海南医療センター情報セキュリティ規則

第１章　　総　　則

（目的）

第１条　　この規則は、海南医療センター（以下「当院」という。）における情報セキュリティ対策を実施するために必要となる統一的な基準を定めることにより、医療情報を適切に保護することを目的とする。

（定義）

第２条　　この規則において、使用する用語の定義は、規則で使用する用語の例によるほか、それぞれ当該各号に定めるところによる。

（１）　職員　　当院の業務に常時勤務する者をいう。

（２）　サーバ等　　情報資産のうち、サービスを提供するコンピュータ及びホストコンピュータをいう。

（３）　情報端末　　情報資産のうち、サーバ等からのサービスの提供を受けるコンピュータをいう。

（４）　管理者権限　情報システムを管理するために必要なアクセス権限をいう。

（５）　システム管理者　医療情報システムの安全管理に関するガイドラインに規定するシステム運用担当者を指す。

第２章　　組　　織

（医療情報システム安全管理責任者）

第３条　システムの適切な運用を管理する医療情報システム安全管理責任者を置く。

２　医療情報システム安全管理責任者は、副院長の職にあるものをもってあてる。

３　医療情報システム安全管理責任者は、当院におけるすべての情報資産に対する情報セキュリティ対策を企画管理者と共に総括する。

（企画管理者）

第４条　　組織体制や情報セキュリティ対策に係る運用を管理する者として、企画管理者を置く。

２　　企画管理者は、事務長の職にあるものをもってあてる。

３　　企画管理者は、当院におけるすべての情報資産に対する情報セキュリティ対策を医療情報システム安全管理責任者と共に総括する。

４　　企画管理者は、第８条に規定するシステム運用委員会の主導により、職員等に対し個人情報保護に関する教育・訓練・研修を実施する。

（システム管理者）

第５条　　医療情報システムにおける端末及びネットワーク並びにその接続機器に関する管理を行うシステム管理者を置く。

２　　システム管理者は、医療情報システム安全管理責任者が任免する。
３　　システム管理者は、医療情報システムに障害が発生した場合の問題解決と医療情報システム安全管理責任者への報告を行う。

（部門責任者）
第６条　　前条に規定するシステム管理者の業務を補佐する者として、各診療部門にそれぞれ部門責任者を置く。
２　　部門責任者は、各診療部門からそれぞれ１名を選出し、システム管理者の承認を得て決定するものとする。ただし、選出の申告がない場合は部門の所属長とする。
３　　部門責任者は、医療情報システムに障害が発生した場合の問題解決とシステム管理者への報告を行う。

（監査責任者）
第７条　　医療情報システムの運用を監査する監査責任者を置く。
２　　監査責任者は、院長が指名する。
３　　監査責任者は、定期的に医療情報の運用に関する監査を行い、監査結果を医療情報システム安全管理責任者に報告する。
４　　医療情報に関する監査を外部に委託する場合は、医療情報システム安全管理責任者の許可を得なければならない。

（システム運用委員会）
第８条　　システムの安全・合理的な運用を図るため、システムの運用管理に関する事項を審議する場として、システム運用委員会を置く。委員会の所掌事務及び組織等の運営に必要な事項は、別に定める。

第３章 情報セキュリティ

(総合的な推進及び調整)
第９条　　当院における情報セキュリティ対策の総合的な推進及び調整は、医療情報システム安全管理責任者が行う。
２　　医療情報システム安全管理責任者は、次に掲げる事項を統括する。
（１）　情報セキュリティに関する組織横断的な調整に関する事項
（２）　情報セキュリティに関する事案の調査又は監査に関する事項
（３）　その他情報セキュリティに係る重要事項に関する事項

(情報の分類)
第１０条　　企画管理者は、すべての情報を適切に取扱い、かつ保護するために、重要性分類に基づき分類しなければならない。

(情報の管理)

第１１条　企画管理者は、所管する情報に関し、責任をもって適正に管理しなければならない。

２　　職員は、重要情報外部へ送付又は持ち出しをしてはならない。ただし、医療情報システム安全管理責任者が業務上特に必要と認めた場合は、この限りではない。

３　　医療情報システム安全管理責任者及び企画管理者は、所管する重要情報が複製された場合、当該情報の所在を明確にしておかなければならない。

(職員の役割及び責任)

第１２条　職員は、情報セキュリティ対策の実施にあたり、次に掲げる役割及び責任を有する。

（１）　規則及び規程に定められている事項を遵守すること。

（２）　規則及び規程について不明な点及び遵守することが困難な点がある場合は、速やかに医療情報システム安全管理責任者及び企画管理者に報告し、指示等を仰ぐこと。

（３）　情報端末を業務目的以外に使用しないこと。

（４）　病院診療情報を業務目的以外に閲覧及び持ち出し利用しないこと。

（５）　不適切な情報の発信、他人の利用 ID 又はパスワードを使う行為、及び利用を許可されていないサーバへのアクセス等、自らが加害者になる行為を行わないこと。

（６）　施設内 LAN 又は情報システムに有害なプログラムを使用し、又は提供する等、施設内 LAN、情報システム若しくは他の職員に損害を与え、又は与えるおそれのある行為を行わないこと。

（７）　個人のプライバシーを侵害する行為を行わないこと。

（８）　その他規程で定める事項を遵守すること

(法令等の遵守)

第１３条　職員は、情報資産の使用において、関係法令及び使用するソフトウェアの使用許諾契約を遵守しなければならない。

(パスワードの管理)

第１４条　職員は、自己の保有するパスワード(以下「パスワード」という。)　を、他の者に不正使用されないよう、次に掲げるとおり、厳重に管理しなければならない。

（１）　パスワードを秘密にしておくこと。

（２）　パスワードのメモを作成した場合は、他の者の目に触れることがないよう適切に管理すること。

（３）　パスワードは、英数字、記号が混在した８文字以上とすること。

（４）　パスワードの設定には、推測されやすいものを使用しないこと。

（５）　パスワードは、定期的に変更するようにすること(職員がパスワードを変更できないものを除く。)。

（６）　情報端末にパスワードを記憶させないこと。

２　その他必要な事項に関しては、別に定める。

（個人所有機器の使用禁止）

第１５条　職員は、重要情報の漏えい及びコンピュータウイルスの感染等を防止するため、個人が所有する情報端末を持ち込み、業務に使用してはならない。

２　職員は、前項の規定にかかわらず、業務上特別の理由がある場合には、情報の漏えい及びコンピュータウイルスの感染等を防止するための措置を講じて、システム管理者の許可を得て情報端末を持ち込み、業務に使用することができる。ただし、施設内 LAN に接続してはならない。

３　前項の場合において、事前にシステム管理者に報告し許可を得なければならない。

（業務に利用するソフトウェア）

第１６条　職員は、情報端末の誤動作、コンピュータウイルスの感染等を防止するため、定められたソフトウェア以外のソフトウェアを情報端末に導入してはならない。

２　職員は、前項の規定にかかわらず、システム管理者が業務上特に必要と認める場合は、定められたソフトウェア以外のソフトウェアを情報端末に導入することができる。

３　前項の場合において、事前にシステム管理者の許可を得なければならない。

（情報端末環境の変更）

第１７条　職員は、情報端末の誤動作、保守の困難化等を防止するため、情報端末に対し、設定の変更、情報端末の改造及び周辺機器の増設を行ってはならない。

２　職員は、前項の規定にかかわらず、システム管理者が業務上特に必要と認める場合は、設定の変更及び周辺機器の増設を行うことができる。

３　前項の場合において、事前にシステム管理者の許可を得なければならない。

４　職員は、ネットワーク機器の設定を変更してはならない。

（職員によるコンピュータウイルス対策）

第１８条　職員は、情報端末へのコンピュータウイルス感染を防止するため、次に掲げる事項を遵守しなければならない。

（１）　記録媒体、電子メール等によりデータ又はソフトウェアを外部から取り入れる場合又は外部にデータを送付する場合は、必ずコンピュータウイルスチェックを行うこと。

（２）　システム管理者が提供するコンピュータウイルスに関する情報及び指導を常に確認し、その情報及び指導に従い必要な措置を講じること。

（３）　コンピュータウイルス対策ソフトウェアの設定を許可なく変更しないこと。

（４）　コンピュータウイルスが発見された場合は、直ちに情報システムの利用を中止し、システム管理者に報告するとともに、指示に従うこと。

（５）　その他規程で定める事項を遵守すること。

（離席時の情報端末設定）
第１９条　職員は、情報漏洩及び不正操作を防止するため、離席するときは、パスワード入力が必要な画面に戻す等、情報システムの業務内容及び機能に応じて適切な対策を講じなければならない。

（情報セキュリティに関する啓発及び周知）
第２０条　医療情報システム安全管理責任者及び企画管理者は、システム管理者と共同して、職員に対し情報セキュリティについての啓発を行わなければならない。
２　医療情報システム安全管理責任者及び企画管理者は、システム管理者と共同して、所属する職員に対して、情報セキュリティに関する周知を行い、その徹底を図らなければならない。

（臨時職員、外部委託事業者等に対する指導）
第２１条　医療情報システム安全管理責任者及び企画管理者は、臨時職員、外部委託事業者等に情報資産を取り扱わせる場合は、規定、この規則及び実施手順の内容を遵守させる等取扱いに関する適切な指導を行わなければならない。

（事務局の管理）
第２２条　総務、人事、経理事務等を行う場所（以下「事務局等」という。）　の施設に関する警備、施錠等の物理的情報セキュリティ対策は、施設の管理責任者及び医療情報システム安全管理責任者並びに企画管理者が行わなければならない。
２　職員は、盗難防止のため、事務局等に配置した情報端末について、施錠可能な保管庫又は什器等に収納できるものは、業務が終了した時点で収納し厳重に保管しなければならない。
３　職員は、第三者に情報を閲覧されることがないようにしなければならない。
４　職員は、情報端末及び記録媒体について、第三者に使用されないよう管理しなければならない。

（機器の取付け等）
第２３条　システム管理者は、サーバ等、情報端末及びネットワーク機器（以下「機器」という。）　を設置する場合、機器の安定稼動を確保し、かつ機器の損傷、配線の損傷及び物理的な不正アクセスを防止するための措置を講じなければならない。

（サーバ等の設置）
第２４条　システム管理者は、サーバ等を設置する場合、設置場所における情報セキュリティ対策について次に掲げる事項について調査し、医療情報システム安全管理責任者並びに企画管理者と協議の上、当該設置場所についての許可を得なければならない。
（１）　地震・火災などに対する対策がなされているか。
（２）　電源に対する対策（停電対策等）がなされているか。

（３）　適切な空調がなされているか。
（４）　権限のない者が容易にアクセスできないようになっているか。
（５）　重要情報が含まれる場合、情報の漏えい対策がなされているか。
（６）　障害発生を検知する対策がなされているか。
（７）　職員が運用状況を確認することができるか。
（８）　ネットワークを使用する場合、ネットワークの安全性は確保されているか。

（記録媒体の管理）
第２５条　職員は、重要情報の盗用、漏えい、紛失及び破損等を防止するため、記録媒体について、次に掲げるとおり、適切な管理を行わなければならない。
（１）　記録媒体を磁気、熱及び光等に影響されない場所へ保管すること。
（２）　重要情報が記録された記録媒体を施錠可能な場所へ保管すること。

（記録媒体の廃棄）
第２６条　職員は、重要情報を記録した記録媒体を廃棄するときは、情報の漏えいを防止するため、物理的に破壊する等情報を復元できないように対処した上で廃棄しなければならない。

（出力物の管理）
第２７条　企画管理者は、情報システムにおける情報が記載された紙等のうち、重要情報が記載されたものについては、情報の盗用、漏えい等を防止するため、次に掲げるとおり厳重に管理しなければならない。
（１）　第三者が閲覧できない場所に保管すること。
（２）　保管場所は、施錠可能な棚又は部屋とすること。
（３）　離席及び退勤する場合は、不正な侵入等から情報資産を保護するため、施錠しなければならない。
（４）　廃棄する場合は、内容が確認できないようにすること。

（外部への記録媒体及び機器の持ち出し）
第２８条　職員は、重要情報の盗用、漏えい、紛失、破損等を防止するため、記録媒体及び機器を外部に持ち出してはならない。
２　前項の規定にかかわらず、職員が第１１条第３項ただし書の規定により重要情報を含む記録媒体又は機器を外部に持ち出すときは、医療情報システム安全管理責任者は、持ち出し及び返却の日時、従事職員、記録媒体の種類又は機器の種類、記録されている情報内容、外部での管理方法等を記録するとともに、持ち出した記録媒体又は機器を厳重に管理しなければならない。
３　職員は、外部に持ち出した記録媒体又は機器を紛失したときは、直ちに情報セキュリティに関する事案への対応に従って医療情報システム安全管理責任者に報告を行わなければならない。

（アクセス制御）

第２９条　医療情報システム安全管理責任者は、情報の盗用及び漏えい並びに不正なアクセス等を防止するため、所管するサーバ等のアクセス権限を明確にし、アクセス権限に基づくアクセス制御を行わなければならない。

（管理者権限）

第３０条　医療情報システム安全管理責任者は、サーバ等の不正な使用、情報の盗用及び漏えい等を防止するため、サーバ等の管理者権限を必要最小限の職員に与え、管理者権限によるサーバ等へのアクセスを必要最小限とするよう指導するものとする。

（利用者 ID 等の管理）

第３１条　システム管理者は、所管する情報システムの利用者 ID を適切に管理し、サーバ等へのログインに関して、不正なログインを防止するため、利用者 ID の設定及びパスワードの設定等の対策を講じるものとする。

（アクセス記録等の取得）

第３２条　システム管理者は、情報システムの不正な使用、改ざん等を防止するため、情報システムにおけるアクセス記録等の取得及び管理を行うものとする。

（障害記録）

第３３条　システム管理者は、情報システムの障害に対する処理について、障害の発見及び発生の日時、障害の発生箇所、障害の種別（ハードウェア障害・ソフトウェア障害・その他）、障害の内容、障害の原因、被害の範囲、障害の対応内容、復旧の日時、再発防止の手順等を障害の実状にあわせて体系的にセキュリティ事故報告書に記録し、これを必要なときに活用できるよう管理を行うものとする。

（バックアップ）

第３４条　システム管理者は、サーバ等に記録された情報について、障害、破損等に備えて日次、週次、月次、情報更新時等情報システムの業務内容及び保有する情報の重要度に応じ、あらかじめバックアップを行う周期及び保管期間を決定した上で定期的に必要なバックアップを行わなければならない。

（情報システムの監視）

第３５条　システム管理者は、情報セキュリティに関する事案を検知するため、必要に応じて、サーバ等情報システムの稼動状態の監視を行うものとする。

（標準ソフトウェア）

第３６条　システム管理者は、情報端末の誤動作及びコンピュータウイルス感染等を防止するため、情報端末において利用するソフトウェアを定めるものとする。

（ネットワークの通信制御）

第３７条　システム管理者は、サーバ等及びネットワーク機器における不正使用を防止するため、ネットワークに関する通信制御を医療情報システム安全管理責任者と協議の上、行わなければならない。

（ネットワークの安全性確保）
第３８条　システム管理者は、施設内 LAN について情報を安全かつ確実に伝送するための対策を講じなければならない。

（施設内 LAN への接続）
第３９条　システム管理者は、施設内 LAN にサーバ等、情報端末、ネットワーク機器等を接続する場合、事前に医療情報システム安全管理責任者の許可を得なければならない。

（施設内 LAN の情報システム利用）
第４０条　システム管理者は、施設内 LAN を利用して新たな情報システムを開発又は導入しようとするときは、事前に医療情報システム安全管理責任者と協議しなければならない。

（外部との接続）
第４１条　システム管理者は、施設内 LAN 及びサーバ等に外部からアクセスする仕組みを構築する場合、管理する区域から専用回線又はインターネット等を通じて、外部に設置した情報システムにアクセスする仕組みを構築する場合又は施設内 LAN 以外（以下「外部ネットワーク」という。） との接続を行う場合は、情報セキュリティ技術面について、施設の管理者及び医療情報システム安全管理責任者と協議をした上で、許可を得なければならない。
２　システム管理者は、外部ネットワークとの接続を行った場合、適切な情報セキュリティ対策及び運用管理を行わなければならない。

（無線ネットワークの使用）
第４２条　システム管理者は、無線ネットワークを使用する場合、事前に医療情報システム安全管理責任者の許可を得なければならない。
２　システム管理者は、無線ネットワークの使用において、接続する情報端末及び利用者の認証を確実に行わなければならない。

（システム管理者によるコンピュータウイルス対策）
第４３条　システム管理者は、コンピュータウイルスによる被害を防止するため、所管する情報システムにおけるコンピュータウイルス対策に関し、次に掲げる事項を実施しなければならない。
（１）　コンピュータウイルス対策の実施状況を医療情報システム安全管理責任者の求めに応じて報告すること。
（２）　サーバ等におけるコンピュータウイルスチェックの実施状況を確認するこ

と。
（３）　コンピュータウイルスチェックのためのパターンファイルは、常に最新のものに保つこと。
（４）　コンピュータウイルスが発見された場合は、定めた実施手順に従い対応を行った後、被害の有無にかかわらず、医療情報システム安全管理責任者へ報告を行うこと。
（５）　職員に対し、企画管理者と共に、コンピュータウイルス対策に関する啓発を行うこと。

（情報システムの調達）
第４４条　医療情報システム安全管理責任者は、情報システムを調達する場合、調達に関する仕様書類の記載内容が情報セキュリティを確保する上で問題にならないよう留意しなければならない。
２　医療情報システム安全管理責任者は、機器及びソフトウェアを調達する場合、当該機器及びソフトウェアが情報セキュリティを確保する上で問題にならないかどうか確認しなければならない。

（仕様書類の管理）
第４５条　医療情報システム安全管理責任者は、情報システムへの不正なアクセス等を防止するため、所管する情報システムに関するシステム設計書、操作手引書等の仕様書類を適切に管理しなければならない。
２　医療情報システム安全管理責任者は、所管する重要な情報システムの追加、変更及び廃棄等を行った場合、仕様書類を最新に更新し、必要に応じて履歴を管理するものとする。

（情報システムの開発、導入及び保守）
第４６条　医療情報システム安全管理責任者は、情報システムの開発、導入及び保守における事故並びに不正行為対策のため、次に掲げる事項を遵守しなければならない。
（１）　情報システムの開発、導入及び保守の責任者を定めること。
（２）　情報システムの開発、導入及び保守の作業者及び作業範囲を明確にすること。
（３）　情報システムの開発、導入及び保守に関する作業手順を明確にすること。
（４）　開発、導入する情報システムは、本番運用している情報システムの正常稼動に影響を及ぼさない措置を講じること。
（５）　開発、導入及び保守を行う場合、情報セキュリティ上の問題となるおそれがあるソフトウェアを使用しないこと。
（６）　開発、導入及び保守の際のアクセス制限を明確にするとともに、使用した利用者 ID 及びパスワードは不要となった時点で速やかに削除すること。
（７）　機器の搬出入を管理すること。
（８）　開発、導入及び保守の記録をとること。

（９）　機器等については、適切な保守を行い、障害に備えること。

２　医療情報システム安全管理責任者は、前項の作業を外部委託事業者に委託する場合は、外部委託事業者に作業事前協議書及び作業報告書を提出させて、前項各号を満たしているかどうかを確認しなければならない。

３　その他必要な事項に関しては、別に規程で定める。

（ソフトウェアの保守及び更新）

第４７条　医療情報システム安全管理責任者は、情報セキュリティに影響を及ぼすソフトウェアの不具合について修正等を行う場合、情報システムに影響を与えないかどうかを調査した上で、速やかに必要な保守又は修正プログラムの適用によるソフトウェアの更新を実施しなければならない。

（機器の修理、廃棄及び返却）

第４８条　医療情報システム安全管理責任者は、機器を修理及び廃棄する場合並びに借用した機器を返却する場合、重要情報の盗用及び漏えいを防止するため、機器に保存されている情報の消去等を行い、当該情報が復元不可能な状態にしなければならない。ただし、当該契約において守秘義務及び情報セキュリティ対策について明記されている場合は、この限りではない。

（委託契約書への記載事項）

第４９条　医療情報システム安全管理責任者は、情報システムの開発、運用及び保守等を外部委託事業者に委託する場合、委託に係る契約書に次に掲げる事項を明記しなければならない。

（１）　規程及びこの規則の遵守に関する事項

（２）　業務上知り得た情報の守秘義務に関する事項

（３）　再委託の禁止又は制限に関する事項

（４）　情報及び関連資料の第三者への提供の禁止並びに目的外の使用の禁止に関する事項

（５）　情報及び関連資料の取扱う者の限定並びに複写及び複製の禁止並びに厳重な保管及び返還に関する事項

（６）　情報及び関連資料の搬送に関する事項

（７）　記録媒体及び情報端末の取扱いに関する事項

（８）　従業員に対する情報セキュリティ教育の実施に関する事項

（９）　事故発生時の報告義務、履行状況の報告及び立入調査に応ずる義務

（１０）　契約に違反した場合における即時の返却義務及び契約解除時の措置

（１１）　契約に違反した場合における損害賠償に関する事項

（外部委託事業者の管理状況等の調査）

第５０条　医療情報システム安全管理責任者は、委託契約履行中の外部委託事業者に対し、必要に応じて当該委託に係る情報セキュリティ対策の実施状況について調査するものとする。

（情報セキュリティに関する情報の収集）

第５１条　医療情報システム安全管理責任者は、情報セキュリティに関する事案が発生した場合に迅速かつ円滑に対処するため、情報セキュリティ技術の向上及び情報セキュリティに関する事案発生時の対応方法等に関する情報について、収集を行うものとする。

２　医療情報システム安全管理責任者は、緊急度の高い情報又は職員にとって必要な情報は、速やかに職員に周知するものとする。

３　医療情報システム安全管理責任者は、前項に規定する情報のほか担当する情報システムに関する情報収集に努め、適正な情報セキュリティ対策に役立てるものとする。

（情報セキュリティに関する事案への対応）

第５２条　職員は、情報セキュリティに関する重要な事案が発生した場合は、報告、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるため、次に定める手順により対応しなければならない。

（１）　情報セキュリティに関する事案を認めた者は、事案の発生時間、発生箇所、発生内容、想定される原因、被害の範囲等を把握して、直ちに医療情報システム安全管理責任者に報告する。

（２）　前号の報告を受けたシステム管理者は、発生した情報セキュリティに関する事案に対して証拠保全、被害拡散防止等必要な対応を行うとともに、医療情報システム安全管理責任者に報告する。

（３）　前号の報告を受けた医療情報システム安全管理責任者は、当該事案にかかわる施設内 LAN への被害拡散防止、復旧、証拠保全等の必要な措置並びに情報システム停止及び利用停止等の必要な指示を行うとともに、事案のレベルに応じて、対応する。

（４）　システム管理者は、医療情報システム安全管理責任者の指示に基づき、当該事案に係る再発防止の暫定措置を実施した後、情報システムを復旧する。

（５）　システム管理者は、当該事案の発生原因、対応方法、被害状況を分析し、必要に応じて医療情報システム安全管理責任者と協議の上、再発防止策を作成し、システム運用委員会に報告し、その承認を得る。

２　医療情報システム安全管理責任者は、情報セキュリティに関する事案の発生に備え、センター全体に係る緊急時対応及び緊急時連絡網を整備しなければならない。

３　医療情報システム安全管理責任者は、所管する情報システム等に係る緊急時対応計画及び緊急時連絡網を整備しなければならない。

（点検）

第５３条　医療情報システム安全管理責任者は、情報セキュリティ対策が適切に行われていることを確認するため、所管する情報システムの運用状況について点検を行うものとする。

（実施手順の見直し）
第５４条　医療情報システム安全管理責任者は、調査及び点検の結果等を踏まえて実施手順の実効性を評価し、見直しが必要な場合は、速やかに実施手順を改正しなければならない。

（整備）
第５５条　この規則に基づく実施手順又は具体的な対策については、各情報資産の運用状況等に合わせて検討を行い、情報システム毎に必要なものから速やかに整備することとする。

（改廃）
第５６条　この規則の改廃はシステム運用委員会の決議による。

（その他）
第５７条　この規則に定めるもののほか、必要な事項に関しては別に定める。

附　則

この規則は、平成２５年３月１日より施行する。

附　則

この規則は、令和４年３月１日より施行する。

附　則

この規則は、令和６年１２月１日より施行する。