情報セキュリティ基本方針

目　次

１．総則

１．１　目的

本方針は、福岡県医師国民健康保険組合（以下、「当組合」という）の取り扱う個人情報を、故意、過失、偶然の区別に関係なく、改ざん、破壊、漏洩から保護すると共に、個人情報を利用する役職員に対して、情報システムに関する安全管理の重要性、及び個人情報の適切な取り扱いと保護についての認識を高め、医療保険者としての信頼感と安心感の向上を図ることを目的として制定する。

１．２　適用範囲

１）適用対象者

情報セキュリティ基本方針（以下、「ポリシー」という）は、役員、職員、契約社員、嘱託職員、出向社員、派遣社員及びパート等（以下、「役職員」という）の雇用形態、職位、資格、勤務地を問わず、全役職員に対して適用する。ただし、ポリシーの対象となる業務を外部に委託する場合には、別途、本ポリシーに準拠した内容の外部委託契約を締結する。

２）適用情報

ポリシーは、情報システムで取り扱う電子情報だけでなく、情報システムへ入力する前の紙媒体の情報や、役職員の履歴書等全ての個人情報に対して適用する。当組合が遵守すべき具体的な事項は、ポリシーに基づいた物理的、組織的、技術的及び人的な対策を、情報システムに関する「運用管理規程」及び紙媒体の情報に関する「機密文書管理規程」にまとめる。

１．３　定義

１）情報セキュリティポリシー（以下、「ポリシー」という）

ポリシーとは、組織内にある情報を安全に運用するための規約を文書化したものである。本ポリシーは、当組合の「個人情報保護方針」に基づいて、当組合の情報システムに関する安全管理についての基本姿勢を示したものである。

２）個人情報

個人情報とは、氏名、住所、生年月日、性別等の個人を特定できる情報または他の情報と組合せて個人を特定できる情報を含んだ情報をいう。なお、個人情報は、特定個人情報も含む。特定個人情報は、個人番号（個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。）をその内容に含む個人情報を指す。

個人情報保護法においては、保護の対象は、「生存する」個人情報であり、死者に関する情報については、保護の対象とならない。番号法における特定個人情報についても同様の取扱いとなるが、特定個人情報のうち、個人番号については、

生存者の個人番号であることが要件でないため、死者の個人番号も保護の対象となる。

法令の定める業務範囲の手続において、個人番号の記入欄のある様式を用いて得られた情報については、様式に個人番号の記入がない個人情報も特定個人情報と同様に取り扱う。

３）情報システム

情報システムとは、当組合で運用する適用、給付、徴収に係る医療保険業務に適用する医療保険システム、健診、検診に係る保健業務に適用する保健システム及び当組合の人事・給与、資産管理、財務会計等に係る業務に適用する業務システム並びにこれらのシステムへの接続機器などをいう。

２．基本原則

当組合の情報システムは、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、保存性を確保する。

２）情報システムの利用に当たっては、守秘義務を遵守し、加入者個人の情報を保護する。

３）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対策を講じる。原則、ソフトウェアのインストール及びUSBメモリ等の外部記憶媒体の接続を禁止する。

３．管理運営体制

３．１　ポリシーの管理体制

１）ポリシーは、情報システム管理委員会（以下、「委員会」という）を設置して、委員会が維持管理を行う。

２）委員会は、委員長を置き、理事長をもってこれに充てる。

３）各部署の長は、委員会の指示を受け、各部署に置いてポリシーが遵守されるように指導、教育を行う。

３．２　情報システムの運用体制

１）情報システムについては、運用責任者を置き、常務理事をもってこれに充てる。

２）運用責任者は、情報システムの安全管理に必要な、組織的、人的、技術的、物理的対策を実施し、維持し、かつ、改善するために不可欠な資源を用意する。

３）運用責任者は、情報システムを円滑に運用するため、情報システムに関する運用を担当するシステム管理者を内部の者から指名することができる。

３．３　苦情・質問窓口の設置

個人情報の取扱い及び情報システムの運用に関して、本人及びシステム利用者からの苦情及び質問を受け付け、適切かつ迅速な対応を行うために、苦情・質問を受け付ける窓口（ヘルプデスク）を設ける。

４．管理方法

４．１　情報の管理

情報システムで取扱う情報は、情報の取得から利用・保管・廃棄までの情報の取扱の流れに沿ったリスク分析を実施し、リスクに対応した適切な取り扱い方法を運用管理規程、機密文書管理規程、他各種手順書等に規定して、適切に管理・運用する。

４．２　保管期間

情報システムで取扱う情報は、法令に定められた保管期間を基本として別途定める。また、情報システムへのアクセスログを記録し、その記録を最低１年保管する。

４．３　利用者識別

情報システムの利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。

４．４　監督及び教育

委員会は、全ての役職員に対して、情報セキュリティの重要性と、個人情報の適切な取り扱い、及び安全管理について意識面及び技術面の向上を目的として、必要かつ適切な監督及び継続的な教育を行う。

４．５　事故の予防と対応

当組合は、ポリシーの遵守により、情報漏洩事故等の発生の予防に努める。万一、事故が発生した場合には、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る。

４．６　罰則規程

委員会は、役職員がポリシーに違反して、当組合の情報セキュリティに重大な影響を与えた場合、又はそれに準ずる悪質な行為などが認められた場合、当組合の就業規則に基づいた処罰を勧告することができる。

５．ポリシーの維持管理

５．１　ポリシーの改訂及び公開

1）ポリシーは、以下のような場合等を想定して、委員会の決議・承認及び運用責任者の承認を経て改訂する。

ａ）IT 技術の発展とポリシーの整合性を維持する必要がある場合

ｂ）社会環境の変化とポリシーの整合性を維持する必要がある場合

ｃ）法令及び標準規格等とポリシーの整合性を維持する必要がある場合

2）各部門で作成した運用規程については部門長の承認を経て改訂することができる。

3）改訂されたポリシー並びに運用管理規程は、改訂後即時に役職員に向けて公開する。原則として、当組合の外部に向けては公開しない。

５．２　監査及び是正措置

1）情報システムの適正な運用とその有効性を維持するために、毎年１回内部監査を実施する。ただし、高度な技術を要する監査が必要な場合は、外部の専門家による外部監査を導入する。

2）運用責任者は、監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な措置を講じる。

附則

１　この基本方針は、平成２７年７月１日から施行する。