(参考) 医療法人〇〇会〇〇病院電子カルテ安全管理規定（事例・抜粋）

1　システム利用者管理手順

（1）システム利用者管理の目的

システム利用者権限は、情報システムを利用する上で、利用資格の識別およびプログラムやデータファイル等への不正アクセスを制御し、データの変更等においてシステム利用者の真正性を高めることを目的とし、システム利用者情報区分によりアクセス権を設定する。

（2）申請・登録・交付・氏名変更・権限失効

① システム利用者権限の交付は、部署の責任者が運用責任者（システム委員会）にシステム利用者の申請書を提出し、カルテ管理委員会の承認を得る。また、システム利用者の異動に伴って総務課またはシステム利用者、部署の責任者から権限失効申請が出た場合、運用責任者（システム委員会）はカルテ管理委員会および監査責任者に報告する。(以下略)

② システム利用者の登録設定・権資産管理（略）

2　データ管理手順

（1）　データの保管方法と場所

電子カルテを中心とした情報システムの医療情報を含むデータおよび機密情報は、施錠管理できるサーバー室内のバックアップ装置に保管し、機密保護を努める。

（2）　データ授受管理手順

電子カルテを中心にした情報システムの医療情報を含むデータおよび機密情報について、データ授受を行う場合は申請書に次の項目を記入し運用責任者（システム委員会）へ提出する。

〇目的、情報資産名称、持ち出し先、返却・消去または破棄方法、返却・消去または破棄予定日、複製物の数

（3）　破棄データ

① 電子記憶媒体の場合

媒体の破棄は、読み取り不能の状態にした後、指定の廃棄場所に破棄する。

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み取り不能にする。

CD・DVD メディア・USB メモリ等…物理的に破壊をして読み取り不能にする。

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、廃棄置き場に破棄する。

3　ドキュメント管理（略）

4　入退室管理（略）

5　情報システム障害対策

（1）　情報システムの障害対応は、運用責任者（システム委員会）がシステム全体の障害対応の詳細について全職員に周知する。

6　ネットワーク管理

（1）　インターネットネットワーク

対外的な情報通信を行うためインターネット・プロトコル技術を利用し世界中にあるネットワークと相互接続されたコンピューターネットワークを院内に構築する。利用の際には、以下の事項を守り利用する。

① 個人情報を含む情報をメールで送受信してはならない。
② メールを院外に自動的に転送してはならない。
③ Web メールやネットディスクなどインターネットを経由して院外のサーバーに個人情報を送受信してはならない。
④ 院内のパソコンを院外からアクセスできる状態にしてはならない。

運用の際には、以下のセキュリティー対策を講じなければならない。

① セキュアネットワークアウトソーシングサービスを利用し、不正アクセス防止、不正通信防止、ウイルス・スパイウェア対策、情報漏えい対策を講じる。

（２） 医療業務用ネットワークの構築

院内の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院内に構築する。

① 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。
② 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さない。
③ 医療情報等の個人データは、院外に持ち出しするノートパソコン、可搬記憶媒体に保存しない。

（３） 個人所有端末のネットワーク接続・外部ネットワーク接続

職員個人が所有する端末のネットワーク接続および外部からネットワークを接続する端末の取り扱いについて以下のとおりとする。

① コンピューターウイルス感染の防止等データ保護のため接続する端末のオペレーションシステムは、運用責任者（システム委員会）が許可したものに限定する。
② 医療情報等の個人データを保存しない。
③ 所定の「個人所有端末利用申請書」で、許可申請を行い運用責任者（システム委員会）が指定した医療情報等の個人データおよび業務データが、端末側にデータを残さないアプリケーションおよび接続方式にて利用を行う。外部接続の際には、データの漏えい、改ざんおよび破壊等を防止するため送信時の暗号化、受信時の復号化する VPN 通信以上のデータの安全かつ適正なセキュリティーの確認が取れた通信回線を用いて以下の接続方式にて行い、すべてシステム利用者識別番号(ユーザ ID)と暗証番号(パスワード)を用いて接続認証を行う。
   - リモートデスクトップ方式、携帯用ゲートウェイ方式、仮想デスクトップ方式、電子署名検証方式

（４） リモート保守回線管理

運用責任者（システム委員会）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。

① リモート保守を行うパソコンには、医療情報等の個人データを保存しない。
② 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わない。
③ リモート保守をできるものは以下の者に限定する。
   - 運用責任者（システム委員会）
   - 病院が契約あるいは依頼したシステム開発会社・コンピューター保守業者

・　上記に関して所定の「院内ネットワークリモート接続利用申請書」を提出し許可の得た回線・端末のみで接続を可能とする。

④　リモート保守状況をログ情報によって定期的にチェックし、システム委員会に報告する。

（５）　ファイル転送用回線管理

運用管理者は、情報システムの保守・運用作業または業務上の理由によりファイル転送プロトコルを使用したファイル転送を行う場合は、ファイル転送の回線を整備する。

①　ファイル転送を行う回線の接続は､作業を行うとき以外行わない。

②　ファイル転送をできるものは所定の「院内ネットワークリモート接続利用申請書」および､「データ授受申請書」にて許可申請を行い運用責任者（システム委員会）が指定した接続方法にて利用を行う。

7　無線 LAN に関する対策

（１）セキュリティー対策

無線 LAN の脅威である｢通信内容の傍受｣､｢無線 LAN の不正利用｣､｢アクセスポイントのなりすまし」等の対策を講じなければならない。

（２）医療機器への考慮

無線 LAN 機器設置および医療機器等設置による動作の影響について留意しなければならない。本院では各種報告書からみて、無線 LAN 設置影響による医療機器等への影響は １ｃｍ以内に近づけた場合を除き影響がないと考える。

8　コンピューターウイルス感染対策

（１）　コンピューター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）　可搬記憶媒体は、コンピューターウイルス対策、暗号化、パスワード認証の機能を兼ね備えた病院指定の媒体を利用する。病院指定以外の可搬記憶媒体を利用する場合は、コンピューターウイルス対策、暗号化、パスワード認証の機能を兼ね備えた媒体を、所定の「外付けデバイス利用申請書」で、許可申請を行い運用責任者（システム委員会）が指定した接続方法・利用方法にて利用を行う。

（３）　病院指定の媒体の管理は、部署の管理者が行わなければならない。業務上の理由により管理本数の追加や破損・故障により交換する場合は、所定の「病院指定可搬記憶媒体使用依頼書」にて依頼をする。

（４）　外部からの持ち込みについて

他施設の可搬記憶媒体を使用した診療情報のデータは、別紙「可搬記憶媒体を使用した診療情報に関する取り扱い手順書(略)」を則って行う。

9　サイバー攻撃

（１）サイバー攻撃（コンピューターウイルスの感染等）を受けた疑いがある場合は、医療情報システムの保守会社に連絡を行う。診療系情報システムの停止や個人情報の流出等の被害等が発生した場合は、厚生労働省へ報告を行う。

（２）サイバー攻撃を受けた際の非常時の対応について、標的型メール攻撃等により医療情報システムがコンピューターウイルス等に感染した場合、以下の対応等を行う必要が生じる場合がある。これらに備え、

関係先への連絡手段や紙での運用等の代替手段を準備する。

①攻撃を受けたサーバー等の遮断や、他の医療機関等への影響波及防止のための外部ネットワークの一時切断。

②他の機器への感染拡大防止や、情報漏えい抑止のための当該感染機器の隔離。

③他の機器への波及調査等、被害確認のための業務システムの停止。

④マルウェア等に感染した場合、バックアップからの重要なファイの復元（重要なファイルは数世代バックアップを取得する）。

（参照：医療情報システムの安全管理に関するガイドライン第５版（2017 年５月）厚労省ホームページ）