情報セキュリティ基本方針

東海記念病院

改訂履歴

2013 年 05 月 17 日　作成
2016 年 12 月 01 日　改訂
2018 年 09 月 05 日　改訂
2023 年 07 月 06 日　改訂

2013 年 05 月 17 日　作成
2023 年 07 月 06 日　改訂

情報セキュリティ方針　1p

東海記念病院（以下、「当院」という）は、患者様の満足と信頼を第一に考え、当院のサービスを通じて知り得た患者様の情報及び当院が保有する情報システム及び情報資産を不正アクセス、過失及び災害などの様々な脅威から保護・管理することを重要な責務だと認識し、ここに『情報セキュリティ基本方針』を定めます。
当院は『情報セキュリティ基本方針』をトップマネジメント及び全ての従業員、更には当院及び協力会社関係者を含めて周知徹底し、継続的な情報セキュリティ対策への取り組みに務めます。

（適用範囲）
　当院が運用する“情報資産”を対象とします。情報資産とは、当院が保有又は運用管理するデータ及び情報システム、ネットワーク機器、更には患者様からお預かりした情報資産を含むものとします。

（情報セキュリティ体制の確立及び維持）
　当院はトップマネジメントを中心として情報セキュリティマネジメントシステムの体制を確立し、情報セキュリティの維持、向上の取組みを行うものとします。また、これらの取組みは定期的に監査し、改善に努めます。

（情報資産の保護）
　情報資産への不正なアクセスや、漏洩、改ざん、紛失等を予防し、安全かつ適正な情報管理体制のもと適切な情報資産の保護に努めます。

（業務委託先の情報保護管理体制）
　当院が管理する業務委託先に対して、適格性を十分に審査し、当院と同等以上のセキュリティレベルを維持するよう要請していきます。また定期的に監査及び見直しをして、これらのセキュリティレベルが継続的に維持されるように管理を行っていきます。

（法令・契約要求遵守）
　当院は情報セキュリティに関する法令、患者様との契約、その他の規範及びガイドラインを遵守します。

（教育・訓練）
　当院は、情報セキュリティの意識向上を図るために従業員に対し情報セキュリティに関する教育・訓練を定期的に行います。

（事故の対応）
　当院は、情報セキュリティ事故の防止に努めるとともに、万一、事故が発生した場合には、速やかに再発防止策を含む適切な対策を講じます。

（改善及び計画）

2013 年 05 月 17 日　作成
2023 年 07 月 06 日　改訂

情報セキュリティ方針　2p

当院は本方針の変更、社会情勢の変化、技術的変化、法令等の変更などに伴い、継続的に情報セキュリティの見直し及び改善を図ります。

（情報セキュリティ対策の推進体制）
東海記念病院における情報セキュリティ対策については、次に掲げる職員又は組織により管理及び推進を行うものとし、その職務内容は次に定めるとおりとする。
（１）最高情報統括責任者（CIO）
東海記念病院における全ての医療情報システム、情報資産及び情報セキュリティ対策に関する最終決定権限及び責任を有する最高責任者とし、院長をもってこれに充てる。
（２）情報統括管理者
東海記念病院における情報セキュリティ対策に関する適正な運用を管理し、情報管理者を統括する。情報課長をもってこれに充てる。
（３）情報管理者
医療情報システムの運用、システム保全、情報資産に関する管理責任者とし、情報課の所属職員をもってこれに充てる。
（４）情報担当者
各部署の情報セキュリティ対策に関する推進担当者とし、医療情報システム委員をもってこれに充てる。
定期的にセキュリティ状況の報告・確認を行う。必要に応じてセキュリティ対策の検討や課題の検討を行う。
（６）医療情報システム委員会
定期的にセキュリティ状況の報告・確認を行う。必要に応じてセキュリティ対策の検討や課題の検討を行う。
東海記念病院における医療情報システムの運用検討、情報セキュリティ対策の推進等を目的として設置されたもので、情報セキュリティポリシーの策定及び変更に関する審議等を行う。
（７）幹部会議
東海記念病院における最高決定機関であり、医療情報システム委員会の審議事項について決定する。

附　則
1. この規程は，2013 年 05 月 17 日から施行する。

2013 年 05 月 17 日　作成
2023 年 07 月 06 日　改訂