医療法人社団　三友会 病院情報システム運用管理規程

第1章 総　則

（目的）
第1条
1 この規程は、医療法人社団三友会（以下「本社団」という。）あけぼの病院及びあけぼのクリニックにおける情報システムにて、法令に保存義務が規定されている診療諸記録の電子媒体による保存のために使用される機器、ソフトウェア及び運用に必要な仕組み全般（以下、「電子保存システム」という。）について、その取扱い及び管理に関する事項を定めることにより、本社団にて情報を適正に保存するとともに、適正な取扱いをするとともに、適正な取扱いをすることで患者の権利、利益の侵害の防止および個人情報の適正な取り扱いを行い、利用者及び管理者の正当性を確保することを目的とする。
2 この規程は付属マニュアルとして「管理者マニュアル」及び「利用者マニュアル」を定める。

（情報システムのデータ保護）
第2条
本社団の情報システムのデータは、この規程及び「管理者マニュアル」および「利用者マニュアル」の定めるところにより保護されるものとする。

（データ及び秘密情報の保護）
第3条
情報システムの診療情報等を含むデータおよび秘密情報は、機密性、一貫性、可用性を維持して保護されなければならない。

（電子保存に関する理念）
第4条
電子媒体に保存された保存義務のある情報が患者の診療や本社団の管理運用上必要とされるときに、信頼性のある情報を迅速に提供できるよう、協力して環境を整え、適正な運営に努めなければならない。
（1） 自己責任の原則
自己責任とは、本社団が運用する情報システムの電子保存システムについて責任を果たすことを意味する。
（2） 真正性・保存性・見読性の原則
真正性とは、正当な人が記録し確認された情報に関し第三者から見て作成の責任と所在が明確であり、かつ、故意又は過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性の記録内容を誤ることをいう。見読性とは、電子媒体に保存された内容を必要に応じて肉眼で見読可能な状態に容易にできることである。なお、“必要に応じて”とは、『診療、患者への説明、監査、訴訟等に関してその目的に応じて』という意味であり、“容易に“とは、『目的にあった速度、操作で見読を可能にすること』を意味する。保存性とは、記録された情報が、法令等で定められた期間にわたって、真正性を保ち、見読可能にできる状態で保存されることをいう。
（3） 周知原則
利用者は情報システムへの信頼を高めるために、診療情報等の保護対策、手続き、規則の存在及びその範囲について適切な知識を得ることができ、管理者はそれについて周知を図る。
（4） 倫理原則
情報システムの保護対策は、他の者の権利および利益を尊重して提供され利用されるべきである。

(5) 一貫性の原則

診療情報等の保護のための対策、手続き、規則には、技術、管理、組織、運営、教育、法律を含めた範囲での関連する考え方を考慮に入れて院内の対策、手続き、規則との統一を図るべきである。

(6) 再評価原則

情報システムの保護施策の要求は、運用形態、利用形態および技術と共に変化するため、診療情報等保護のため対策、手続き、規則は定期的に再評価する。

(7) 患者のプライバシーおよび個人情報保護の原則

診療情報の二次的利用(診療や病院管理を目的としない利用)についても、患者の個人情報およびプライバシーが侵害されることのないように注意しなければならない。

(真正性の担保)

第5条

本社団は電子保存に関する真正性を担保する為、以下の通り定める。

(1) 情報システム管理者(以下、「システム管理者」という。)は、電子保存システムの入力者及び確定者の登録を管理し、そのアクセス権限を定め、不正な利用を防止しなければならない。

(2) パスワードの最低文字数、有効期間等を定めなければならない。

(3) 認証の有効回数、超過した場合の対処を定めなければならない。

(4) 入力者及び確定者は、自身の認証番号やパスワードを管理し、これを他者に利用させてはならない。

(5) 入力者及び確定者は、電子保存システムの情報の参照や入力(以下「アクセス」という。)に際して、認証番号やパスワード等によって、システムに自身を認識させなければならない。

(6) システム管理者は、電子保存システムを正しく利用させるため、入力者及び確定者の教育と訓練を行わなければならない。

(7) 入力者及び確定者は、作業終了あるいは離席する際は、必ずログアウト操作を行わなければならない。

第2章 責　任

(業務の明確化)

第6条

業務の管理者は、情報システムを利用する業務内容を、以下の範囲において明確にしておかなければならない。

(1) 業務の名称

(2) 業務の目的

(3) 業務の管理者とその者の権限の範囲

(4) 利用者とその者の権限の範囲・診療情報等の記録の内容

(利用者権限の付与の決定)

第7条

システム運用責任者は業務責任者と協議して、その権限付与について各利用者にその内容を周知し、その徹底を図らなければならない。

(診療情報等の取り扱い)

第8条

システム管理者は、診療情報等に対して、以下の方針に則り取扱い権限の付与に関し、協議を行うものとする。

(1) 診療情報等の登録、参照、更新の各権限は、情報システムごとに分離されること。

(2) 利用者への権限の付与規定の決定は、病院長、システム運用責任者、業務責任者が行うこと。

(3) 業務上不必要な権限は付与しないこと。

第3章 運　用

（教育および訓練）

第9条

1 業務責任者は、利用者あるいは利用者になるものに対して、診療情報等を保護する目的とその必要性を十分に理解させ、その対策を推進するために、教育訓練を行うものとする。

2 システム管理者は新規の業務担当者に対して、操作前に教育訓練を行うものとする。

（廃棄）

第10条

システム運用責任者は、ハードコピーを取った資料などの不要となった診療情報等を安全な方法で、かつ、速やかな廃棄・消去することを各部門に指導しなければならない。

第4章 電子保存に関する情報の範囲

（情報の範囲）

第11条

本社団において、電子保存にする際に対象とする情報の範囲については、システム運用管理者の審議を経て、病院長がそれを定める。また、電子保存を行う対象のシステム（イントラネットに属さないスタンドアロン含む）は、以下のとおりとする。

（１）電子カルテシステム　　（２）医事会計システム　（３）画像管理システム
（４）検体検査システム　（５） 生理検査システム　（６）リハビリ部門システム
（７）栄養管理システム　（８）内視鏡画像管理システム　（９）健診システム

（システムの機能要件）

第12条

情報システム（イントラネットに属さないスタンドアロン含む）は、次の機能を備えるものとする。

(1) 情報にアクセスしようとする者の識別と認証
(2) 利用者のアクセス制限の設定と不正なアクセスを排除する機能
(3) 利用者が入力した情報について確定操作を行うことができる機能
(4) 利用者が確定操作を行った情報を正確に保存できる機能
(5) 管理上または診察上の必要がある場合、記録されている情報を速やかに出力する機能
(6) 記録された情報の複製（バックアップ）を作成する機能。

（保存期間）

第13条

電子保存を行う診療に関わる情報の保存期間は、法令を順守し、本社団に定められた保存期間とする。

第5章　管理組織

（システム管理者）

第14条

本社団はシステム管理者を置き、病院長及び所長をもってこれに充てる。なお、システム管理者の職責は以下の通りとする。また、システム管理者が遵守・注意すべき事項は「管理者マニュアル」に定める。

（1）必要な場合、病院長及び所長はシステム管理者を別に指名することができる。
（2）機器及びソフトウェアの導入に当たって診療録等の保存義務に適合するように留意する。
（3）システムの機能が支障なく運用される環境を整備する。
（4）電子保存された情報の安全性を確保し、常に利用可能な状態におく。
（5）機器ソフトウェアに変更があっても情報が継続時に利用できるよう維持する。
（6）利用者の登録を管理し、不正利用を防止する。
（7）マニュアルの整備：取扱いマニュアルを整備し、利用者に周知の上、利用可能にする。
（8）教育と訓練：利用者に対し、取扱い並びにプライバシー及び個人情報保護に関する研修を行う。
（9）情報システムについての苦情・質問を受け付ける窓口を設け、その対応を行う。受け付けた苦情・質問に対して、その内容を検討し、速やかに必要な措置を講ずる。
（10）緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、文書化し、利用者に周知の上、常に利用可能な状態におく。
（11）情報システムの利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行う。
（12）職務により定められた権限によるデータアクセス範囲を定め、必要に応じてハードウェア・ソフトウェアの設定を行う。また、その内容に沿って、アクセス状況の確認を行い、業務上において情報漏えい等のリスクが予想されるものに対し、運用管理規程の見直しを行う。また、事故発生に対しては、速やかに運用責任者に報告し利用者に周知する。
（13）利用者に対し、定期的に情報システムの取扱い及びプライバシー保護に関する研修を行う。
（14）システム構成やソフトウェアの動作状況に関する内部監査を定期的に実施する。
（15）システム管理者は定期的に情報の所在確認を行い、障害時の対応体制が最新のものであるように管理する。
（16）データバックアップ作業が適切に行われていることを確認する。
（17）電子保存システムで使用されるソフトウェアを、使用の前に審査を行い、情報の安全性に支障がないことを確認する。
（18）定期的にソフトウェアのウィルスチェックを行い、感染の防止に努める。
（19）適宜、業務において規程に則った運用がなされていることを確認する。

（運用責任者）

第15条

本社団は情報システムの運用を円滑に行うために運用責任者を置き、病院長及び所長をもってこれに充てる。なお、運用責任者の職責は以下の通りとする。

（1）必要な場合、病院長及び所長は運用責任者を別に指名することができる。
（2）情報システムを円滑に運営し、情報システム全体の管理を行う。
（3）情報システムが常に効率の効率化及び円滑化の為に情報収集し、合理的な運営を指針する為に適切にシステム管理者に諮問を行う。

（個人情報保護責任者）

第16条

本社団は情報システムの保護を確実に行うために個人情報保護責任者を置き、病院長及び所長をもってこれに充てる。なお、個人情報保護責任者の職責は、本社団の定める「個人情報保護規程」による。

（情報システムの管理）

第17条

本社団は情報システムの管理に関し、以下の通り定める。

（1）機器の管理

（ア） サーバ室の施錠管理を行う

（イ） 院内情報システム端末機器の管理を行う

（ウ） OA端末機器の管理を行う

（エ） 院内情報システムおよびOA端末機器に接続する外付けデバイスの管理を行う

（オ） サーバ室には、無停電電源装置を備える

（2）ソフトウェアの管理

（ア） ソフトウェアを使用前に審査を行い安全性の確認を行う

（イ） ウィルスチェックを行い感染の防止に努める

（3）ネットワーク管理

本社団の拠点間システムネットワークのネットワーク接続及びイントラネットにおけるセキュリティ管理を万全に行い、接続拠点間の安定運用を維持する

（4）記録媒体の管理

（ア） データ保護(RAID)によるサーバシステムを構築する。

（イ） サーバシステムを経由していないソフトウェア管理のデータベースのバックアップは、USBメモリまたは外付けHDDを使用する。

（5） その他の事項

（ア） 情報システムに用いる機器及びソフトウェアを導入するに当たって、システムの機能を確認する。

（イ） 情報システムの機能要件に挙げられている機能が支障なく運用される環境を整備する。

（ウ） 診療情報の安全性を確保し、常に利用可能な状態に置いておく。

（エ） 機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持する。

（オ） システム管理者は情報システムの利用者の登録を管理し、そのアクセス権限を定め、不正な利用を防止する。

（カ） 情報システムを正しく利用させるため、作業手順書の整備を行い利用者の教育と訓練を行う。

（キ） 患者及び利用者から、情報システムについての問い合わせや苦情を受け付ける窓口を設ける。

（ク） 機器・媒体やソフトウェアの変更に当たっては、データ移行のための業務計画を作る。

（ケ） 機器やソフトウェアに変更があった場合においても、電子保存された情報が継続的に使用できるよう維持する。

（コ） 電子保存システムの記録媒体を含む主要機器は管理者によって入退室管理された場所に設置する。

（サ） 機器の設置場所には無水消火装置、漏電防止装置、無停電電源装置等を備える。

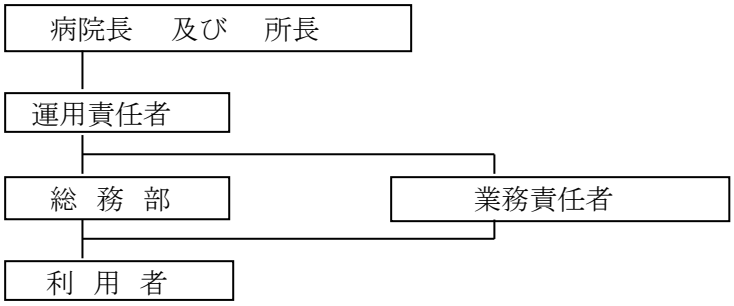
（シ） 設置機器は定期的に点検を行う。

第6章　安全管理

（組織体制）

第18条

システム運用の組織は以下の通りとする。



（データ破棄）

第19条

個人情報を記した媒体の廃棄に当たっては、以下の通り安全かつ確実に行い、システム管理者が作業前後に確認し、結果を記録に残さなければならない。

（1）電子記憶媒体（USBメモリなど、パソコン等に接続できる全ての電子媒体を指す。以下「記録媒体」という）の場合

媒体の破棄は、読取り不能の状態にした後、指定の廃棄場所に破棄する。

（ア）ハードディスク

ハードディスクデータ完全抹消ソフトを用いデータを破棄するか、物理的に破壊をして読取り不能にする。

（イ）CD・DVDメディア・USBメモリ等

物理的に破壊をして読取り不能にする。

（2）紙帳票の場合

業務運用上発生する廃棄帳票は、シュレッダーにかけ、廃棄置場に破棄する。

（ドキュメント管理）

第20条

1 ドキュメント管理は以下の通りとする。なお、取り扱いドキュメントとは、システムプログラム・ユーザースプログラム等情報システムの医療情報を含むデータ及び機密情報が記述されている全てのドキュメントを指す。

（1）媒体の場合

磁気媒体に記憶されたプログラムドキュメントは、施錠管理される場所あるいは施錠管理のできる保管ロッカーに保管する。

（2）紙帳票の場合

紙に記述されたドキュメントは、施錠管理される場所あるいは施錠管理のできる所定の保管ロッカーに保管する。

2 ドキュメントの保管、バックアップの作業に当たる者は、手順に従って行い、その作業の記録を残し、システム管理者の承認を得なければならない。

（入退室管理）

第21条

サーバ室への入退室の管理は以下の通りとする。

（1）サーバ室へ入退できる者は、運用責任者の了解を得た以下の者に限定する。

・病院職員（情報システムに関し権限付与のある者。）

・運用支援要員
・システム開発者
・本社団が契約あるいは依頼した保守業者
・本社団が認めた訪問者

(2) サーバ室への入退者は名簿に記録を残さなければならない。また、運用責任者は入退出の記録の内容について定期的にチェックを行わなければならない。

(3) 夜間あるいは時間外の訪問者は、時間外受付を通して事務当直者の確認を得なければならない。

(情報システム障害対策等)

第22条

1 運用責任者は情報システムの障害に対応し、システムの障害対応の詳細について全職員に周知しなければならない。

2 運用責任者は機器・システムの状態や通信状態を収集・把握し、ログを適切に記録しなければならない。

(ネットワーク管理)

第23条

本社団は情報システムのネットワーク管理に関し、以下の通り定める。

(1) イントラネットの構築

情報システム利用に限定された医療業務用ネットワークを本社団内に構築すること。なお、利用にあたり、以下の事項を遵守すること。

(ア)医療情報等の個人データを取り扱う機器・端末は、イントラネットに接続しなければならない。
(イ)医療情報等の個人データは、許可なく情報システムの外に出してはならない。
(ウ)医療情報等の個人データを、可搬記憶媒体に保存してはならない。

(2) インターネットの構築

外部的な情報通信を行うため、イントラネットと切り離した単独でのコンピュータネットワークを本社団内に構築すること。なお、利用にあたり、以下の事項を遵守すること。

(ア)個人情報を含む情報をメールで送受信してはならない。
(イ)インターネットを経由して本社団外のサーバに個人情報を 送受信してはならない。
(ウ)本社団内の端末を本社団外からアクセスできる状態にしてはならない。

(3) リモート保守回線管理

運用責任者は、情報システムの保守・運用作業を行うためリモート保守の回線を整備すること。
リモート保守に関して以下の項目を以下の事項を遵守し利用すること。
(ア)リモート保守を行う端末には、医療情報等の個人データを保存してはならない。
(イ)リモート保守を行う回線の接続は、作業を行うとき以外行ってはならない。
(ウ)リモート保守をできる者は、本社団が契約あるいは依頼したシステム開発会社・コンピュータ保守業者に限定し、保守を行う時は必ず 運用責任者の了解を得なければならない。
(エ)リモート接続はVPN網を使用し、外部のインターネットを経由してはならない。

(4) 無線LANに関する対策

セキュリティ対策不正アクセスの対策として、SSID によるアクセス制限を行う。また、SSIDは、システム運用責任者が管理する。

(ウイルス感染対策)

第24条

本社団はウイルス感染対策として以下の通り定める。

(1) インターネットに接続している端末には、ウイルス感染の防止等データ保護のために端末にウイルス対策ソフトを常駐させるなど必要な措置を講じなければならない。

（2）インターネットに接続している端末で使用したUSBメモリ及び外付けHDDは、イントラネットワーク端末に接続してはならない。

（記録媒体への複写）
第25条
情報を記録媒体に複写する場合は、以下の事項に留意しなければならない。
（1）個人情報を可搬型記録媒体で渡す場合は記録を残す。
（2）特に許可した場合を除き，データのバックアップ業務以外には，外部記憶媒体への個人情報の複写を禁止する。
（3）媒体使用時は，必ずウイルス等の不正なソフトウェアの混入がないか確認する。

（記録媒体の保護）
第26条
記録媒体を保護する為、以下の事項に留意しなければならない。
（1）記録媒体は、記録された情報が保護されるよう、別の媒体にも補助的に記録する。
（2）品質の劣化が予想される記録媒体は、あらかじめ別の媒体に複写する。
（3）システム管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳に記録しなければならない。また、その内容を定期的にチェックし、所在状況を把握しなければならない。

（利用者の責務）
第27条
情報システムの利用について、利用者は以下の事項を遵守しなければならない。また、情報システムの利用方法及び遵守・注意事項は「利用者マニュアル」に定める。
（1）利用者は、情報システムの情報の参照や入力（以下「アクセス」という。）に際して、認証番号やパスワード等によってシステムに自身を認識させ、自身の認証番号やパスワードを管理し、これを他者に利用させてはならない。
（2）利用者は、情報システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行い、入力情報に対する責任を明示しなければならない。
（3）利用者は、与えられたアクセス権限を超えた操作をしてはならない。
（4）利用者は、参照した情報を、目的外に利用してはならない。
（5）利用者は、患者のプライバシーを侵害してはならない。
（6）利用者は、システムの異常を発見した場合、速やかにシステム管理者に連絡し、指示を仰がなくてはならない。
（7）利用者は、不正アクセスを発見した場合、速やかにシステム管理者に連絡し、指示を仰がなくてはならない。
（8）利用者は、離席する際、ログアウトを必ず行わなければならない。
（9）個人情報の取り扱いについては、医療法人社団三友会個人情報保護規程に則り運用を行わなければならない。

（私物端末の持ち込み）
第28条
私有のパソコン等（携帯電話、スマートフォン、タブレット端末、複合機等のインターネットを使用できる全ての機器・媒体を指す。以下「パソコン」という）を持ち込み、診療情報等の個人情報にアクセスするための病院情報システム（イントラネットワーク）に接続してはならない。但し、やむを得ない場合にはシステム管理者の承認を受け、定められた安全管理措置を行って接続を行う。

（情報等の持ち出し）
第29条

1 システム管理者は、情報、情報機器、端末、記録媒体、情報資産及びソフトウェア並びに紙帳票（以下「情報等」という）の持ち出しに関し、リスク分析を行い、持ち出し対象となる情報等を定める。本社団はシステム管理者の判断を追認し、利用者及び職員等（本社団に係わる全ての者を指す以下「職員等」という）は当該持ち出し対象となる情報等以外の情報等を外部へ持ち出してはならない。なお、持ち出し対象となる情報等は別表としてまとめ、職員等に公開する。

2 情報等を持ち出す場合は、所属、氏名、連絡先、持ち出す情報等の内容、格納する媒体、持ち出す目的、期間を別途定める書式でシステム管理者に届け出て、承認を得なければならない。

3 職員等は持ち出した情報等を、定められている以外のアプリケーションがインストールされた機器等で取り扱ってはならない。また、持ち出した情報等には、定められている以外のアプリケーションをインストールしてはならない。

4 職員等は、持ち出した情報等の盗難、紛失時には、直ちにシステム管理者に届け出なければならない。届け出を受け付けたシステム管理者は、その情報等の重要度にしたがって、迅速に対応しなければならない。

5 システム管理者は、情報等の持ち出しについてマニュアルを整備し、職員等に周知の上、常に閲覧可能な状態にしておかなければならない。

6 システム管理者は、職員等に対し、情報等の持ち出しについて研修を行わなければならない。

7 システム管理者は、持ち出す情報等について起動パスワード等を設定しなければならない。なお当該パスワードは推定しやすいものは避け、また定期的に変更しなければならない。

8 システム管理者は、持ち出す情報等について、ウイルス対策ソフトをインストールし、対策を施さなければならない。

（自然災害やサイバー攻撃等による非常時の対策）

第30条

本社団は自然災害やサイバー攻撃等による非常時の対策として以下の通り定める。

（1） 災害、サイバー攻撃等により、一部医療行為の停止等、医療サービス提供体制に支障が発生する非常時の場合、運用責任者の指揮の下、別途定める事業継続計画に従って運用を行うこと。

（2） 災害、サイバー攻撃等により一部医療行為の停止等、医療サービス提供体制に支障が発生した場合、別途定める一覧の連絡先に連絡すること。なお、所管官庁については、「医療情報システムの安全管理に関するガイドライン」の「自然災害やサイバー攻撃等による非常時の対策」に記載されている連絡先に連絡すること。

（3） システムの縮退運用時や非常時の運用に関して運用管理規程を作成し、職員等に周知の上、常に閲覧可能な状態におくこと。

（個人情報の取り扱い）

第31条

個人情報の取り扱いについては、本社団の定める「個人情報保護規程」に則り処理を行うこと。また、職員が当該情報システムを使用する事により知りえた情報は、在職中はもとより退職後においても守秘義務を負い、私的利用及び第三者への開示・漏洩をしてはならない。

（1）**「個人情報管理責任者」**とは、個人情報保護計画の策定、実施、評価、改善等の個人情報保護のための業務について、統括責任と権限を有する者を言う。（別紙参照）

（2）**「個人情報取り扱い担当者」**とは、個人情報をコンピューターへ入力、出力、台帳、申込書等の個人情報を記載した帳票を保管、管理する担当者をいう。（別紙参照）

（3）**「個人情報保護監査責任者」**とは、個人情報管理責任者から独立した公平かつ客観的な立場にあり、監査の実施及び報告を行う権限を有する者を言う。（別紙参照）

第7章 賠　　償

（損害賠償）
第32条
職員等が故意又は過失によって本規則に違反し本社団に損害を与えた場合は、就業規則による制裁のほか、本人または身元保証人に対し、損害賠償の全部または一部につき請求をする事がある。なお、その賠償責任は退職後も免れない。

第8章　附　　則

（協力）
第33条
各業務の管理者は、この規程の実施および診療情報等の保護のための対策、手続きおよび規則を可能な限り有効なものにするため、各管理者と協議し、調整し、協力しなければならない。

（義務と懲罰）
第34条
診療情報については、秘密を守る義務を課するとともに、これに違反した場合には就業規則に則り懲罰を科す。

（改廃）
第35条
本規程を改廃する時は、職員代表の意見を聞き、理事会において決定し、行われるものとする。

（施行）
第36条
この規程は、平成 27 年 8 月 1 日から施行する。
平成 31 年 1 月 1 日　　改訂
令和 6 年１２月１日　　改訂