

## 熊本大学病院個人情報管理要項

〔平成17年4月1日制定  
平成31年3月13日最終改正〕

(趣旨)

第1条 この要項は、病院（以下「本院」という。）が保有する個人情報の管理に関し必要な事項を定める。

(定義)

第2条 この要項における用語の意義は、独立行政法人等の保有する個人情報の保護に関する法律（平成15年法律第59号。以下「法」という。）第2条の定めるところによる。

(保護管理者)

第3条 本院に、国立大学法人熊本大学個人情報管理規則（平成17年4月1日制定。以下「管理規則」という。）第3条に定める総括保護管理者のもとに保護管理者を置き、病院長をもって充てる。

(副保護管理者)

第4条 本院に、管理規則第6条に定める副保護管理者を置き、別表に掲げる者をもって充てる。

2 保有個人情報を病院情報管理システム等で取り扱う場合において、副保護管理者は、当該情報システムの管理者と連携して適切に管理するものとする。

(保護担当者)

第5条 本院に、管理規則第5条に定める保護担当者を置き、別表に掲げる者をもって充てる。

(職員等の責務)

第6条 職員等（保有個人情報を取り扱うことのある大学院生及び学生並びに派遣労働者を含む。以下同じ。）は、法の趣旨に則り、関連する法令及び学内規則等の定め並びに総括保護管理者、保護管理者、副保護管理者及び保護担当者の指示に従い、保有個人情報を取り扱うものとする。

(教育研修)

第7条 保護管理者は、職員等に対し、保有個人情報の適切な管理のために、総括保護管理者の実施する教育研修への参加の機会を付与する等の必要な措置を講ずる。

(アクセス制限)

第8条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報にアクセスする権限を有する職員等及び当該職員等の権限について、それらの利用目的を達成するために必要最小限の範囲に制限する。

2 アクセス権限を有しない職員等は、保有個人情報にアクセスしてはならない。

3 職員等は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスしてはならない。

(複製等の制限)

第9条 職員等が業務上の目的で保有個人情報を取り扱う場合であっても、保護管理者は、次の各号に該当する事項は、当該保有個人情報の秘匿性等その内容に応じて、当該事項を行うことができる場合を限定し、職員等は、保護管理者又は副保護管理者の指示に従い取り扱う。

- (1) 保有個人情報の複製
- (2) 保有個人情報の送信

- (3) 保有個人情報記録されている媒体の外部への送付又は持出し
- (4) その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為  
(誤りの訂正等)

第10条 職員等は、保有個人情報の内容に誤り等を発見した場合には、保護管理者又は副保護管理者の指示に従い、訂正等を行う。

(媒体の管理等)

第11条 職員等は、保護管理者の指示に従い、保有個人情報記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行う。

(廃棄等)

第12条 職員は、保有個人情報又は保有個人情報記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行う。

(保有個人情報の取扱状況の記録)

第13条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、台帳等を整備して、当該保有個人情報の利用及び保管等の取扱いの状況について記録する。

(アクセス制御)

第14条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、病院情報管理システム等についてパスワード等（パスワード、ICカード、生体情報等をいう。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を整備（その定期又は随時の見直しを含む。）するとともに、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15条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、病院情報管理システム等について当該保有個人情報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的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。

(アクセス状況の監視)

第15条の2 保護管理者は、保有個人情報の秘匿性等その内容及びその量に応じて、当該保有個人情報への不適切なアクセス監視のため、保有個人情報を含む又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合に警告表示がなされる機能の設定、当該設定の定期的確認、アクセスログの確認、操作ログの分析等の必要な措置を講ずる。

(管理者権限の設定)

第15条の3 保護管理者は、保有個人情報の秘匿性等その内容に応じて、情報システムの管理者権限の特権を不正に窃取された際の被害の最小化及び内部からの不正操作等の防止のため、当該特権を最小限とする等の必要な措置を講ずる。

(外部からの不正アクセスの防止)

第16条 保護管理者は、保有個人情報を取り扱う病院情報管理システム等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。

(不正プログラムによる漏えい等の防止)

第17条 保護管理者は、不正プログラムによる保有個人情報の漏えい、滅失又はき損の防止のため、病院情報管理システム等について、ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に必要な措置（導入したソフトウェアを常に最新の状態に保つことを含む。）を講ずる。

（病院情報管理システム等における保有個人情報の処理）

第17条の2 職員等は、保有個人情報について、一時的に加工等の処理を行うため複製等を行う場合には、その対象を必要最小限に制限し、処理終了後は不要となった情報を速やかに消去する。

2 保護管理者は、保有個人情報の秘匿性等その内容に応じて、随時、当該情報の消去等の実施状況を重点的に確認する。

（暗号化）

第18条 保護管理者は、保有個人情報の秘匿性等その内容に応じて、病院情報管理システム等についてその暗号化のために必要な措置を講ずる。

2 職員等は、その措置を踏まえ、処理する保有個人情報について、当該保有個人情報の秘匿性等その内容に応じて、適切に暗号化を行う。

（入力情報の照合等）

第19条 職員等は、病院情報管理システム等で取り扱う保有個人情報の重要度に応じて、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の内容の確認、既存の保有個人情報との照合等を行う。

（バックアップ）

第20条 保護管理者は、保有個人情報の重要度に応じて、病院情報管理システム等につい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21条 保護管理者は、保有個人情報に係る情報システムの設計書、構成図等の法人文書について外部に知られることがないように、その保管、複製、廃棄等に必要な措置を講ずる。

（端末の限定）

第22条 保護管理者は、保有個人情報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ために必要な措置を講ずる。

（端末の盗難防止等）

第23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、執務室の施錠等の必要な措置を講ずる。

2 職員等は、保護管理者が必要がある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いない。

（第三者の閲覧防止）

第24条 職員等は、端末の使用に当たっては、保有個人情報第三者に閲覧されることがないように、使用状況に応じて病院情報管理システム等からログオフを行うことを徹底する等の必要な措置を講ずる。

（記録機能を有する機器・媒体の接続制限）

第24条の2 保護管理者は、保有個人情報の秘匿性等その内容に応じて、当該保有個人情報の漏えい、滅失又は毀損の防止のため、スマートフォン、USBメモリ等の記録機能を有する機器・媒体の病院情報管理システム等端末等への接続の制限（当該機器の更新への対応を含む。）等の必要な措置を講ずる。

（入退管理）

第25条 保護管理者は、保有個人情報を取り扱う基幹的なサーバ等の機器を設置する室その他の区域（以下「情報システム室等」という。）に立ち入る権限を有する

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、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等の措置を講ずる。また、保有個人情報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、必要があると認めるときは、同様の措置を講ずる。

2 保護管理者は、必要があると認めるときは、情報システム室等の出入口の特定化による入退の管理の容易化、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の管理について、必要があると認めるときは、立ち入り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26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。

（保有個人情報の提供）

第27条 保護管理者は、国立大学法人熊本大学個人情報保護規則（平成17年4月1日制定。以下「保護規則」という。）第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、原則として、提供先における利用目的、利用する業務の根拠法令、利用する記録範囲及び記録項目、利用形態等について書面を取り交わす。

2 保護管理者は、保護規則第9条第2項第3号及び第4号の規定に基づき行政機関及び独立行政法人等以外の者に保有個人情報を提供する場合には、安全確保の措置を要求するとともに、原則として、提供前又は随時に実地の調査等を行い、措置状況を確認してその結果を記録するとともに、改善要求等の措置を講ずる。

3 保護管理者は、保護規則第9条第2項第3号の規定に基づき行政機関又は独立行政法人等に保有個人情報を提供する場合において、前2項に規定する措置を講ずる。

（業務の委託等）

第28条 保有個人情報の取扱いに係る業務を外部に委託する場合には、個人情報の適切な管理を行う能力を有しない者を選定することがないように、必要な措置を講ずる。また、契約書に、次に掲げる事項を明記するとともに、委託先における責任者及び業務従事者等の管理及び実施体制、個人情報の管理の状況についての検査に関する事項等の必要な事項について書面で確認する。

(1) 個人情報に関する秘密保持、目的外利用の禁止等の義務

(2) 再委託の制限又は事前承認等再委託に係る条件に関する事項

(3) 個人情報の複製等の制限に関する事項

(4) 個人情報の漏えい等の事案の発生時における対応に関する事項

(5) 委託終了時における個人情報の消去及び媒体の返却に関する事項

(6) 違反した場合における契約解除、損害賠償責任その他必要な事項

2 保有個人情報の取扱いに係る業務を外部に委託する場合には、委託する保有個人情報の秘匿性等その内容に応じて、委託先における個人情報の管理の状況について、年1回以上の定期的検査等により確認する。

3 委託先において、保有個人情報の取扱いに係る業務が再委託される場合には、委託先に第1項の措置を講じさせるとともに、再委託される業務に係る保有個人情報

の秘匿性等その内容に応じて、委託先を通じて又は委託元自らが前項の措置を実施する。保有個人情報の取扱いに係る業務について再委託先が再々委託を行う場合以降も同様とする。

4 保有個人情報の取扱いに係る業務を派遣労働者によって行わせる場合には、労働者派遣契約書に秘密保持義務等個人情報の取扱いに関する事項を明記する。

(事案の報告及び再発防止措置)

第29条 保有個人情報の漏えい、滅失又は毀損等の事案の発生又は兆候を把握した場合等、安全確保の上で問題となる事案(以下「事案」という。)が発生した場合に、その事実を知った職員等は、直ちに保護管理者に報告する。

2 保護管理者は、被害の拡大防止又は復旧等のために必要な措置を速やかに講ずる。ただし、外部からの不正アクセス及び不正プログラムの感染が疑われる当該端末等のLANケーブルを抜く等、被害拡大防止のため直ちに行うことができる措置については、直ちに行う(職員等に行わせることを含む。)ものとする。

3 保護管理者は、事案の発生した経緯、影響範囲、被害状況等を調査し、総括保護管理者に速やかに報告する。ただし、特に重大と認める事案が発生した場合には、直ちに総括保護管理者に当該事案の内容等について報告する。

4 保護管理者は、事案の発生した原因を分析し、速やかに再発防止のために必要な措置を講ずる。

(公表等)

第30条 保護管理者は事案の内容、影響等に応じて、速やかに事実関係及び再発防止策の公表、当該事案に係る保有個人情報の本人への対応等の措置を総括保護管理者と協議の上、講ずる。

(点検)

第31条 保護管理者は、自ら管理責任を有する保有個人情報の記録媒体、処理経路、保管方法等について、定期に及び必要に応じ随時に点検を行い、必要があると認めるときは、その結果を総括保護管理者に報告する。

(評価及び見直し)

第32条 保護管理者は、保有個人情報の適切な管理のための措置については、点検又は管理規則第39条に定める監査の結果等を踏まえ、実効性等の観点から保有個人情報等の適切な管理のための措置について評価し、必要があると認めるときは、その見直し等の措置を講じ、総括保護管理者に報告する。

(苦情への対応)

第33条 保護管理者は、個人情報の取扱いに関する苦情について、迅速かつ適切に対応できるよう体制整備を行う。

(雑則)

第34条 この要項に定めるもののほか、個人情報保護の管理に関し必要な事項は、病院長が別に定める。

附 則

この要項は、平成17年4月1日から施行する。

附 則

この要項は、平成18年7月1日から施行する。

附 則

この要項は、平成22年10月1日から施行する。

附 則

この要項は、平成24年5月9日から施行する。

附 則

この要項は、平成27年4月8日から施行し、改正後の第7条第2項、第15条第1項、第15条の2から第17条まで、第24条の2、第25条及び第28条の規定は、平成27年4月1日から適用する。

附 則

この要項は、平成28年4月1日から施行する。

附 則

この要項は、平成29年4月1日から施行する。

附 則

この要項は、平成30年4月1日から施行する。

附 則

この要項は、平成31年4月1日から施行する。

別表（第4条、第5条関係）

副保護管理者	保護担当者
診療科長	医局長、外来医長、病棟医長
中央診療施設等の長	副部長、副センター長、教員
副総合臨床研究部長	センター長
医療情報経営企画部長	副部長、教員
薬剤部長	副部長、室長
看護部長	副部長、看護師長
医療技術部長	副部長、部門長
栄養管理部長	副部長
医療の質・安全管理部長	副部長
感染制御部長	副部長
病院事務部の各課長	各課の副課長相当の者、各課の係長相当の者
寄附講座の特任教授又は特任准教授	特任講師、特任助教