを削除する。

（１２）情報セキュリティ事故発生時の対応

* 取扱者は、情報セキュリティ事故が発生又は発生したと思料する事象を発見した場合には、原因の特定、被害拡大の防止、証拠保全等必要な措置を講ずるとともに、速やかに厚生労働省に報告する。

（１３）データの廃棄

* 難病等データの利用後は、厚生労働省から提供を受けた保存媒体をセキュリティ便または手渡しにて返却する。
* 研究で使用したサーバおよび全ての記憶媒体に保存された、提供データおよび生成物（成果物を除く）は専用のデータ消去ソフトにより消去する。
* 研究で使用した印刷物については、成果物を除いて全てシュレッダーにより廃棄する。
* 利用場所ごとのデータ措置報告書に消去を実施した証明書を添付した上で、厚生労働省に提出する。
* 情報処理機器自体を破棄する場合、機器に残存した読み出し可能な情報がないことを確認する。
* 情報の破棄を外部事業者に委託した場合は、確実に情報が破棄されたことを、証憑または事業者の説明により確認する。
* データ消去後に当該機器を外部ネットワークに接続する際には、あらかじめコンピューターウイルス等の有害ソフトウェアが無いか検索し、IPS機能のあるファイアウォールを導入する。

（１４）機器の保守

* 難病等データの利用期間中に、サーバ及び端末の保守を行う場合には、保守を行う者と保守契約を締結し、機密保持の義務を課す。
* 保守はオンサイトで実施し、サーバ室又は研究室内で行う。
* 保守作業には管理責任者が立ち会う。

（１５）緊急時の事業継続等

* 大規模災害等の不測の事態により、難病等データの紛失、漏えい等があった場合には速やかに厚生労働省へ連絡し、事後の対応を協議する。
* 予期せぬデータの滅失による研究事業の遅滞、中断等の事態を避けるため、中間生成物については、定期的にバックアップをとり、外付けＨＤＤに保存する。

４．内部監査

本規程に定める運用が適切に行われているか確認することを目的として、「難病等データの利用に当たっての内部監査（自己点検）規程」を作成する。この規程に基づき、内部監査（自己点検）を実施する。

厚生労働省から管理状況報告書の提出を求められた場合には、速やかに当該内部監査（自己点検）規程に従った監査を行い、その結果を厚生労働省へ報告する。

５．外部からの問い合わせ

難病等データの利用にあたっては、国民の理解を得ることが重要であるため、当該利用について外部から問い合わせがあった場合には、原則として管理責任者が対応することとする。

付表１

利用場所入退室管理台帳

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | 日付 | 入室時間 | 退室時間 | 氏名 |  解錠/施錠 |
|  | /　/ | ： | ： |  | □解錠□施錠 |
|  | /　/ | ： | ： |  | □解錠□施錠 |
|  | /　/ | ： | ： |  | □解錠□施錠 |
|  | /　/ | ： | ： |  | □解錠□施錠 |

（適宜、行を追加して使用）

付表２

操作端末利用管理台帳

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| No | 日付 | 利用開始時間 | 利用終了時間 | 氏名 | 管理番号 | 作業内容等 |
|  | /　/ | ： | ： |  |  |  |
|  | /　/ | ： | ： |  |  |  |
|  | /　/ | ： | ： |  |  |  |
|  | /　/ | ： | ： |  |  |  |

（適宜、行を追加して使用）

付表３

記憶媒体利用管理台帳

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | 書込日付 | 削除日付 | 氏名 | 管理番号 | 備考(用途、持出の有無、格納した中間生成物等) |
|  | /　/ | /　/ |  |  |  |
|  | /　/ | /　/ |  |  |  |
|  | /　/ | /　/ |  |  |  |
|  | /　/ | /　/ |  |  |  |

（適宜、行を追加して使用）

付表４

作成帳票管理台帳

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | 作成日付 | 作成者氏名 | 破棄日付 | 破棄者氏名 | 備考（帳票名等） |
|  | /　/ |  | /　/ |  |  |
|  | /　/ |  | /　/ |  |  |
|  | /　/ |  | /　/ |  |  |
|  | /　/ |  | /　/ |  |  |

（適宜、行を追加して使用）