下仁田厚生病院情報セキュリティ基本方針

１．目的

本基本方針は、下仁田南牧医療事務組合下仁田厚生病院（以下、当院という。）が保有する情報資産の機密性、完全性及び可用性を維持するため、情報セキュリティ対策に関する基本的事項を定めることを目的とする。

２．基本方針

当院は、個人情報の保護と医療サービスの継続性を確保するために、以下の方針に基づき、セキュリティ対策の水準を高めていく。

（１）安全かつ持続的な医療サービス提供を実現する

（２）サイバーセキュリティに対する脅威から事業を保護する

（３）リスクマネジメントの対象としてサイバーセキュリティを確保する

３．用語の定義

本基本方針において、次に掲げる用語の意義は、当該各号に定めるところによる。

（１）情報資産

診療情報その他当院の業務に関して取り扱う全ての情報並びにこれらを取り扱う情報システム、ネットワーク、機器、記録媒体、施設、関連文書及び委託先又は外部サービス上に保管もしくは処理される情報をいう。

（２）診療情報

診療録、看護記録、検査結果、画像情報、処方情報その他患者の診療に関して作成又は取得される情報をいう。

（３）医療情報システム

診療情報その他当院の業務に関する情報を取り扱うための情報システム、ネットワーク、端末、ソフトウェア及びこれらに附帯する設備をいう。

（４）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（５）機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を保証することをいう。

（６）完全性

情報資産が破壊、改ざん又は消去されていない状態を保証することをいう。

（７）可用性

情報資産にアクセスすることを認められた者が、必要なときに情報資産にアクセスできる状態を保証することをいう。

（8）情報セキュリティインシデント

情報セキュリティが侵害されている事態をいう。具体的には情報資産の漏えい、滅失、毀損、改ざん、不正利用、利用不能その他情報セキュリティを侵害し、又は侵害するおそれのある事態をいう。

（9）職員等

当院の役員、職員、非常勤職員、派遣職員、研修生、実習生、委託事業者及び当院の情報資産を利用する全ての者をいう。

4．適用範囲

（1）本基本方針の適用は、当院及び下仁田南牧医療事務組合議会が保有し、又は管理する全ての情報資産並びにこれを取り扱う全ての職員等に適用する。

（2）前項の適用範囲には、情報資産の取得、作成、利用、保存、移送、提供、外部委託、保守、廃棄その他これらに関連する一切の取扱いを含む。

5．法令等の遵守

当院は、情報セキュリティ対策の実施に当たり、関係法令、関係省庁の指針、医療分野における関連ガイドライン、契約上の義務及び院内諸規程を遵守する。

6．対象とする脅威

情報資産に対する脅威を以下のように想定し、情報セキュリティ対策を実施する。

（1）不正アクセス、標的型メール攻撃、ウイルス感染等のサイバー攻撃による情報資産の漏えい、破壊、改ざん・消去、重要情報の詐取等

（2）職員等による誤操作、設定不備、情報機器の紛失、無断持出し、内部不正、権限の不適切な利用その他人的又は運用上の要因による事故

（3）自然災害、大規模停電等によるサービスおよび業務の停止

7．情報セキュリティの管理体制の整備

（1）当院は情報セキュリティ対策を推進するため、医療情報システムに関する責任者、個人情報に関する責任者、その他必要な責任者を置き、管理体制を整備する。

（2）管理体制においては役割及び責任を明確にし、必要に応じて情報セキュリティインシデントに対応する体制を整備する。

８．リスクアセスメントの実施

（１）当院は、情報資産の重要性、想定される脅威、脆弱性、業務への影響等を踏まえ、情報セキュリティに関するリスクを適切に把握し、評価し、その結果に応じて必要な対策を講ずる。

（２）前項の評価は、情報システムの新規導入、更改、構成変更、外部委託又は外部サービス利用その他必要な場合に実施し、又は見直すものとする。

９．情報資産の分類及び管理

当院は、情報資産をその重要性に応じて分類し、当該分類に応じた人的、物理的、技術的及び運用上の対策を講ずる。特に診療情報及び個人情報については、その重要性に鑑み、厳格な管理を行う。

１０．総合的な情報セキュリティ対策の実施

当院は、情報資産を保護するため、次に掲げる対策を総合的に実施する。

（１）組織的対策

当院の情報資産について、情報セキュリティ対策を推進する体制を確立する。

（２）人的対策

全ての職員等に対し、情報セキュリティに関する教育、啓発及び訓練を継続的に実施し、情報セキュリティ意識の向上及び事故防止を図る。

（３）物理的対策

サーバー室、インターネット回線、職員等のパソコン等の管理について、物理的な対策を講じる。

（４）技術的対策

情報資産を不正なアクセス等から適切に保護するため、パソコン等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（５）運用上の対策

ネットワーク及び情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。

（６）業務継続及び復旧に関する対策

情報セキュリティインシデントが発生し、又は発生する恐れがある場合、早急な報告及び初動対応を行い、被害拡大の防止、原因の調査、復旧対応を講ずる。

１１．外部委託及び外部サービスの管理

当院は、業務の全部又は一部を外部委託し、又は外部サービスを利用する場合に

は、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要な対策が確保されていることを確認し、必要に応じて契約に定めた措置を講じる。

１２．情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシー及び情報セキュリティ実施手順の遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

１３．情報セキュリティポリシーの見直し

情報セキュリティ監査、自己点検、リスクアセスメント及びインシデント対応の結果並びに社会的環境、技術的環境及び脅威の変化を踏まえ、本基本方針及び対策基準等を定期的に評価し、必要に応じて見直す。

附 則

（施行期日）

この情報セキュリティ基本方針は、令和８年３月１日から施行する。