

# 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）、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）および医療情報、企業運営等にかかる機密情報。
2. 院内に整備された医事システム、オーダーリングシステム、PACS、文書管理システム、インシデントレポートシステム、イントラネット等のシステムネットワーク、部門に設置された調剤システム、健診システム、透析システム等の部門システムおよび、そのネットワークを構成する周辺機器。
3. 当院ホームページ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（管理者）

1. 当院に、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。（情報管理委員会については、第6条に別途定める）ただし、電子システムの運用管理における実務担当者として、事務部門からシステム管理者が選任され、実務を担当する。
2. システム管理者は、患者の基本情報を提供する医事システム、各部門システムと連携するオーダーリングシステム、各部門間の情報伝達手段であるイントラネット等のシステムネットワークについて、統合的に管理を行う。ただし、各部門に導入された医療機器等と連携する電子システム（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. システム管理者が管理する電子システム  
オーダーリングシステム、医事会計システム（これに付随する再来機システム、カルテ保管システム等を含む）、PACS、インシデントレポートシステム、文書管理システム、病歴

システム、イントラネットシステム、インターネット接続端末等

## 2. 各部門の長が管理するシステム

各部門に導入された業務システム（調剤システム、検査システム、放射線システム等）

### 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. 第4条に定める管理者は、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. 第4条に定める管理者は、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. 第4条に定める管理者は、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なければならない。
4. 第4条に定める管理者は、重大なシステム障害が発生した場合において、復旧に複数の情報処理事業者が関わる電子システムにおいては、速やかに復旧できるように、担当者を決め、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個別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. フロッピーディスク、CD-R、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. 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。
  - 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. 電子情報を不正に削除、改ざんする行為。
  - カ. 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）
  - キ. 院外より院内ネットワークに接続する行為。

- ク、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する行為。(接続許可端末を除く)
- ケ、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。
- コ、その他、法律および公序良俗に反する行為。

#### 第9条（利用者）

1. 第4条に定める管理者は、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、第4条に定める管理者に行う。管理者が適正と判断した場合は、申請にかかる変更等を適用し、情報管理委員会に報告しなければならない。利用者の申請が、第4条に定める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（または委員長より業務を付託された担当者）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。

#### 第11条（バックアップ）

第4条に定める管理者は、電子システム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）

第4条に定める管理者は、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）

第4条に定める管理者は、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（真正性の保持）

第4条に定める管理者は、電子システムおよび電子情報の真正性を保持するため、定期的にハードウェアおよびマスタ等のメンテナンスを行わなければならない。

#### 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. 第4条に定める管理者は、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、また第4条に定める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、情報管理委員会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（導入業者）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、 manifests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、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、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、ファイルを添付する場合は、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）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