長崎国際大学薬学部医療情報学研究室個人錠情報取り扱いマニュアル

令和２年６月１日

1.基本方針

長崎国際大学薬学部医療情報学研究室（以下「本研究室」という。）において，人を対象とした臨床研究での研究対象者（以下「研究対象者」という。）の個人情報を利用して研究を実施する教員・学生・共同研究者等（以下「研究者」）は，「長崎国際大学薬学部医療情報学研究室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」）を遵守する。
本研究室では，この目的を果たすため，「長崎国際大学薬学部医療情報学研究室個人錠情報取り扱いマニュアル」（以下「マニュアル」）を策定する。
本研究室で研究を行うすべての者が，情報セキュリティポリシーの実施に責任を負うとともに，情報セキュリティポリシー及びマニュアルを尊重し，遵守しなければならない。

2.情報の分類と管理

情報システム内の情報は，情報セキュリティ責任者が管理責任を有する。
また，情報を利用する者は，情報の分類に従い，自己責任において適切に管理・利用する責任を有する。
これらは，情報が複製又は伝送された場合の当該複製等も対象である。

2.1.情報の分類

本研究室内の全ての情報は情報重要性分類に従い取り扱う。
情報の分類は情報セキュリティポリシーに従い，情報セキュリティ責任者が分類する。

2.1.1 重要性分類の定義と例

重要性分類４　業務上必要とする最小限の者のみが扱う情報（極秘の情報を含む。）
例：研究対象者のゲノム情報

重要性分類３　公開することを予定していない情報（秘の情報を含む。）
例：研究対象者の要配慮個人情報（本人の人種，信条，社会的身分，病歴，犯罪の経歴，犯罪により害を被った事実その他本人に対する不当な差別，偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報）

重要性分類２　外部に公開する情報のうち業務上重要な情報
例：重要性分類 4 または 3 に該当する情報について個人を特定できないよう匿名化の加工を施した医療情報

重要性分類１　上記以外の情報

2.1.2.分類の手順：

①　研究対象の医療情報を入手したすべての研究者は，その研究情報の重要性分類を把握

し，当該研究の研究責任者に遅滞なく報告する。

② 報告を受けた研究者責任者は，重要性分類の適切性を確認後，その分類と，当該医療情報を利用する研究の計画について，情報セキュリティ責任者に遅滞なく報告する。

③ 報告を受けた情報セキュリティ責任者は，報告された重要性分類に誤りがないか確認し，当該情報の重要性分類を決定するとともに，その情報に対する各研究者のアクセス権限を決定する。

④ 情報セキュリティ責任者は，情報内容の概要，情報の利用目的，分類，アクセス権限の情報，暗号化の指示等を帳簿（電磁的記録も可）に記録するとともに，当該情報を取り扱う研究の研究責任者に通知する。

⑤ 研究責任者は当該情報の管理内容について，研究者へ通知する。

2.2.情報の管理

2.2.1　情報の分類の表示

・研究責任者は，情報の分類の表示については，第三者が重要性の識別を容易に認識できないよう，適切な管理を行う。

2.2.2　情報の管理及び取扱い

・重要度分類 4 の情報：

電子データファイルにパスワードを設定するとともに，暗号化ソフトウエアを用い，ファイル自体を暗号化し，容易にそれとわからないようにした上で，研究ブース内の盗難防止策を講じた端末に保存する。印刷物は許可された者のみで閲覧し，閲覧後速やかにシュレッダー等で判別不能な状態にして廃棄する。外部への持ち出しは原則禁止。

・重要度分類 3 の情報：

電子データファイルにパスワードを設定した上で，研究ブース内の盗難防止策を講じた端末に保存する。印刷物は許可された者のみで閲覧し，閲覧後速やかにシュレッダー等で判別不能な状態にして廃棄する。外部への持ち出しは原則禁止。

・重要度分類 2 の情報：

重要度分類 3 以上の情報に加工を施した際に利用した変換テーブル等は当該ファイルとは別に保管する。電子データファイルはパスワードを設定することが望ましい。

・研究責任者は，以下の場合は，情報セキュリティ責任者の許可を得る。

重要性分類 3 以上の情報を複製する場合，個人情報の利用目的を変更/追加する場合，やむを得ず加工せずに外部に持ち出す必要が生じた場合（原則禁止），重要性分類 3 以上を記録した記録媒体を廃棄する場合

・情報セキュリティ責任者は、外部持ち出しの運用について、「長崎国際大学薬学部医療情報学研究室における個人を特定できる情報を含む医療情報等の外部持ち出しに関する申合せ」に従う。

・研究責任者は，当該研究での医療情報の取り扱いについて，すべての研究者が情報セキュ

リティポリシー及びマニュアルに従うよう，指導し，管理する。

3.研究ブースの管理

システム管理者は，以下の項目を実施しなければならない。

3.1. サーバの管理

・重要性分類 3 以上の情報を取り扱う基幹的なサーバを設置するための「研究ブース」を設置し，管理する。

3.2. 研究ブースの設置と管理

・外部からの不正な侵入に備え，研究ブースに施錠装置等を設置し，必要に応じて警報装置，監視設備等を設置する。

・厚生労働省のレセプト情報・特定健診等情報データベース（NDB）から提供を受けた情報を取り扱う研究ブース（以下，「特別研究ブース)）は，他の研究を取り扱うための研究ブースと共有しない。

例）特別研究ブース（NDB 研究のための研究ブース）：

施錠管理した研究室内に別途設けられた特定の区域

研究ブース（重要性分類 3 以上のデータを取扱うための研究ブース）：

施錠管理した研究室内

3.3. 入退室の管理

・特別研究ブースに関しては別途定める。

・研究ブースに入室できる権限を有する者は，本学の教職員，本研究室の学生，本研究室研究の共同研究者とする。それ以外の部外者が入室する際には，用件を確認し，本学の教職員の立会い等を行う。

・研究ブース及び保管施設の入退室の管理について，必要があると認める時は，入室に係る認証機能を設定する。その際，パスワード等の漏洩防止のために，パスワード等を適切に管理する。

4.研究者に関する管理

・情報セキュリティ責任者は，研究者の研究室配属時又は共同研究開始時にポリシーのうち守るべき内容を理解させ，「長崎国際大学薬学部医療情報学研究室における個人情報保護に関する誓約書の取扱要項」に従い，本人の同意を得た上で，実施及び遵守させる。

5.技術的セキュリティ

5.1.端末管理

・情報セキュリティ責任者は，研究ブース内に重要性分類 3 以上を取扱う端末（以下「特定端末」）を設置する。

・特定端末への各ユーザのログインは，ローカルパワーユーザとする。

・特定端末の，本来用途以外の使用を禁止する。
・特定端末には，ウィルス対策ソフトを導入する。

5.2.ネットワーク接続

・特定端末は特に必要でない限りはネットワークへ接続しない。
・特定端末をネットワークに接続する際には，事前に情報セキュリティ責任者に申請し承認を得る。
・接続が許可された場合は，ウィルス対策ソフトを導入し，パターンファイルを最新にアップデートする。

5.3.利用者管理

・特定端末の利用者管理は，研究責任者が行う。
・特定端末のユーザ認証は，ユーザ ID＋パスワードで行う。
・他人のユーザ ID の利用は厳禁とし，不正運用発覚時はユーザ ID の停止及び罰則の対象となり得る。
・期間が設定された利用者（有期雇用採用者等）及び利用期間が明確な利用者の場合は，必ず利用期間制限を行う。
・一旦登録した利用者が，再就職ないし休職からの復帰の際は，以前と同じユーザ ID を利用する。

6.管理状況の報告と確認

・情報セキュリティ責任者は，毎年 4 月及び研究終了時に研究責任者に対して，前回確認後の管理状況について書面で報告させる。
・情報セキュリティ責任者は，毎年 4 月にシステム管理者に対して，前年度の管理状況について書面で報告させる。
・情報セキュリティ責任者は管理状況確認書類を報告から 5 年間保管する（電磁的記録も可)。

7.相談窓口の設置

・研究責任者は、情報セキュリティに関する相談窓口を設置する。
・相談窓口は必要に応じホームページ等で公開する。

附　則

この規定は令和２年７月１日から施行する。