総合病院 落合病院　情報セキュリティに関する基本規程

第１条（目的）

当院および当院職員が保有、管理する電子情報および電子システムについて、これらの取り扱いおよび過失、事故、災害、犯罪等からの保護について定める。

第２条（電子情報および電子システムの定義）

１．院内のサーバコンピュータ、コンピュータ端末（個人の持ち込みを含む）、モバイル端末（個人の持ち込みを含む）、その周辺媒体（電子情報を保存できるすべての媒体）に電子化されて保存・利用されている個人情報（個人情報の定義については、個人情報保護基本規程第２条に定める）および医療行為にかかる情報、企業運営等にかかる情報、機密情報。

２．院内で稼働している電子システムネットワークのすべて。（詳細は第５条に定義）

３．当院ウェブサイトおよび電子メールの情報。

第３条（適用範囲）

第２条に定義された電子情報および電子システムを取り扱う場合すべてに適用される。

第４条（管理体制）

１．当院に、病院長が指名する運用責任者および監査責任者を置く。
運用管理については、情報システムを円滑に運営するため実務担当者として、事務部門からシステム管理者を選任しする。したがって、運用責任者は当該部門の長とする。
監査については、落合病院情報管理委員会（以下、情報管理委員会）を常任委員会として置き、電子情報および電子システムの適切な取扱いについて監督し協議する。

２．システム管理者は、電子カルテシステムおよび付随するサブシステム、医用画像システム、文書システム、統合診療支援システム、透析支援システム、検査システム、調剤システム、イントラネット等のシステムおよびネットワーク全般について、統合的に管理を行う。ただし、このうち各部門に導入された医療機器等と連携する部門システム（調剤システム、検査システム、放射線システム等）については、各部門の長が運用ルールを策定し管理する。

３．管理上のシステムの分類は第５条に定めるとおりとする。

第５条（電子システムの分類）

以下に、当院における電子システムの管理上の分類を定義する。

１．医療系情報システム
電子カルテシステムおよび付随するサブシステム、医用画像システム PACS、文書管理システム Yahgee、統合診療支援システム CITA、透析システム Future Net、部門システム（薬局システム、検査システム）におけるハードおよびソフトウェア、周辺デバイスを含むシステムの運用に必要な仕組み全般とする。

２．情報系システム

イントラネットシステムおよびイントラネットワークを利用する介護システムにおけるハードおよびソフトウェア、周辺デバイスを含むシステムの運用に必要な仕組み全般とする

第６条（情報管理委員会）

情報管理委員会は、院内で利用される個人情報および電子情報の.適切な取扱いについて監督し、協議する。また、情報システムおよび情報セキュリティについて、ＰＤＣＡサイクルに基づいて見直しを行い、電子システムが有効かつ効率的に機能しているか検証を行う。

第７条（災害およびトラブル）

１．システム管理者は、電子システムの利用において、必要かつ十分な内容のマニュアル等を整備（システム付属のものでも可）し、適切な場所に保管または保存するとともに、容易に参照できるようにしなければならない。

２．システム管理者は、誤操作等の人為的ミスによるシステム障害等の発生を避けるため適切な操作方法および禁止事項を利用者に周知徹底しなければならない。

３．システム管理者は、災害やトラブル等によるシステム障害が発生した場合を想定し、その対応をあらかじめ定めておかなければならない。

４．システム管理者は、重大なシステム障害が発生した場合においても、速やかに復旧できるように、事業者間の連絡体系および作業体系を確立させておかなければならない。

第８条（禁止事項）

１．各電子システムにおける固有の禁止事項については、第４条の管理者により別に定める。

２．以下に該当する行為は、情報管理委員会の許可がある場合を除き、一切を禁止する。

ア．院内の端末に、実行プログラム（アプリケーションソフト等）をインストールする行為。また、業務に関係しないデータファイルを保存する行為。

イ．ＵＳＢメモリ等の記録メディアを用いて、第２条に定義された電子情報およびプログラムファイル等を院外に持ち出す行為。（電子情報の持ち出し申請については、第１０条に別途定める）

ウ．クライアント PC 本体およびモバイル端末自体を所定の場所から持ち出す行為。（診療行為および業務運営上、必要不可欠な場合を除く）

エ．個人が所有するコンピュータ端末を院内ネットワークに接続する行為。また、ルータ等のアクセスポイント（有線・無線を問わず）を設置する行為

オ．電子システムに、本人以外のＩＤおよびパスワードでログインする行為。

カ．電子情報を不正に削除、改ざんする行為。

キ．電子システムの作業画面や個人情報を含むファイル、共有ファイル等をディスプレイに表示したまま長時間放置しておく行為。（席を立つ等）

ク．院外より院内ネットワークに接続を試みる行為。

ケ．院内ネットワークから外部ネットワークおよびインターネットに接続を試みる行為。（接続許可端末を除く）

コ．第４条に定める管理者より使用権限を与えられていない利用者が、電子システムのサーバコンピュータを操作する行為。

サ．端末画面をスマートフォン等のガメラ機能で撮影する行為。（診療行為および業務運営上、必要不可欠な場合を除く）

シ．インターネットを利用する際の禁止事項については、第１８条以降に定義する。

ス．その他、法令および公序良俗に反する行為。

第９条（利用者）

１．システム管理者は、入職時もしくは異動時において利用者にＩＤとパスワードを付与する。その際、利用者の職種、役職等に応じたアクセス権限等を設定する。

２．電子情報および電子システムを利用する者は、当該システムの規程および運用ルールを遵守し、セキュリティ上の問題、運用上の問題、システム上の問題を発見した場合は、速やかに第４条に定める管理者に報告しなければならない。

３．アクセス権限の変更や新規ＩＤの取得、ソフトウェアのインストールなど、利用に関する申請は、システム管理者に行う。利用者の申請について、システム管理者では判断できかねる場合は、情報管理委員会にて審議を行う。

第１０条（電子情報の持ち出し）

業務上、電子情報およびプログラムファイル等を院外に持ち出す場合は、「電子情報使用許可申請書」を情報管理委員長に提出し、承認を得なければならない。持ち出した電子情報の利用に際しては、利用者は同申請書の「注意・禁止事項」を遵守し、情報管理委員長（または委員長より業務を付託された担当者）は、利用の終了を確認し、情報管理委員会に報告しなければならない。ただし、円滑に運営するため実務担当者としてシステム管理者が委員長を代行することができるものとする。

第１１条（バックアップ）

システム管理者は、電子システムおよびネットワーク等の障害等により電子情報が喪失する事態に備え、定期的にバックアップをとり、情報が喪失した場合に、その時点に近い状態に復旧しなければならない。

第１２条（安全保護対策）

システム管理者は、不正アクセス、情報の紛失、改ざん、漏えい等から電子情報および電子システムを保護し、かつ、業務効率を著しく低下させないように、合理的な安全保護措置を講じなければならない。

第１３条（原因究明）

システム管理者は、セキュリティ上の問題、運用上の問題、システム上の問題が発生または報告された時は、迅速に原因究明を行い、その被害を最小限にとどめる対策をとらなければならない。

第１４条（電子保存の三原則）

システム管理者は、医療情報システムにおける電子保存の三原則（真正性、見読性、保存性）を担保するため、定期的にサーバコンピュータおよびネットワークにかかる主要機器のメンテナンスを行わなければならない。これは、医療情報システムに限らず、院内電子システム全般において留意すべきである。

第１５条（サーバ室）

１．サーバ室の入退室に際しては、入退室管理簿に記録をつけなければならない。

２．システム管理者は、定期的にサーバ室の機器点検および空調点検を行わなければならない。

３．サーバ室の電子ロックの暗証番号は、病院管理者および施設管理者および第４条に定める管理者に付与するが、その他の利用者が暗証番号の付与を希望する場合は、情報管理委員会に申請し、承認を得なければならない。ただし、入室については業務委託する情報処理事業者およびサーバ室の機能維持にかかるメンテナンス等の専門業者、システム管理者等が不在の場合で、緊急的に入室の必要が生じた場合は、管理者の指示のもと、入室することができる。

４．サーバ室のサーバコンピュータを廃棄または入れ替え等で、室外に持ち出す必要がある場合は、システム管理者の承認を得なければならない。また廃棄が決定してから廃棄するまでの間、他の場所に移動させてはならない。これは、サーバ室以外に設置されたサーバコンピュータに対しても同様である。

第１６条（廃棄）

１．サーバコンピュータの廃棄については、第１５条の３の手順に従うが、専門業者にハードディスクの完全消去を依頼し、物理的破壊等によりデータが決して復元されないように処理することが望まれる。可能であれば、契約書または同意書等に条項を盛り込んでおくことが望ましい。

２．サーバコンピュータ以外のパーソナルコンピュータ等（クライアントサーバシステムにおけるクライアントコンピュータやノートパソコン等）の廃棄については、当院職員が廃棄場で適正に処分されていることを確認しなければならない。産廃事業者に委託する場合は、マニフェストにより、適正に処分されていることを確認しなければならない。

３．外付けＨＤＤ、ＵＳＢメモリ、ＣＤ、ＤＶＤ等の記録メディアの廃棄については、記憶領域のデータ削除（初期化）のみならず、物理的な破壊等によるセキュリティ対策を講じなければならない。

第１７条（業務委託）

第４条に定める管理者は、電子システムの管理・運営・保守等の業務の一部またはすべてを委託する場合、委託先の情報処理事業者において、経済産業省策定の「医療情報を受託管理する情報処理事業者向けガイドライン」を遵守するよう求め、可能であれば、契約書または同意書等に条項を盛り込んでおくことが望ましい。また、守秘義務契約、損害賠償等についても同様である。

第１８条（インターネット）

１．ウェブサイト上で本人または当院職員の個人情報、所属部署および当院の情報（住所、管理者名、メールアドレス等）を登録する場合（学会申し込み等）は、ＵＲＩやサイトの内容等を確認し、そのサイトの信頼性を十分検証したうえで行わなければならない。

２．院内の端末からインターネット上のファイル等をダウンロードする場合は、ＵＲＩやサイトの内容等を確認し、そのサイトおよびファイルの信頼性を十分検証したうえで行わなければならない。（プログラムのインストールは、第８条に定める禁止事項に該当する）

３．院内の端末からＳＮＳやツイッター、動画共有サイト等の多様なコミュニケーション機能、ファイルアップロード機能、情報の共有機能等を備えたウェブサイトは原則として利用してはならない。ただし、災害発生時等における情報収集、本人の同意を得て行う情報発信等の目的による利用においてはこの限りではない。

４．スマートフォンや個人所有のＰＣ等を利用する場合においても、当院施設および設備、提供される食事等のサービス、職員、患者、家族等の画像および動画をＳＮＳにアップロードすることを原則として禁止する。ただし、災害発生時等における情報収集、本人の同意を得て行う情報発信等の目的による利用においてはこの限りではない。

第１９条（電子メール）

１．電子メールは、インターネット上で盗聴、改ざん、なりすまし等を完全に防止できないものであることを認識し、特に、個人情報を含むファイルを添付する場合は、パスワードの設定を原則とし、個人情報保護に十分配慮しなければならない。

２．お見舞いメールについては、情報管理委員会かつ落合病院広報委員会（以下、広報委員会）またはシステム管理者の許可なく印刷および転送等してはならない。

第２０条（ウェブサイト）

当院ウェブサイト（ウェブサイトを構成する各種ファイル）を、広報委員会またはシステム管理者の許可なく、アップロードおよび削除等してはならない。

制定日　平成１６年１２月　１日
改訂日　平成２３年　２月　１日
令和　元年１２月１６日