松江市立病院　病院情報システムのセキュリティ方針書

1　方針

松江市立病院情報システム（ 以下「病院情報システム」という。）が取り扱う情報は不当に暴かれたり、不当に内容が改ざんされたり、不当に処理が妨害されたりしないように管理及び保護されなければならない。

病院情報システムで処理、保管されているデータに関するいかなる情報も、この病院情報システムに関係のない者には公表しないことを原則とする。

2　目的

病院情報システムのセキュリティ方針書（以下「セキュリティ方針」という。）は、「病院情報システムのデータ保護に関する倫理規程」（以下「倫理規程」という。）と上記の方針に則って、情報の管理や保護のための技術的な対策及びシステムの利用者や管理者への教育の実施等を定めた「セキュリティ・ガイドライン」を定めることを目的とする。

3　修正

情報システム委員会（ 以下「委員会」という。）は、セキュリティ方針に定められた事項について修正の必要が生じた場合には、速やかに見直しをおこなうものとする。

4　適用範囲

セキュリティ方針は、病院情報システムを構成する全ての部分（コンピュータシステムに関連する装置、病院情報システムの運用に携わる人、病院情報システムの利用者等をいう。以下同じ。）に適用する。

特に、個人情報（診療情報等を含む。）を扱う全ての部分に対しては、運用時の必須要件としてセキュリティ方針を適用する。

5　配布

セキュリティ方針は、病院情報システムに関係する全ての者に配布する。

6　委員会

1）　委員会は、情報セキュリティ方針を実施するため、その実施方法について、その評価や問題点などを検討し、情報セキュリティの保護、管理をおこなうとともに、病院内で実施される情報セキュリティ対策に矛盾が生じないよう調整をおこなう。

2）　委員会は、次のような事項を担当する。

（1）　倫理規程にもとづいた情報セキュリティ方針の適切な運用とそれに関する責任についての検討

（2）　情報財産に対する脅威についての監視と予防対策の検討

（3）　院内で発生したセキュリティ事件の検討及び監視

（4）　情報セキュリティを強化するためのイニシアティブ

(5)　セキュリティ対策を実践するための病院長への提言

7　リスク管理

リスク管理は、セキュリティ対策と保護対象となる情報の価値とのバランスを維持するために、下記の点に留意して方針が決定されなければならない。

1)　病院情報システムのセキュリティ上の想定脅威(発生が懸念される不正暴露､改ざん、処理妨害等｡)

2)　想定脅威に対して､その発生が及ぼす損失とそのセキュリティ対策費用及び利便性を考慮した有効な対策とその速やかな実施

8　個人情報保護

病院情報システムが扱う個人情報は、個人情報の保護に関する法律（平成１５年法律第５７号）により保護に努めなければならない。他人の財産を管理し、しかも、一度暴露等の事故が発生すると、取り戻すことができないという情報固有の特性を考え、委託民間企業も含めた病院情報システムに関与するすべての利用者は、その保護に最優先で取り組まなければならない。

9　責任

1)　病院長は、病院情報システムのセキュリティ管理の総括責任を負う。

2)　医療情報システム安全管理責任者（以下「安全管理責任者」という。）は、少なくとも毎年一回､セキュリティ方針及び「セキュリティ・ガイドライン」にもとづいて、病院情報システムのセキュリティ管理状況を調査し、必要に応じて、その内容の見直しを病院長に提言する。

10　セキュリティ管理

病院情報システムのセキュリティ確保のため、以下の管理者・責任者はセキュリティ管理に努めなければならない。

1）安全管理責任者

2）利用者管理者

3）業務管理者

11　責任の分散

セキュリティ管理の責任を分散し、特定の個人に権限と責任が集中して、矛盾を引き起こさないように配慮する。

12　違反者に対する処置

セキュリティ方針を含む運用管理規程の定めた情報セキュリティに違反した者には、ペナルティを科する。

13　診療にかかわる情報へのアクセス

1)　診療にかかわる情報にアクセスできる者は、医師及び関連する医療スタッフとし、

患者による直接アクセスは、おこなえないこととする。ただし、医師の判断により診療にかかわる情報を患者に開示する場合は、医師の責任においておこなうこととする。

なお、診療の準備、症例研究、カンファレンス等の目的で診療にかかわる情報にアクセスする場合も同様に、医師の責任においておこなうこととする。

2） 診療にかかわる情報へのアクセスについては、診療上必要な範囲とし、みだりに不必要な情報にはアクセスしない。

14　電子カルテへのアクセス

1） 通常時の電子カルテへのアクセスは、外来・入院を問わず、受診を希望する旨の根拠となる情報が患者または患者の代理人の意思により表明され、かつ、患者の登録手続きが済まされていなければおこなうことができない。

2） 緊急時の電子カルテへのアクセス

（1） 患者氏名が不詳の場合は、新規に仮の患者番号を採番し、患者登録をおこなう。

（2） 患者番号の採番にあたっては、患者の重複登録にならないよう万全の配慮と、採番後の重複確認をしなければならない。

（3） 患者氏名が確認できた場合で、既に患者番号が存在していたときは、新規に採番した患者番号と既存の患者番号について、その取り扱いを早急に関係部門と調整しなければならない。

15　物理的なセキュリティ管理

自然災害や装置の故障、盗難、破壊等から電子カルテシステムを保護するために以下の対策を実施する。

1） コンピュータ装置本体、ネットワーク管理装置等、病院情報システムの処理に重大な影響を与える装置は盗難や破壊、関係者以外の利用から保護するための物理的な対策を実施する。

2） 全装置の一覧表を維持管理し、不正な持ち出し等が発生しないようにする。

3） システム診断用のハード及びソフト（例えば、プロトコルアナライザーやメモリー用テスター等）の使用は利用目的を限定し、その使用を管理する。

4） ネットワーク回線は、全ての部分で物理的に保護されることとし、定期的に検査する。

5） 電源設備の故障により瞬断や停電の場合でも、無停電電源供給装置（UPS）等の別系統電源供給によって電力の供給を可能とする。

6） 故障または障害の発生により、病院情報システムが正常に稼働できない場合の「病院情報システム障害時対策マニュアル」は、別途定める。

16　情報セキュリティ管理

1） 利用者の識別と認証

（1） 個々の情報に対して、権限を持っている利用者に対して、その権限の範囲内でのみ利用させるようにするため、利用者権限を定め、利用者管理者にて管理する。

（2） 利用者は、利用者番号によって識別し、本人の確認は、パスワードによっておこ

なう。

2) ファイル管理

(1) ファイル（データベース含む。）やプログラムを管理しているシステムあるいは業務上特別な条件下で動作するツール、さらに後利用データベースにおいて患者の個人情報に影響を与えるデータなどは、特別に権限を付与された利用者のみ利用できる。

(2) システム運用関連及びファイル（データベース含む。）管理関連のプログラムやデータの変更は、特別な権限を付与された者のみがおこなうことができる。

(3) 上記の変更については、事前に変更手続きを規定し、その規定に則って実施する。

(4) ファイル（データベース含む。）やプログラム管理しているシステムは、運用中は常時、業務管理者が管理できる状態にしておく。

(5) 利用者は、特別な環境下でない限り、ファイル（データベース含む。）やプログラムを管理しているシステムを、同時に複数の端末からは利用できない。

(6) 利用されるソフトウェアは、ライセンス契約に準拠したものであることが保証できるようにしておく。

3) ネットワークセキュリティ管理

(1) ネットワークの利用及びネットワークの構成の登録・変更には、事前の手続きを規定し、その規定に則って実施するようにする。

(2) 内部ネットワークから部門システム等を介して外部と通信する場合（リモートメンテナンスなど。）には、院外のリモートメンテナンス端末の管理方法も把握して許可を与えなければならない。

(3) 院内の外部ネットワークは、内部ネットワーク（業務で使用するサーバ及び端末が接続されたネットワーク）と当面接続しないものとする。

(4) 特に許可された者以外は、院外回線を通じて内部ネットワークを利用できない。

(5) 各部門システムを通じて直接院外の回線を結びつけてダイアルアップネットワークを構築する場合は、必ずその機能に関する仕様書を委員会に提出し、定期的にその安全性の維持について通信ログを報告しなければならない。

(6) 個人情報に関係するような重要なデータをネットワーク上で使用する場合は、ネットワーク環境がセキュリティの確保上完全ではないことを考慮した上で使用しなければならない。

4) 分散管理

(1) 部門サーバ間のセキュリティレベルを統一する。

(2) 部門サーバ間で一貫したセキュリティ属性の解釈がおこなえるように管理する。

5) 電子メール管理

(1) プライバシーに関係するような重要データを、電子メールで送信する場合は、その送信方法について考慮されなければならない。

(2) メール発信者、メール内容、メール受信者についての許可範囲は、「利用者マニュアル」に明確に定め成文化しておくこと。

6) 管理

(1) 利用者管理者は、情報セキュリティの管理のため、管理情報を収集し、それらを

管理し、その結果を安全管理責任者に報告する。

(2) 安全管理責任者は、常に第三者的立場を堅持して公正にシステムの不正あるいは改ざんあるいは混同の存在について指摘しなければならない。

(3) 管理情報には、利用者（利用者番号)、利用場所、日時、アクセスした資源名、利用事象のタイプ、アクセスの可否結果を記録しておく。

(4) 管理情報が収められているファイルは、保護されなければならない。

(5) 利用者管理者は、管理情報を少なくとも週 1 回、チェックする。

(6) 違反に関する管理記録は、少なくとも 60 日間は保存しておく。

(7) 管理ツールの使用は、安全管理責任者及び利用者管理者に限る。

7) データ保全とウィルス対策

(1) 利用者が持ち込むデータや、システム運用に直接関連するプログラム等重要なプログラムを扱う場合には、利用前にウィルスチェックを実施する。

(2) ウィルス対策プログラムは、全ての端末に配置しておく。

(3) 利用者は、使用中にウィルス感染の疑いが生じた場合は、利用者管理者に報告する。

(4) 利用者管理者は、障害の状況を分析しウィルスが確認された場合は、安全管理責任者へ報告した後、その旨を全利用者に通知して注意を喚起し、同時に病院長に報告しなければならない。

(5) メディアの管理は、業務管理者が管理する。

8) 法的に使用される情報の管理

(1) 法的に使用される電子カルテ情報は、その真正性を確保するように講じられていること。

(2) 法的に使用される電子カルテ情報の真正性は、操作をおこなう者の利用者番号とパスワードで認識させ、確定情報は、確定入力を動機付けできる画面で構成し、その修正は原本を保存しながら修正データが見読できるように設計されていること。

(3) 法的に使用される電子カルテ情報は、法的に求められる期間中保存でき、機器等の新調によるデータの互換性は保持できるように講じてあること。

(4) 法的に使用される電子カルテ情報を、保存及び出力するシステムは、法的に求められる期間内は、常に稼動できる状態にしておくこと。

(5) 法的に使用される電子カルテ情報の所在を明確にし、法的保存期間の情報の開示を求められた場合、速やかに開示できるようにすること。

(6) 文書での保存が法的に必要な情報は、その法的根拠が保たれる状態で保存しなければならない。

17 運用管理

1) 運用管理

(1) 病院情報システムは、運用管理規程にもとづき運用されるとともに、以下の条件に従って適切に管理されなければならない。

(2) システムが災害にあった場合の対処方法と復旧方法について手順を明確にし、必

要に応じて委員会で見直しを実施すること。

(3) システムのバックアップを頻回に実施するとともに、バックアップ媒体は、サバー室設置の通常バックアップとランサムウエア対策バックアップサーバーに保管する。

(4) 機密性の高いバックアップデータは、暗号化するなどして厳重に保管されること。

(5) 可搬媒体（テープ、ディスク、カセット及びプリントしたレポート等。）に関する管理手順を明確にし、利用者に遵守させること。

(6) システム資源の容量を定期的に確認し、容量不足が予想される場合には速やかに対処すること。

2) システム管理

(1) 利用者の本人確認は、システムの利用を開始する時点で実施する。

(2) 不正なシステム利用は、許可しない旨のメッセージを表示する。

3) 作業手順書

システムの運用を適切に管理するために、「管理者マニュアル」及び「利用者マニュアル」のほかに、障害時業務継続手順として「病院情報システムダウン対策マニュアル」を定めるものとする。

18 スタッフセキュリティ

1) 外部委託管理

(1) 病院情報システムを利用することのできる職員を雇用する委託企業は、職員に十分な利用者教育をおこなわなければならない。

(2) 病院情報システムの利用者は、守秘義務と同時に、部門システムと病院情報システムの関係を熟知して、部門システムに対する院外からのアクセスに注意を払わなければならない。

(3) 部門システムに院外アクセスを持つ委託企業は、その構造について委員会の許可を得なければならない。

(4) 部門システムは、部門内でログ管理をし、定期的に、定められた内容で委員会に報告しなければならない。

(5) 委託契約の締結に際しては、契約上に職員の病院情報セキュリティに関する項目を盛り込まなければならない。

2) 教育・訓練

(1) 病院情報システムの利用者は、病院情報システムの利用を許可される前にセキュリティ方針及びセキュリティ対策、運用の教育を受けなければならない。

(2) 利用者は、1 年に一度、セキュリティ方針及びセキュリティ対策の研修を受けなければならない。

(3) 教育内容には、以下の項目が盛り込まれなければならない。

ア 病院情報システムの利用者に対する教育

・ セキュリティ侵害や情報の漏洩が何によって起きるかを含めた、個人情報保護、機密性、完全性、可用性、情報公開及び情報セキュリティの概念

・ 個人情報保護、機密性及びセキュリティに影響を与える情報技術

・ 利用者のセキュリティ管理における個人の責任及び立場による責任範囲の違い
・ 診療情報の重要性と、その利用者及び使用用途
・ 利用者情報の重要性
・ 情報セキュリティに対する想定脅威の種類
・ データ保護の方式
・ 情報セキュリティ違反の重大さとペナルティ
・ セキュリティに対する定期的な評価と改良

イ　業務管理者に対する教育

初めて業務管理者になった者に対する教育は、利用者に対する教育に加えて以下の項目を履修しなければならない。

・ 情報セキュリティ教育のプログラムを確立するための管理責任
・ 情報セキュリティ方針とその実践を実現、監視、評価するための戦略
・ 全ての利用者に対する情報の取扱い方法・内容
・ 情報セキュリティに影響を与える新技術や、セキュリティ計画に影響を与える規制・規則について熟知する責任
・ 利用者への適切なインセンティブや報奨を与えること
・ 不適切な情報の漏洩によって発生する法律上の要件やペナルティ
・ セキュリティに対する侵害時の一貫した対応と訓練

(4)　病院情報システムを利用するすべてのスタッフは、安全管理責任者が開催する情報セキリティ研修を受けなければならない。

3)　アクセスログの開示

個人情報保護のため、申請により、病院情報システムの保有する申請者の個人情報について、利用者のアクセスログを開示する。

附　則

1．この方針書は、平成 17 年 8 月 1 日から施行する。
2．この方針書に定める事務は、情報システム委員会が所掌する。
3．事務局は、資産経営課情報システム係に置く。

平成 18 年	4 月	1 日	改訂
平成 21 年	4 月	1 日	改訂
平成 22 年	4 月	1 日	改訂
平成 27 年	12 月	15 日	改訂
平成 28 年	4 月	1 日	改訂
平成 29 年	10 月	1 日	改訂
令和 3 年	7 月	1 日	改訂
令和 5 年	4 月	1 日	改訂
令和 6 年	4 月	1 日	改正