国保国吉病院組合情報セキュリティ基本方針

(目的)

1　IT 技術の著しい進展により、医療分野においても医療情報システムの導入など電子化が急速に普及していることに伴い、情報漏えい等のリスクも高まっていることから、国保国吉病院組合(以下「当組合」という。)の保有する情報資産(医療情報に限る。)の機密性、完全性及び可用性を維持する対策を整備し、もって当組合を利用する地域住民の方々(以下「利用者」という。)の個人情報を守るとともに、医療機関としての信頼感と安全感の向上を図ることを目的とする。

(位置付け)

2　この基本方針及び医療情報システム運用管理規程をもって、国保国吉病院組合情報セキュリティポリシーとする。

(定義)

3　この基本方針において用いる用語の定義は次のとおりとする。

(1)　ネットワーク　コンピュータ等を相互に接続するための通信網、その構成機器(ハードウェア及びソフトウェア)をいう。

(2)　情報システム　コンピュータ、ネットワーク及び電磁気的記録媒体で構成され、情報処理を行う仕組みをいう。

(3)　情報資産　ネットワーク及び情報システムの開発と運用に係るすべての情報並びにネットワーク及び情報システムで取り扱うすべての情報をいう。

(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)　医療情報システム　当組合で運用する電子カルテシステム及び電子カルテシステムと接続する部門システム並びに接続機器など診療情報を取り扱うシステムをいう。

(6)　機密性　情報に関して正当な権限を持った者だけが、情報にアクセスできること。

(7)　完全性　情報に関して破壊、改ざん又は消去されていないこと。

(8)　可用性　情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできること。

(適用範囲)

4　この基本方針の適用範囲は、医療情報システムで取り扱う電子情報だけでなく、医療情報システムへ入力する前の紙媒体の情報等、当組合で扱う全ての医療情報とし、適用対象者は、当組合に勤務する全職員、および当組合の情報資産を利用する全ての関係者（委託業者等を含む）とする。

(医療情報システム運用の基本原則)

5　当組合の医療情報システムは、次に掲げる基本原則により運用する。

(1)　保存義務のある情報の電子媒体による保存については、情報の真正性、見読性及び保存性を確保すること。この場合において、情報の真正性、見読性及び保存性の確保とは、厚生労働省の所管する法令の規定に基づく民間事業者等が行う書面の保存等における情報通信の技術の利用に関する省令(平成 17 年厚生労働省令第 44 号)第 4 条第 4 項第１号、第２号及び第３号にそれぞれ対応する措置をいう。

(2)　医療情報システムの利用にあたっては、守秘義務を遵守し、利用者の個人情報を保護すること。

(3)　医療情報システムへのコンピュータウィルスの侵入及び外部からの不正アクセスに対して必要な措置を講ずること。そのため、原則として、ソフトウェアのインストール及び私物 USB メモリなどの外部記憶媒体の接続を原則として禁止すること。

(通常運用責任と事後責任)

6　医療情報システムの運用に当たっては、当組合セキュリティポリシーに従い適正な管理を行うとともに、定期的に運用管理全般の見直しを行わなければならない。また、何らかの不都合な事態が生じた場合は、その事実を速やかに公表し、再発防止策を含む適切な対策を速やかに講じなければならない。

(組織体制)

7　医療情報システムの適正な運用を図るため、次の職及び組織を置く。

(1)　医療情報システム運用責任者及び個人情報保護責任者　医療情報システムの運用及び個人情報の保護に関する最終責任者であり、いすみ医療センター病院長(以下「院長」という。)をもって充てる。

(2)　医療情報システム管理者　医療情報システムを円滑に運用するための管理責任者であり、院長が指名する者をもって充てる。

(3)　医療情報システム安全管理者　医療情報システムの適正な運用を図るための責任者であり、事務局長をもってこれに充てる。

(4)　医療情報システム部門管理者　電子カルテシステムに接続する各部門システムの責任者であり、それぞれの部門の管理責任者をもって充てる。

(5)　医療情報システム監査責任者　医療情報システムの適正な運用を図るため、定期的及び臨時的な監査を行う責任者であり、院長が指名するものをもって充てる。

(6)　医療情報システム委員会　医療情報システムに関し必要な事項を審議するため設置するものであり、院長を委員長とし、その運営については別に定める。

(情報の管理)

8　医療情報システムで取り扱う情報については、情報の取得から利用・保管・廃棄までの流れに沿ったリスク分析を実施し、そのリスクに対応した取扱い

方法について規程を定めるなど、適切に管理運用しなければならない。

(保管期間)

9　医療情報システムで取り扱う情報の保管期間は、それぞれ該当する法令に定める保管期間を基本として別に定める。また、医療情報システムへのアクセスログについては、その記録を5年間保管しなければならない。

(使用者識別)

10　医療情報システムの使用に当たっては、使用者の登録を管理し、そのアクセス権限を規定し、不正な利用を防止するための措置を講じなければならない。

(標準規格等)

11　医療情報システムにおいて用いられる各種規格については、医療情報システムの安全管理に関するガイドラインに掲載されている標準規格等に可能な限り準拠するものとし、その改訂状況を常に確認して、整合性を維持するよう努めなければならない。

(教育)

12　個人情報を扱う当組合の職員は、情報セキュリティの重要性と、個人情報の適切な取扱い及び安全管理について、定期的に意識面及び技術面の向上を目的とした教育研修を継続的に受けなければならない。

(監査)

13　医療情報システムの適正な運用を維持するために、定期的に内部監査を実施し、その結果を医療情報システム運用責任者に報告するものとする。この場合において、問題点の指摘等があった場合は、医療情報システム運用責任者は、直ちに必要な措置を講じなければならない。

(改訂)

14　この基本方針を改訂する場合は、医療情報システム運用責任者の承認を受けなければならない。

(問い合わせの窓口)

15　医療情報システムの運用に関して、利用者からの質問、問い合わせに応じる担当窓口を設置する。

附則

この訓令は、令和８年３月１日から施行する。