大阪大学医学部附属病院の保有する個人情報の管理に関する内規

第１章　総則

（趣旨）

第１条　国立大学法人大阪大学医学部附属病院（以下「病院」という。）における個人情報の管理については、国立大学法人大阪大学の保有する個人情報の管理に関する規程又は別に定めるもののほか、この内規の定めるところによる。

第２章　安全管理措置

第１節　組織的安全管理措置

（保護管理者）

第２条　国立大学法人大阪大学の保有する個人情報の管理に関する規程国立大学法人大阪大学における個人情報の管理に関する規程第４条に基づき病院に、国立大学法人大阪大学の総括保護管理者（以下「総括保護管理者」という。）のもとに保護管理者を置き、大阪大学医学部附属病院長（以下「病院長」という。）をもって充てる。

２　保護管理者は、病院における個人情報の適切な管理を確保する。

（保護担当者）

第３条　国立大学法人大阪大学の保有する個人情報の管理に関する規程国立大学法人大阪大学における個人情報の管理に関する規程第５条に基づき病院に、医療情報担当及びその他情報担当の保護担当者を置く。

２　保護担当者（医療情報担当）は医療情報部長をもって充て、保護担当者（その他情報担当）は事務部長をもって充てる。

３　保護担当者は、保護管理者を補佐し、保護管理者が行う個人情報の管理に関する事務を担当する。

（個人情報セキュリティリーダー）

第４条　各部署でのルールの理解やその徹底のための呼びかけ、個人情報の管理状況を調査、トラブル発生時に速やかに情報共有を行うため、次のとおり個人情報セキュリティリーダーを置く。

（１）診療科、中央診療施設の各部署

（２）薬剤部、医療技術部

（３）看護部の各病棟、各外来

（４）未来医療開発部の各センター

（５）事務部の各課

（運用状況の記録）

第５条　保護担当者は、本内規に基づく運用状況を確認するため、次の各号に定める項目について利用状況等を記録し、その記録を一定期間保存し、分析するための体制を整備するものとする。

⑴　個人情報データベース等の利用・出力状況

⑵　個人情報が記載又は記録された書類・媒体等の持ち運び等の状況

⑶　個人情報データベース等の削除・廃棄の状況（委託した場合の消去・廃棄を証明する記録を含む。）

⑷　個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況（ロ

グイン実績、アクセスログ等）

（取扱状況の確認手段）

第６条　保護担当者は、個人情報の取扱状況を確認するための手段として、台帳等を整備して次の各号に定める事項を記録するものとする。

(1)　個人情報データベース等の種類、名称

(2)　個人情報の項目

(3)　責任者・取扱部署

(4)　利用目的

(5)　アクセス権を有する者

(6)　その他総括保護管理者が必要と認める事項

（情報漏えい事案への対応）

第７条　保護管理者は、個人情報の漏えい、滅失又は毀損による事故（以下「漏えい事案等」という。）が発生したことを把握した場合又はその可能性が高いと判断した場合は、適切に対処するものとする。

２　保護管理者は、総括保護管理者と連携して漏えい事案等に対処するものとする。

３　保護管理者は、漏えい事案等が発生したと判断した場合は、速やかに漏えい事案等が発生した経緯、被害状況等の調査を行い、その結果等を総括保護管理者に報告するとともに、被害の拡大防止又は復旧等のために必要な措置を講ずるものとする。

４　保護管理者は、漏えい事案等の発生した原因を分析し、再発防止のために必要な措置を講ずるものとする。

第２節　人的安全管理措置

（監督）

第８条　保護管理者は、職員等（保有個人情報を取り扱うことのある学生、本学と雇用関係にない医療従事者及び派遣労働者を含む。以下同じ。）に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該職員等に対する必要かつ適切な監督を行わなければならない。

（教育及び研修）

第９条　保護管理者は、病院の職員等に対し、個人データの適切な管理のために、国立大学法人大阪大学（以下、「本法人」という。）及び病院の実施する教育研修等への参加の機会を付与するものとする。

第３節　物理的安全管理措置

（個人データを取り扱う区域）

第１０条　病院は、個人データの情報漏えい等を防止するため、次の各号に定める区域を明確にし、それぞれ当該各号に定める措置を講ずるものとする。

(1)　管理区域

入退室管理及び管理区域へ持ち込む機器、電子媒体等の制限を行う。

(2)　取扱区域

権限を有しない者により、個人データを容易に閲覧等することを防止する。

（機器及び電子媒体等の盗難等の防止）

第１１条　病院は管理区域及び取扱区域における個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、個人データを取り扱う機器、電子媒体又は書類等を、施錠できるキャビネット又は書庫に保管するものとする。

（複製等の制限）

第１２条　保護管理者は、職員等が個人データを取り扱う場合において、その行為が次の各号に該当するときは、当該個人データの秘匿性等その内容に応じて、当該行為を行うことができる場合を限定するものとし、職員等は、当該行為を行うにあたっては、保護管理者の指示に従うものとする。

(1)　個人データの複製

(2)　個人データの送信

(3)　個人データが記録されている媒体の外部への送付又は持出し

(4)　その他個人データの適切な管理に支障を及ぼすおそれのある行為

２　前項により個人情報が記録された電子媒体又は書類等の持出しを行う場合には、法令等により別に定めがある場合を除き、次の各号に掲げる安全策を講じるものとする。

(1)　個人情報が記録された電子媒体を安全に持ち出す方法

ア　持ち出しデータの暗号化

イ　持ち出しデータのパスワードによる保護

ウ　施錠できる搬送容器の使用

エ　追跡可能な移送手段の利用

(2)　個人情報が記載された書類等を安全に持ち出す方法

封緘、目隠しシールの貼付

（個人データの削除及び機器、電子媒体等の廃棄）

第１３条　個人データが記録された電子媒体、書類等を廃棄又は削除する場合は、次の各号に掲げる措置を講ずるものとする。

(1)　個人データが記録された書類等を廃棄する場合、焼却、溶解、シュレッダーによる細断等の復元不可能な手段をとるものとする。

(2)　情報システム（パソコン等の機器を含む。）において個人データを削除する場合、容易に復元できない手段をとるものとする。

(3)　個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等により、復元不可能な手段をとるものとする。

第４節　技術的安全管理措置

（アクセス制御）

第１４条　病院は、情報システムを使用して取り扱う個人データの範囲を限定するため、個人データへのアクセス制御は次の各号に掲げる方法により適切に行うものとする。

(1)　個人データを取り扱うことのできる情報システム端末等を限定する。

(2)　各情報システムにおいて、アクセスすることのできる個人情報データベース等を限定する。

(3)　ユーザーID に付与するアクセス権により、個人データを取り扱う情報システムを使用できる者を限定する。

（アクセス者の識別と認証）

第１５条　個人データを取り扱う情報システムを使用する担当者が正当なアクセス権を有する者であることを、ユーザーID、パスワード、磁気・IC カード等の識別方法により識別した結果に基づき認証しなければならない。

（外部からのアクセス等の防止）

第１６条　病院は、次の各号に掲げる方法により、情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用するものとする。

(1)　個人データを取り扱う情報システムと外部ネットワーク（又はその他の情報システム）との接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。

(2)　情報システム及び機器に、セキュリティ対策ソフトウェア、ウイルス対策ソフトウェア等を導入し、不正ソフトウェアの有無を確認する。

(3)　機器、ソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。

(4)　定期に及び必要に応じ随時にログ等の分析を行い、不正アクセス等を検知する。

（情報システムの使用に伴う漏えい等の防止）

第１７条　病院は、個人データをインターネット等により外部に送信する場合、次の各号に掲げる方法により、通信経路における情報漏えい、情報システム内に保存されている個人データの情報漏えい等を防止するものとする。

(1)　情報システムの設計時に安全性を確保し、継続的に見直す（情報システムの脆弱性をついた攻撃への対策を講ずることも含む。）。

(2)　通信経路の暗号化

(3)　情報システムに保存されている個人データの暗号化又はパスワードによる保護

第５節　外的環境の把握

第１８条　病院が、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じなければならない。

第６節　その他

（委託先における安全管理措置）

第１９条　病院は、委託先での個人データの取得、利用、保管、提供、削除及び廃棄段階における安全管理措置について、第３節から前節までの安全管理措置と同等の措置が講じられるよう委託先に必要かつ適切な監督を行わなければならない。

第３章　職員等の責務

第２０条　職員等は、法の趣旨に則り、関連する法令及び規程等の定め並びに総括保護管理者、保護管理者及び保護担当者の指示に従い、個人情報を取り扱わなければならない。

第４章　個人データの取扱い

第１節　利用目的の特定等

（利用目的の特定）

第２１条　職員等は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。

２　職員等は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

（利用目的による制限）

第２２条　職員等は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

２　職員等は、合併その他の事由により他の個事業を承継することに伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えて、当該個人情報を取り扱ってはならない。

３　前２項の規定は、次に掲げる場合については、適用しない。

⑴　法令に基づく場合

⑵　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

⑶　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

⑷　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

⑸　当該個人情報を学術研究の用に供する目的（以下「学術研究目的」という。）で取り扱う必要があるとき（当該個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

⑹　学術研究機関等に個人データを提供する場合であって、当該学術研究機関等が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

（不適正な利用の禁止）

第２３条　職員等は、違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない。

（適正な取得）

第２４条　職員等は、偽りその他不正の手段により個人情報を取得してはならない。

２　職員等は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。

⑴　法令に基づく場合

⑵　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

⑶　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意

を得ることが困難であるとき。

(4)　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(5)　当該要配慮個人情報を学術研究目的で取り扱う必要があるとき（当該要配慮個人情報を取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

(6)　学術研究機関等から当該要配慮個人情報を取得する場合であって、当該要配慮個人情報を学術研究目的で取得する必要があるとき（当該要配慮個人情報を取得する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（本法人と当該学術研究機関等が共同して学術研究を行う場合に限る。）。

(7)　当該要配慮個人情報が、本人、国の機関、地方公共団体、学術研究機関等、法第５７条第１項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合

(8)　その他前各号に掲げる場合に準ずるものとして政令第９条で定める場合

（取得に際しての利用目的の通知等）

第２５条　保護管理者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

２　保護管理者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

３　保護管理者は、利用目的を変更した場合は、変更された利用目的について、本人に通知し、又は公表しなければならない。

４　前３項の規定は、次に掲げる場合については、適用しない。

(1)　利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

(2)　利用目的を本人に通知し、又は公表することにより病院の権利又は正当な利益を害するおそれがある場合

(3)　国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(4)　取得の状況からみて利用目的が明らかであると認められる場合

（データ内容の正確性の確保等）

第２６条　職員等は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない。

第２節　加工情報の作成等

（仮名加工情報の作成等）

第２７条　保護管理者は、仮名加工情報（仮名加工情報データベース等を構成するものに限る。以下同じ。）を作成するときは、他の情報と照合しない限り特定の個人を識別することができないようにするために必要なものとして個人情報保護委員会規則で定める基準に従い、個人情報を加工しなければならない。

２　保護管理者は、仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等（仮名加工情報の作成に用いられた個人情報から削除された記述等及び個人識別符号並びに前項の規定により行われた加工の方法に関する情報をいう。以下同じ。）を取得したときは、削除情報等の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準に従い、削除情報等の安全管理のための措置を講じなければならない。

３　保護管理者は、第２２条の規定にかかわらず、法令に基づく場合を除くほか、第２１条第１項の規定により特定された利用目的の達成に必要な範囲を超えて、仮名加工情報（個人情報であるものに限る。以下この条において同じ。）を取り扱ってはならない。

４　仮名加工情報についての第２５条の規定の適用については、同条第１項及び第３項中「、本人に通知し、又は公表し」とあるのは「公表し」と、同条第４項第１号から第３号までの規定中「本人に通知し、又は公表する」とあるのは「公表する」とする。

５　保護管理者は、仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去するよう努めなければならない。この場合においては、第２６条の規定は、適用しない。

６　保護管理者は、第３１条第１項及び第２項並びに第３２条第１項の規定にかかわらず、法令に基づく場合を除くほか、仮名加工情報である個人データを第三者に提供してはならない。この場合において、第３１条第４項中「前３項」とあるのは「第２７条第６項」と、同項第３号中「、本人に通知し、又は本人が容易に知り得る状態に置いて」とあるのは「公表して」と、同条第５項中「、本人に通知し、又は本人が容易に知り得る状態に置かなければ」とあるのは「公表しなければ」と、第３３条第１項ただし書中「第３１条第１項各号又は第４項各号のいずれか（前条第１項の規定による個人データの提供にあっては、第３１条第１項各号のいずれか）」とあり、及び第３４条第１項ただし書中「第３１条第１項各号又は第４項各号のいずれか」とあるのは「法令に基づく場合又は第３１条第４項各号のいずれか」とする。

７　保護管理者は、仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合してはならない。

８　保護管理者は、仮名加工情報を取り扱うに当たっては、電話をかけ、郵便若しくは民間事業者による信書の送達に関する法律（平成１４年法律第９９号）第２条第６項に規定する一般信書便事業者若しくは同条第９項に規定する特定信書便事業者による同条第２項に規定する信書便により送付し、電報を送達し、ファクシミリ装置若しくは電磁的方法（電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法であって個人情報保護委員会規則で定めるものをいう。）を用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用してはならない。

（仮名加工情報の第三者提供の制限等）

第２８条　保護管理者は、法令に基づく場合を除くほか、仮名加工情報（個人情報であるものを除く。次項及び第３項において同じ。）を第三者に提供してはならない。

２　第３１条第４項及び第５項の規定は、仮名加工情報の提供を受ける者について準用する。この場合において、同条第４項本文中「前３項」とあるのは「第２８条第１項」と、同項第３号中「、本人に通知し、又は本人が容易に知り得る状態に置いて」とあるのは「公表して」と、同条第５項中「、本人に通知し、又は本人が容易に知り得る状態に置かなければ」とあるのは「公表しなければ」と読み替えるものとする。

３　第２章及び第１９条で定める安全管理措置の規定は、仮名加工情報取扱事業者による仮名加工情報の取扱いについて準用する。

（行政機関等匿名加工情報等の作成及び提供等）

第２９条　病院は、行政機関等匿名加工情報（行政機関等匿名加工情報ファイルを構成するものに限る。）を作成することができる。

２　病院は、次の各号のいずれかに該当する場合を除き、行政機関等匿名加工情報を提供してはならない。

⑴　法令に基づく場合

⑵　保有個人情報を利用目的のために第三者に提供することができる場合において、当該保有個人情報を加工して作成した行政機関等匿名加工情報を当該第三者に提供するとき。

３　第３１条の規定にかかわらず、病院は、法令に基づく場合を除き、利用目的以外の目的のために削除情報（保有個人情報に該当するものに限る。）を自ら利用し、又は提供してはならない。

４　行政機関等匿名加工情報の作成及び提供等に関し、必要な事項は別に定める。

（行政機関等匿名加工情報等の従事者の義務）

第３０条　行政機関等匿名加工情報、法第１０７条第４項に規定する削除情報及び国立大学法人大阪大学における行政機関等匿名加工情報の提供等に関する規程第１１条の規定により行った加工の方法に関する情報（以下「行政機関等匿名加工情報等」という。）の取扱いに従事する病院の職員等若しくは職員等であった者、法第１１９条第３項の委託を受けた業務に従事している者若しくは従事していた者又は病院において行政機関等匿名加工情報等の取扱いに従事している派遣労働者若しくは従事していた派遣労働者は、その業務に関して知り得た行政機関等匿名加工情報等の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。

第５章　個人データの提供及び業務の委託等

（第三者提供の制限）

第３１条　職員等は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

⑴　法令に基づく場合

⑵　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

⑶　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

(4)　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(5)　当該個人データの提供が学術研究の成果の公表又は教授のためやむを得ないとき（個人の権利利益を不当に侵害するおそれがある場合を除く。）。

(6)　当該個人データを学術研究目的で提供する必要があるとき（当該個人データを提供する目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）（本法人と当該第三者が共同して学術研究を行う場合に限る。）。

(7)　当該第三者が学術研究機関等である場合であって、当該第三者が当該個人データを学術研究目的で取り扱う必要があるとき（当該個人データを取り扱う目的の一部が学術研究目的である場合を含み、個人の権利利益を不当に侵害するおそれがある場合を除く。）。

2　保護管理者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、総括保護管理者に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。ただし、第三者に提供される個人データが要配慮個人情報又は第２４条第１項の規定に違反して取得されたもの若くは他の法人等からこの項本文の規定により提供されたもの（その全部又は一部を複製し、又は加工したものを含む。）である場合は、この限りでない。

(1)　本法人の代表者である総長の氏名

(2)　第三者への提供を利用目的とすること。

(3)　第三者に提供される個人データの項目

(4)　第三者に提供される個人データの取得の方法

(5)　第三者への提供の方法

(6)　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

(7)　本人の求めを受け付ける方法

(8)　その他個人の権利利益を保護するために必要なものとして個人情報保護委員会規則で定める事項

3　保護管理者は、前項第１号に掲げる事項に変更があったとき又は同項の規定による個人データの提供をやめたときは遅滞なく、同項第３号から第５号まで、第７号又は第８号に掲げる事項を変更しようとするときはあらかじめ、その旨について、個人情報保護委員会規則で定めるところにより、総括保護管理者に届け出なければならない。

4　次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。

(1)　病院が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合

(2)　合併その他の事由による事業の承継に伴って個人データが提供される場合

(3)　特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的並びに当該個人データの管理について責任を有する者の氏名又は名称及び住所並びに法人にあっ

ては、その代表者の氏名について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

5　保護管理者は、前項第３号に規定する利用する者の利用目的又は当該責任を有する者を変更しようとするときはあらかじめ、総括保護管理者に届け出なければならない。

（外国にある第三者への提供の制限）

第３２条　保護管理者は、外国（本邦の域外にある国又は地域をいう。以下この条及び第３５条第１項第２号において同じ。）（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有している外国として個人情報保護委員会規則で定めるものを除く。以下この条及び同号において同じ。）にある第三者（個人データの取扱いについて法第４章第２節の規定により講ずべきこととされている措置に相当する措置（第３項において「相当措置」という。）を継続的に講ずるために必要なものとして個人情報保護委員会規則で定める基準に適合する体制を整備している者を除く。以下この項及び次項並びに同号において同じ。）に個人データを提供する場合には、前条第１項各号に掲げる場合を除くほか、あらかじめ外国にある第三者への提供を認める旨の本人の同意を得なければならない。この場合においては、同条の規定は、適用しない。

2　保護管理者は、前項の規定により本人の同意を得ようとする場合には、個人情報保護委員会規則で定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない。

3　保護管理者は、個人データを外国にある第三者（第１項に規定する体制を整備している者に限る。）に提供した場合には、個人情報保護委員会規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない。

（第三者提供に係る記録の作成等）

第３３条　保護管理者は、個人データを第三者（法第１６条第２項各号に掲げる者を除く。以下この条及び次条（第３５条第３項において読み替えて準用する場合を含む。）において同じ。）に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。ただし、当該個人データの提供が第３１条第１項各号又は第４項各号のいずれか（前条第１項の規定による個人データの提供にあっては、第３１条第１項各号のいずれか）に該当する場合は、この限りでない。

2　保護管理者は、前項の記録を、当該記録を作成した日から別に定める期間保存しなければならない。

（第三者提供を受ける際の確認等）

第３４条　保護管理者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第３１条第１項各号又は第４項各号のいずれかに該当する場合は、この限りでない。

(1)　当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者の氏名

(2)　当該第三者による当該個人データの取得の経緯

2　保護管理者は、第１項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところに

より、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。

３　保護管理者は、前項の記録を、当該記録を作成した日から別に定める期間保存しなければならない。

（個人関連情報の第三者提供の制限等）

第３５条　保護管理者は、第三者が個人関連情報（個人関連情報データベース等を構成するものに限る。以下同じ。）を個人データとして取得することが想定されるときは、第３１条第１項各号に掲げる場合を除くほか、次に掲げる事項について、あらかじめ個人情報保護委員会規則で定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。

⑴　当該第三者が法第１６条第７号に定める個人関連情報取扱事業者から個人関連情報の提供を受けて本人が識別される個人データとして取得することを認める旨の当該本人の同意が得られていること。

⑵　外国にある第三者への提供にあっては、前号の本人の同意を得ようとする場合において、個人情報保護委員会規則で定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報が当該本人に提供されていること。

２　第３２条第３項の規定は、前項の規定により個人関連情報取扱事業者が個人関連情報を提供する場合について準用する。この場合において、同条第３項中「講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供し」とあるのは、「講じ」と読み替えるものとする。

３　前条第２項及び第３項の規定は、第１項の規定により個人関連情報取扱事業者が確認する場合について準用する。この場合において同条第２項中「の提供を受けた」とあるのは、「を提供した」と読み替えるものとする。

（委託先の監督）

第３６条　保護管理者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

第６章　病院情報システムにおける安全の確保等

（アクセス制御）

第３７条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）の秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずる。

２　保護管理者は、前項の措置を講ずる場合には、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。

（アクセス記録）

第３８条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）の秘匿性等その内容に応じて、保有個人情報（病院情報システムで取り扱うもの）へのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期に又は随時に分析するために必要な措置を講ずる。

２　保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずる。

（外部からの不正アクセスの防止）

第３９条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）を取り扱う情報システムへの外部からの不正アクセスを防止するため、経路制御等の必要な措置を講ずる。

（コンピュータウイルスによる漏えい等の防止）

第４０条　保護管理者は、コンピュータウイルスによる保有個人情報（病院情報システムで取り扱うもの）の漏えい、滅失又はき損の防止のため、コンピュータウイルスの感染防止等に必要な措置を講ずる。

（暗号化）

第４１条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）の秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずる。

（入力情報の照合等）

第４２条　職員等は、病院情報システムで取り扱う保有個人情報（病院情報システムで取り扱うもの）の重要度に応じて、入力原票と入力内容との照合、処理前後の当該保有個人情報（病院情報システムで取り扱うもの）の内容の確認、既存の保有個人情報（病院情報システムで取り扱うもの）との照合等を行う。

（バックアップ）

第４３条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）の重要度に応じて、バックアップを作成し、分散保管するために必要な措置を講ずる。

（情報システム設計書等の管理）

第４４条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）に係る情報システムの設計書、構成図等の文書について外部に知られることがないよう、その保管、複製、廃棄等について必要な措置を講ずる。

（端末の限定）

第４５条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）の秘匿性等その内容に応じて、その処理を行う端末を限定する等の必要な措置を講ずる。

（端末の盗難防止等）

第４６条　保護管理者は、端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の措置を講ずる。

２　職員等は、保護管理者が必要と認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならない。

（第三者の閲覧防止）

第４７条　職員等は、端末の使用に当たっては、保有個人情報（病院情報システムで取り扱うもの）が第三者に閲覧されることがないよう、使用状況に応じて病院情報システムからログオフを行うことを徹底する等の措置を講ずる。

第７章　情報システム室等の安全管理

（入退室の管理）

第４８条　保護管理者は、保有個人情報（病院情報システムで取り扱うもの）を取り扱う基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）に入室する権限を有する者を定めると

ともに、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずるものとする。また、保有個人情報（病院情報システムで取り扱うもの）を記録する媒体を保管するための施設を設けている場合においても、同様の措置を講ずる。

２　保護管理者は、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずる。

３　保護管理者は、情報システム室等及び保管施設の入退室の管理について、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずる。

（情報システム室等の管理）

第４９条　保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置、監視設備の設置等の措置を講ずる。

２　保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずる。

第８章　雑則

（苦情の処理）

第５０条　保護管理者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

（死者の情報の取り扱い）

第５１条　当該患者が死亡した後においても、本院が当該患者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のため、個人情報と同等の安全管理措置を行う。

（遺伝情報に関する個人情報）

第５２条　遺伝情報に関する個人情報の本内規の適用にあたっては、特別な配慮を必要とする。

附　則

１　この内規は、令和４年７月２２日から施行し、令和４年４月１日から適用する。

２　大阪大学医学部附属病院の保有する個人情報の適切な管理に関する規程（平成１７年４月１日制定）は廃止する。