医療法人緑栄会個人情報保護規程

第一章　　総則

（目　　的）

第　１条　　この規程は、医療法人緑栄会（以下「当法人」という）の事業遂行上取り扱う個人情報を適切に保護するために必要な基本的事項を定めたものである。

（適用範囲）

第　２条　　この規程は、当法人の役員及び職員に対して適用する。 また、個人情報を取り扱う業務を外部に委託する場合の委託先及び労働者派遣法に基づく派遣労働者に対しても適用する。

（用語の定義）

第　３条　　以下の通り用語を定義する。

①個人情報

患者等の個人を特定することができる情報のすべて。

②役員

当法人定款で規定する役員を指し、理事長、理事、監事を含む。

③職員

当法人の業務に従事する者で、正職員のほか、嘱託職員、派遣職員、臨時職員、各研究員を含む。

④開示

情報の内容を書面等で示すこと。

第二章　　個人情報保護方針の策定等

（個人情報保護方針の策定）

第　４条　　当法人の理事長（以下「理事長」）は、個人情報の保護・管理に対する姿勢を示し、役員及び職員に周知させるとともに、一般に公開するために個人情報保護方針を策定しなければならない。

方針に含む基本事項は以下の内容とする。

①個人情報の収集、利用及び提供に関する事項

②個人情報への不正アクセス、改ざん、破壊、漏洩及び個人情報の紛失等の防止に関する事項

③個人情報に関する法令及びその他の規範の遵守に関する事項

④個人情報の保護・管理に係る措置の継続的改善に関する事項

（個人情報保護方針の周知）

第　５条　　理事長は、当法人の策定した「個人情報保護方針」を役員及び職員へ周知させる。

（個人情報保護方針の公開）

第　６条　　「個人情報保護方針」の一般への公開は、院内掲示等による。

（個人情報保護方針の見直し）

第　７条　　理事長は「個人情報保護方針」を必要に応じ適宜見直さなければならない。

第三章　　個人情報保護管理体制

（管理体制）

第　８条　　理事長は個人情報の保護・管理を適切に実施するために、個人情報保護責任者、総括個人情報管理者、各部署個人情報取扱責任者及び監査責任者を設置する。

それぞれの役割、責任及び権限は以下のとおりとする。

①個人情報保護責任者

個人情報保護責任者は理事長が就任し、当法人の個人情報保護に関する責任者として個人情報保護活動にあたる。

②総括個人情報管理者

総括個人情報管理者は事務部長が就任し、個人情報保護責任者を補佐するとともに、各部署の個人情報取扱責任者を指揮する。

③各部署個人情報取扱責任者

各部署における個人情報取扱責任者は各所属長が就任し、各部署で定める細則等に従い、個人情報を適切に運用する。

④個人情報保護委員会

個人情報保護委員会は、理事長及び各部長によって組織するものとし、必要に応じ各課（室）長その他を招集するものとする。

第四章　　個人情報保護の措置

（個人情報の収集）

第　９条　　個人情報の収集は、当法人が行う事業の範囲内で利用目的を明確に定め、その目的達成に必要な限度においてのみ行わなければならない。

２．　個人情報の収集は、適法かつ公正な手段で行わなければならない。

（個人情報の利用及び提供）

第１０条　　個人情報の利用及び提供は、情報を有する本人が同意を与えた利用目的の範囲内で行うものとする。 ただし、生命、身体、財産の保護のために必要な場合、本人の同意を得ることが困難であるとき等法令の定めによる場合は、同意なく利用及び提供することが出来る。

２．　個人情報の利用及び第三者への提供を行う場合は、前項但書による場合を除き、事前に本人の同意確認を確実に実施しなければならない。

（個人情報の適正管理）

第１１条　　個人情報は利用目的に応じ必要な範囲内において、正確かつ最新の内容に保つよう努めなければならない。

２．　取得した個人情報に関するリスク（個人情報への不正アクセス、改ざん、破壊、漏洩及び個人情報の紛失等）に対して、合理的な安全対策が講じられなければならない。

３．　当法人が業務を委託するために個人情報を外部へ預託する場合、個人情報保護が損なわれることのないよう、適切な措置がとられなければならない。

（個人情報に関する情報主体の開示、訂正請求等に関する権利）

第１２条　　個人情報を有する本人から自己の情報について開示を求められた場合は、合理的な期間内に速やかに対応しなければならない。

２．　開示の結果、誤った情報があり、訂正又は削除を求められた場合は、原則として合理的な期間内に速やかに対応し、当該個人情報の受領者に対して通知を行わなければならない。

（教育・訓練の実施）

第１３条　　個人情報保護責任者は、役員及び職員に対し、教育資料に基づき継続的かつ定期的に教育・訓練を行う。

（苦情及び相談）

第１４条　　個人情報の取扱に関する苦情等の窓口業務は、医事課受付部門が担当し、必要に応じ総括個人情報管理者（事務部長）へ連絡し、適正かつ迅速な処理に努める。

（情報漏えい事故発生時の措置）

第１５条　　情報漏えい事故が起きた際には、当事者及びその所属長は、速やかに『情報漏えい報告シート』を記載し、総括個人情報管理者（事務部長）へ報告する。総括個人情報管理者は、速やかに個人情報保護委員会を開き、再発防止対策を検討する。また、個人情報漏えいの事実または漏えいの恐れを把握したときは、直ちに所轄官庁に報告しなければならない。

第五章　情報システムの安全確保等

（アクセス制御）

第１６条　　所属長は、保有個人情報（情報システムで取り扱うものに限る。以下この章おいて同じ）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ものとする。

２．　所属長は、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ものとする。

３．　職員は、自己の利用する保有個人情報に関して認証機能が設定されている場合、その認証機能の適切な運用を行うものとする。

（アクセス記録）

第１７条　　特定個人情報へのアクセスに際しては、所属長は、アクセス状況を記録し、その記録を一定の期間保存し、定期に又は随時に分析するために必要な措置を講ずるものとする。

２．　所属長は、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ものとする。

（管理者権限の設定）

第１８条　　所属長は、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１９条　　所属長は、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ネットワーク経路制御等の必要な措置を講ずるものとする。

（不正プログラムによる漏えい等の防止）

第２０条　所属長は、不正プログラムによる保有個人情報の漏えい、滅失又は毀損の防止のため、ソフトウエ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（導入したソフトウエアを常に最新の状態に保つことを含む）を講ずるものとする。

（情報システムにおける保有個人情報の処理）

第２１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するものとする。

２．　所属長は、前項の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２２条　所属長は、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する。

２．　職員は、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（適切なパスワードの選択、パスワードの漏えい防止の措置等を含む）を行うものとする。

（入力情報の照合等）

第２３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２４条　所属長は、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２５条　所属長は、保有個人情報に係る情報システムの設計書、仕様書、ネットワーク構成図等の文書について漏えい等が行われないよう、その保管、複製、廃棄等について必要な措置を講ずるものとする。

（端末の限定）

第２６条　所属長は、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２７条　所属長は、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ものとする。

２．　職員は、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。ただし、所属長の指示に従い、業務の必要最小限の範囲において行うときはこの限りではない。

３．　職員は、前項の規定に基づき、端末を外部へ持ち出したときは、紛失による漏えい等が行われないよう取扱いに注意するものとする。

（第三者の閲覧防止）

第２８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２９条　　所属長は、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・媒体の情報システム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。

第六章　　規程等の見直し等

社会情勢や情報主体の意識の変化、施行状況、監査の結果等を考慮し、本規程等を見直すものとする。

2016 年 9 月 1 日改訂
2015 年 9 月 5 日改訂
2014 年 10 月 15 日改訂
2007 年 1 月 16 日作成