個人情報と研究データの取り扱いについて

（１）　研究者は、研究の実施に伴って取得された個人情報等であって当該研究者の所属する研究機関が保有しているものについて、漏えい、滅失又はき損の防止その他の安全管理のため、適切に取り扱わなければならない。
安全管理には物理的安全管理（入室管理，盗難管理など）、技術的安全管理（個人情報とそれを扱うシステムへのアクセス制御、不正アクセス防止など）を含む。

（２）　研究責任者は、研究の実施に際して、保有する個人情報等が適切に取り扱われるよう、学長と協力しつつ、当該情報を取り扱う他の研究者等に対して、必要な指導・管理を行わなければならない。

（３）　学長は、保有する個人情報等の漏えい、滅失又はき損の防止その他保有する個人情報等の安全管理のため、必要かつ適切な措置を講じなければならない。

（４）　学長は、当該研究機関において研究の実施に携わる研究者等に保有する個人情報等を取り扱わせようとする場合には、その安全管理に必要な体制及び規程を整備するとともに、研究者等に対して、保有する個人情報等の安全管理が図られるよう必要かつ適切な監督を行わなければならない。

（５）　研究者（研究責任者）は、個人情報保護のため情報・試料は可能な限り ID などをつけ、できる限り早い時期に匿名化する。匿名化された情報と対応表は別の場所で保管する。

（６）　対応表は、西南女学院大学保健福祉学部長室で管理し、庶務課長を管理者とする。研究責任者・分担者がこれらの情報を必要とする場合は管理者の許可のもと室内で閲覧する。退出時には施錠を行う。鍵の管理は庶務課が行う。

（７）　研究者（研究責任者）は、個人情報をパソコンで操作する場合（対応表の作成も含む）は、インターネットに接続しない状態でパソコンを用い、パソコン外の記録媒体（ハードディスク、USBメモリなど）に保存された電子ファイル化した個人情報を処理する。この場合、パソコン外の記録媒体を使用しない時は、施錠可能な棚に保管し、施錠を行う。
インターネットに接続することがないパソコンを用いる場合は、パソコン本体にユーザーID とパスワードを設定、研究責任者・分担者以外が使用できないようにし、使用しない時は、施錠可能な棚に保管し、施錠を行う。
なお、電子ファイル化した対応表は（６）の規定に従う。

（８）　研究者（研究責任者）は、個人情報を電子ファイルにて保存する場合は、暗号化しパスワードを設定する。なお、USBメモリを使用する場合は、アンチウイルス機能のついたものを利用し、USBメモリ自体にパスワードをかける。
なお、対応表と研究データとは別の施錠可能な棚に保管し施錠を行う。西南女学院大学保健福祉学部長室の施錠可能な棚に保管し、施錠を行う。

（９）　研究者（研究責任者）は、電子ファイルの破棄を行う際に専用のソフトウェア等により復元不可能な状態にしなければならない。紙媒体の情報はシュレッダーによる裁断、あるいは専門業者による溶解によることとする。

（１０） 研究者（研究責任者）は、個人情報を含む研究データを業者や学生が扱う場合、委託契約あるいは雇用契約において守秘義務を明示しなければならない。また、研究参加者へのインフォームド・コンセントに際して、その旨を明示する。

（１１） 人体から取得された血液、組織等や装置の破棄は適切な方法で行う。

（１２） 個人情報の漏洩、滅失、毀損が生じた場合は、学長に遅滞なく報告する。

以　上

（1）（2）（3）（4）関連の根拠：

「人を対象とする医学系研究に関する倫理指針」に示されている。

ガイドラインに下記の説明がある。

2(1)の「保有する個人情報等の安全管理のため、必要かつ適切な措置」に関して、保有 する個人情報等の性質に応じて、研究機関の長の責任の下、以下に掲げる物理的及び技術 的安全管理措置を適宜選択して実施するものとする。安全管理のための措置の手法の具体 例については、「個情法ガイドライン(通則編)」の「(別添)講ずべき安全管理措置の 内容」、「行政機関の保有する個人情報の適切な管理のための措置に関する指針」及び「独 立行政法人等の保有する個人情報の適切な管理のための措置に関する指針」等の関連する指針を参照のこと。

○「物理的安全管理」とは、入館(室)管理、保有する個人情報等の盗難の防止等の措置を指し、以下の事項が含まれる。

1 個人データを取り扱う区域の管理入退館(室)管理の実施

2 機器及び電子媒体等の盗難等の防止

3 電子媒体等を持ち運ぶ場合の漏えい等の防止

4 個人データの削除及び機器、電子媒体等の廃棄

○ 「技術的安全管理」とは、保有する個人情報等及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、保有する個人情報等 に対する技術的な安全管理措置を指し、以下の事項が含まれる。

1 アクセス制御(アクセス権限の管理、アクセス記録等)

2 アクセス者の識別と認証

3 外部からの不正アクセス等の防止(不正ソフトウェア対策等)

4 情報システムの使用に伴う漏えい等の防止(移送・通信時の対策、動作確認時の対策、情報システムの監視等)

（5）対応表の管理者を庶務課長とする根拠

学校法人西南女学院個人情報の保護に関する規則

第４条 本学院は、第1条の目的を達成するため、学校法人西南女学院における個人情報の保護に関する統括管理責任者（以下「統括管理責任者」という。）を置き、理事長をもって充てる。

2 法人本部、大学、大学短期大学部、中学校・高等学校、幼稚園及びこれらに準ずる機関（以下「各所属」という。）ごとに個人情報の保護に関する管理者（以下「管理者」という。）を置くものとする。

大学における情報セキュリティポリシー

「情報セキュリティ対策基準」

（4） 情報資産管理責任者：学科長、別科長、課長

・情報セキュリティの適正な運用及び管理を行うため、情報資産を取り扱う学科・別科・課（これに準ずるものを含む）に情報セキュリティに関する権限及び責任を有する情報資産管理責任者を置き、情報資産を取り扱う学科・別科・課の代表者をもってこれに充てる。
・情報資産管理責任者は、所轄する情報資産に係る情報セキュリティ実施手順の作成・維持・管理を行うとともに、定められている事項について教職員に実施及び遵守させなければならない。

＊　以上の規程によって，学科長，別科長，課長が管理者となり得るが，研究を行う当事者となり得る学科長，別科長は望ましくない。