東北医科薬科大学病院個人情報保護に関する規程

（目的）

第１条　この規程は、学校法人東北医科薬科大学個人情報保護に関する規程（以下「大学規程」という。）、に基づき、東北医科薬科大学病院（以下「病院」という。）が保有する個人情報の保護について、必要な事項を定めるものとする。

（定義）

第２条　この規程における用語の意義は、大学規程第２条の定めるところによる。

（個人情報保護管理責任者）

第３条　病院に、次の各号のとおり、大学規程第４条第１項に定める個人情報保護管理責任者を置く。

（1）　病院長（病院の教育・研究・診療に係る保有個人情報）

（2）　事務部長（事務部各グループに係る文書）

2　管理責任者は、保有個人情報の適切な管理を確保する。保有個人情報を情報システムで取り扱う場合、管理責任者は、当該情報システムの管理者と連携して、その任に当たる。

（個人情報保護管理者）

第４条　病院に、次の各号に定める組織単位ごとに、大学規程第５条第１項に定める個人情報保護管理者を置く。

（1）　東北医科薬科大学病院組織規程第７条、第８条に定める診療科

（2）　東北医科薬科大学病院組織規程第９条に定める中央診療部門

（3）　東北医科薬科大学病院組織規程第１０条、第１１条、第１２条及び第１３条に定める特殊診療部門、院内共同利用部門、薬剤部及び看護部

（4）　東北医科薬科大学病院組織規程第１４条に定める事務部各グループ

2　前項の保護管理者は、前項各号に掲げる組織の長を持って充てるものとする。

3　保護管理者は、保護管理責任者を補佐し、保有個人情報の管理に関する事務を行う。

（個人情報管理委員会）

第５条　病院に、東北医科薬科大学病院個人情報管理委員会（以下「委員会」という。）を置く。

2　委員会の構成、業務については、「個人情報管理委員会規程」に定めるものとする。

（教育研修）

第６条　保護管理者は、保有個人情報の適切な管理のため、保有個人情報の取扱いに従事する職員（派遣労働者を含む。以下「職員」という。）に対して、管理責任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ものとする。

（職員の責務）

第７条　職員は、法の趣旨に則り、関連する法令及び規程等の定め並びに管理責任者、保護管理者の指示に従い、保有個人情報を取り扱わなければならない。

2　職員は、前項の責務を記載した誓約書に署名し、病院に提出しなければならない。

（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とその権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限らなければならない。

2　アクセス権限を有しない職員は、保有個人情報にアクセスしてはならない。
3　職員は、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、次の各号に掲げる行為については、当該保有個人情報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し、職員は、保護管理者の指示に従い行うものとする。
（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、保護管理者の指示に従い、訂正等を行うものとする。
（媒体の管理等）
第 11 条　職員は、保護管理者の指示に従い、保有個人情報が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、施錠等を行うものとする。
（廃棄等）
第 12 条　職員は、保有個人情報又は保有個人情報が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ものとする。
（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ものとする。
（アクセス制御）
第 14 条　保護管理者は、保有個人情報（情報システムで取り扱うものに限る。以下第 22 条まで（第 20 条を除く。）において同じ。）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、生体情報等をいう。以下同じ。）を設定する等のアクセス制御のために必要な措置を講じなければならない。
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（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定期的な措置を講ずるものとする。
（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、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ものとする。
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じなければならない。
（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の監視のため、保有個人情報を含むか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等の必要な措置を講ずるものとする。

（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ものとする。

（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、ファイアウォールの設定による経路制御等の必要な措置を講じなければならない。

（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、滅失又は毀損等（以下「情報漏えい等」という。）の防止のため、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。）を講じなければならない。

（情報システムにおける保有個人情報の処理）

第 18 条　職員は、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限り、処理終了後は不要となった情報を速やかに消去しなければならない。保護管理者は、当該保有個人情報の秘匿性等その内容に応じて、随時、消去等の実施状況を重点的に確認するものとする。

（暗号化）

第 19 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、その暗号化のために必要な措置を講ずるものとし、職員は、これを踏まえ、その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ものとする。

（入力情報の照合等）

第 20 条　職員は、情報システム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ものとする。

（バックアップ）

第 21 条　保護管理者は、保有個人情報の重要度に応じて、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ものとする。

（情報システム設計書等の管理）

第 22 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じなければならない。

（端末の限定）

第 23 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ものとする。

（端末の盗難防止等）

第 24 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じなければならない。
2　職員は、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ならない。
（第三者の閲覧防止）
第 25 条　職員は、端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう、使用状況に応じて情報システム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ものとする。
（記録機能を有する機器・媒体の接続制限）
第 25 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情報漏えい等の防止のため、スマートフォン、USB メモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機能の更新への対応を含む。）等の必要な措置を講ずるものとする。
（入退管理）
第 26 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「サーバ室等」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、利用及び持出しの制限又は検査等の措置を講じ、保有個人情報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、必要があると認めるときは、同様の措置を講ずるものとする。
2　保護管理者は、必要があると認めるときは、サーバ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ものとする。
3　保護管理者は、サーバ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ものとする。
（サーバ室等の管理）
第 27 条　保護管理者は、外部からの不正な侵入に備え、サーバ室等に施錠装置、警報装置、監視設備の設置等の措置を講ずるものとする。
2　保護管理者は、災害等に備え、サーバ室等に、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ものとする。
（保有個人情報の提供）
第 28 条　保護管理者は、法令に基づく提供に該当し、利用目的以外の目的のため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ものとする。
（匿名加工情報の作成等）
第 29 条　保護管理者は、匿名加工情報を作成するときは、特定の個人を識別すること及びその作成に用いる個人情報を復元することができないよう保有個人情報を加工するものとする。この場合において当該匿名加工情報に含まれる個人の情報の項目を公表するものとする。
（匿名加工情報の第三者提供）

第 30 条　保護管理者は、匿名加工情報を第三者に提供するときは、あらかじめ第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供方法について公表するとともに当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を明示するものとする。

（匿名加工情報の管理措置等）

第 31 条　保護管理者は、匿名加工情報の安全管理のために必要かつ適切な措置、当該匿名加工情報の取扱いに関する苦情の処理その他の当該匿名加工情報の適正な取扱いを確保するために必要な措置を講じ、当該措置の内容を公表するものとする。

（業務の委託等）

第 29 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、必要な措置を講じ、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ものとする。

(1)　個人情報に関する秘密保持、持出し及び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廃棄、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
(7)　漏えい事案等が発生した場合の委託先の責任に関する事項
(8)　従業者に対する監督・教育に関する事項
(9)　契約内容の遵守状況について報告を求めることに関する事項
(10)　病院が必要があると認めるときは委託先に対して実地の調査を行うことができる事項

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業務等個人情報の取扱いに関する事項を明記するものとする。

（相談及び苦情の対応）

第 30 条　保護管理者は、個人情報の保管、利用、提供等に関する相談及び苦情に対応するため、必要な措置を講じ、適切かつ迅速な処理に努めなければならない。

（情報漏えい等発生時の事案の報告及び再発防止措置）

第 31 条　保有個人情報の情報漏えい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。）又は事案の発生のおそれを認識した場合に、その事案等を認識した職員は、直ちに当該保有個人情報を管理する保護管理者に報告しなけれ

ばならない。
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じなければならない。
3　保護管理者は、発生した事案の経緯、被害状況等を調査し、管理責任者に報告するものとする。ただし、特に重大と認める事案が発生した場合には、直ちに管理責任者に当該事案の内容等について報告しなければならない。
4　保護管理者は、発生した事案の原因を分析し、再発防止のために必要な措置を講じなければならない。
5　管理責任者は、個人データの漏えい等が発生し、個人の権利利害を害するおそれが大きいものとして次に掲げる事態が生じたときは、当該事態を知った後、速やかに個人情報保護委員会（内閣府外局）及び文部科学省に報告しなければならない。
(1)　要配慮個人情報が含まれる個人データ（高度な暗号化その他の個人の権利利益を保護するために必要な措置を講じたものを除く。以下同じ。）の漏えい、滅失若しくは毀損
(2)　不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
(3)　不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
(4)　個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

6　前項の場合における報告事項は、次に掲げるものとする。
(1)　概要
(2)　漏えい等が発生し、又は発生したおそれがある個人データの項目
(3)　漏えい等が発生し、又は発生したおそれがある個人データに係る本人の数
(4)　原因
(5)　二次被害又はそのおそれの有無及びその内容
(6)　本人への対応の実施状況
(7)　公表の実施状況
(8)　再発防止のための措置
(9)　その他参考となる事項

7　管理責任者は、第5項に定める事態を知った後、当該事態の状況に応じて速やかに、当該本人の権利利益を保護するために必要な範囲において、本人に対し、前項第1号、第2号、第4号、第5号及び第9号に定める事項を通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利 利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

（公表等）
第32条　管理責任者は、発生した事案の内容、影響等に応じて、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講じるものとする。
（点検）
第33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、その結果を管理責任者に報告するものとする。

（評価及び見直し）
第 34 条　保護管理者等は、監査又は点検の結果等を踏まえ、実効性等の観点から保有個人情報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ずるものとする。
（雑則）
第 35 条　この規程に定めのない事項は、個人情報保護の保護に関する法律（平成 15 年法律第 57 号)、その他の関連法令に従う。

附則
平成 17 年 4 月 1 日付、東北厚生年金病院医療安全管理マニュアル別添、個人情報保護管理規程、個人情報保護取扱規程として施行する。
平成 25 年 4 月 1 日付、東北薬科大学病院医療安全管理マニュアル別添、個人情報保護管理規程、個人情報保護取扱規程として施行する。
平成 28 年 4 月 1 日付、東北医科薬科大学病院個人情報保護に関する規程として施行する。
令和 2 年 1 月 10 日付、一部改定し施行する。
令和 4 年 4 月　1 日付、一部改定し施行する。

個人情報管理委員会