

## 21-2. 地域医療振興協会健康保険組合 システム等運用管理規程

### 第1章（総則）

（目的）

第1条 本規程は、組合の情報セキュリティ基本方針及び個人情報保護管理規程に従い、当組合の業務を取り扱う情報システム（以下「情報システム」という。）及び個人情報等を含むデータ又は情報（記録様式、媒体の種類を問わない。以下「データ」又は「情報」という。）の安全かつ合理的な運用及び適正な管理を図るとともに、データ又は情報の漏えい、滅失、毀損等の防止を図るために必要な事項を定めることを目的とする。

（適用対象）

第2条 本規程の適用対象となる情報システムは、組合の業務を取り扱う全てのシステム（システムのオペレーション手順、コードブック等を含む。）とし、主なものは次に掲げるものとする。

- （1）基幹業務システム
- （2）健康保険組合に対する社会保険手続に係る電子申請システム及びレセプトオンライン請求システム
- （3）個人番号を介した情報連携に使用するシステム
- （4）公益社団法人地域医療振興協会の情報システム
- （5）金融機関との取引に使用するシステム

2 本規程の適用対象となるデータ又は情報は、次に掲げるものとする。

- （1）個人情報
- （2）組合に関し外部に知られることを適当としないデータ又は情報
- （3）事故等が発生した場合に、その復元等が著しく困難となるおそれのあるデータ又は情報

### 第2章（組織的な対策）

（管理運営体制）

第3条 本規程の実施にかかる管理運営体制は次の実務責任者により構成されるものとする。

- （1）本規程の実施にかかる管理責任者として「データ保護管理者」を置くものとし、原

則として個人情報取扱責任者が就任するものとする。

- (2) データ保護管理者の指示のもとに本規程の実施にかかる実務担当者として「データ保護担当者」を置くものとし、原則として個人情報保護管理担当者が就任するものとする。
- (3) 本規程の適正な実施にかかる監査の実施者として「情報システム監査責任者」を置くものとし、原則として監事が就任するものとする。

(実務責任者の責務等)

第4条 データ保護管理者は、以下の責務等に基づいて実務を行うものとする。

- (1) 本規程に定める組織的、人的、技術的、物理的安全対策の実施により情報システム及びデータ又は情報の取扱いについて、適正かつ円滑な運用を図る。必要な場合には、当該情報システムを管理する者に協力を求めるものとする。
  - (2) 情報システムの機能要件に挙げられている機能が支障なく運用される環境を整備する。
  - (3) 情報システム及びデータ又は情報の取扱いについての苦情対応窓口を設置する。
  - (4) 監査結果に基づく是正等の必要な措置を講じる。
  - (5) 情報システム及びデータ又は情報を取り扱う担当者として、当該取扱いが必要となる業務ごとに「事務担当者」を任命し、アクセス権限を付与する。
  - (6) 情報システム及びデータ又は情報について不正利用が行われた場合、又はその疑いが見込まれる場合、事務担当者が使用した電子メール、インターネットへのアクセス、その他情報システム及びデータ又は情報の使用履歴及び内容について調査することが出来るものとする。調査に当たっては、当該システムを管理する者に必要な協力を求めるものとする。
- 2 データ保護担当者は、以下の責務等に基づいて実務を行うものとする。
- (1) 情報システムに用いる機器及びソフトウェアを導入するに当たって、システムの機能を確認する。
  - (2) 個人情報の安全性を確保し、常に利用可能な状態に置いておく。
  - (3) 機器やソフトウェアに変更があった場合においても、情報が継続的に使用できるよう維持する。
  - (4) 情報システムへの事務担当者の登録及びアクセス権限を定める。
  - (5) 作業手順書の整備を行い事務担当者への教育及び周知を実施する。
  - (6) 情報システムにかかる安全管理の見直し及び改善の基礎として、データ保護管理者

にシステムの運用状況を報告する。

(7) 情報システムにかかるマスタの管理及び変更追加時におけるデータ保護管理者への報告等により、正常な稼動状況を維持管理する。

3 情報システム監査責任者は、以下の責務等に基づいて実務を行うものとする。

(1) 情報システム及びデータ又は情報の取扱いにかかる監査を実施し、その結果について監査報告書をもってデータ保護管理者に報告する。

(2) 監査の実施においては、監査の客観性及び公平性を確保する。

(事務担当者の責務)

第5条 事務担当者は、付与されたアクセス権限に基づき情報システムを利用することが出来る。この場合において、法令及び関連規程を遵守することはもとより、以下の責務等に基づいて実務を行うものとする。

(1) 自身のアクセス権限にかかるパスワード等の情報を管理し、これを他者に利用させない。

(2) 第1号に定める管理が正当に行われなかったために生じた事故や障害に対しては、当該担当者が責任を負う。

(3) 情報システムへの情報入力に際して、確定操作（入力情報が正しい事を確認する操作）を行って、入力情報に対する責任を明示する。

(4) 付与されたアクセス権限を越えた操作を行わない。

(5) 情報システム及び参照した情報を業務の目的外に利用しない。

(6) 加入者等のプライバシーを尊重し、職務上知ることが必要な情報以外の情報にアクセスしてはならない。

(7) 利用者は、法令上の守秘義務の有無に関わらず、アクセスにより知り得た情報を目的外に利用し、又は正当な理由なしに漏らしてはならない。異動、退職等により職務を離れた場合においても同様である。

(8) 情報システムの異常を発見した場合、速やかにデータ保護管理者又はデータ保護担当者に報告し、その指示に従う。

(9) 不正アクセスを発見した場合、速やかにデータ保護管理者又はデータ保護担当者に報告し、その指示に従う。

(10) 離席する際は、窃視防止策を実施する（ログアウト又はスクリーンロック等）。

(11) ウィルスに感染又はそのおそれを発見した場合、ネットワークから端末を切り離すとともに、速やかにデータ保護管理者又はデータ保護担当者に報告し、その指示に従

う。

(12) 電子メール等の利用に際し、公序良俗に反する、著作権又は他者の財産を侵害するおそれがあるものなど組合の信用、品位を傷つけるおそれのある内容を発信、公開してはならない。

(予防処置及び是正処置)

第6条 組合は、加入者、システム利用者等からの苦情、緊急事態の発生、監査報告、外部審査機関等からの指摘により、システムの機能、運用状況等に問題がある場合には、問題に対する予防処置及び是正処置（以下「処置等」という。）のための責任及び権限を定め、処置等の手順を定めて、これを実施する。

2 前項に定める処置等は、以下の手順で行うものとする。

- (1) 発生した問題の内容を確認のうえ、問題の原因を特定する。
- (2) 発生した問題の処置等を立案する。
- (3) 立案された処置等について、期限を定めて実施して、実施結果を確認する。
- (4) 実施された処置等の有効性を確認する。
- (5) 発生した問題について、問題の内容、原因、実施した処置等の実施結果及び有効性を記録する。

3 適切な情報システムの運用を維持するため、組合会において年に一度、データ保護管理者より個人情報保護にかかる安全管理措置の実施状況及び次の事項について報告をうけるとともに、必要な都度、本規程の見直しについて審議するものとする。

- (1) 監査及びデータ保護管理者の運用状況に関する報告
- (2) 苦情を含む外部からの意見
- (3) 前回までの見直しの結果に対するフォローアップ
- (4) 法令等の規範の改正状況
- (5) 社会の情勢等の変化、国民の認識の変化、技術の進歩などの諸環境の変化
- (6) 情報システムの運用状況の変化
- (7) 内外から寄せられた改善のための提案

(事故への対応)

第7条 組合は、事故が発生した場合、再発防止策を含む適切な対策を速やかに講じるとともに、事故発生の実態、対応及び再発防止策等の対策を速やかに公表しなければならない。

2 データ保護管理者又はデータ保護担当者は、事故等発生の予防に努めるため、情報システムの扱う情報について、予見されるリスクを洗い出すとともに、事故発生時の危険

度を明確にして、リスクを回避する方法を提示するリスク分析を行う。リスクには、事業継続性を考慮して、災害及び障害を含めるものとする。

- 3 データ保護管理者又はデータ保護担当者は、リスク分析の結果を記録し維持・管理する。

(非常時の対策)

第8条 データ保護管理者は、前条第2項及び第3項に定める事項とあわせ、災害、サイバー攻撃などにより医療保険サービスの提供体制に支障が発生する「非常時」の場合を想定して、非常時と判断するための基準、手順、緊急連絡網、判断者等の判断する仕組み、システムの閉塞及び縮退運用等の手順（以下「非常時運用」という。）及び正常状態への復帰手順を定めた事業継続計画（以下「BCP」という。）等、非常時における対策を策定するものとする。

- 2 データ保護管理者は、前項に定めるBCP等の対策を利用者に周知の上、常に利用可能な状態におく。

(監査)

第9条 本規程における法令、関連通知、「医療情報システムの安全管理に関するガイドライン」への準拠状況、情報システムの運用状況及びデータの取扱いについて、少なくとも年に1度、第4条第3項に定める監査を受けなければならない。

- 2 データ保護管理者は、情報システム監査責任者から監査結果の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置等を講じなければならない。
- 3 データ保護管理者は必要な場合、臨時監査を情報システム監査責任者に進言することができる。

(苦情・質問受付)

第10条 組合は、個人情報の取扱い及び情報システムの運用に関し、加入者及びシステム利用者からの苦情及び質問の受付窓口（以下「受付窓口」という。）を設置するものとする。

- 2 受付窓口は、直接又は間接的に苦情を受けた際に、別途定められた手順に則って速やかに対応しなければならない。
- 3 受付窓口は、受付けた苦情・質問を整理し、データ保護管理者に報告しなければならない。
- 4 データ保護管理者は、受付窓口の報告を受け、問題点の指摘等がある場合には、直ちに必要な処置等を講じる。

(秘密保持義務)

第11条 組合の役職員等（雇用形態を問わず、組合内において組合に関連する業務に従事す

る全ての者をいう。)は、健康保険法(大正11年法律第70号)第22条の2の規定に基づき秘密保持義務を負っており、在職中のみならず、退職後においても職務上知り得た個人情報等第2条に定める本規程の適用対象に関する秘密を漏らしてはならない。

2 組合は、役職員等を採用するに当たり、前項の秘密保持義務を周知するものとする。

(業務委託契約)

第12条 組合業務を外部委託する場合には、以下の処置を実施するものとする。

2 守秘義務を含む業務委託契約を結ぶものとする。なお、別途守秘契約を結ぶ場合、契約の署名者は理事長又はデータ保護管理者とし、委託先の署名者はデータ保護管理者に相当する者とする。

3 前項に定める契約に、前項に規定する守秘義務のほか次に掲げる事項を規定し、十分な個人情報の保護水準を担保しなければならない。

(1) 健康保険組合における個人情報保護に関する遵守基準

(2) 目的外使用の禁止

(3) 再委託の禁止

(4) 契約解除事項の設定

(5) 損害賠償

(6) 業務処理状況に対する調査・監査権

4 再委託は前項第3号に基づき禁止するものとする。ただし、やむを得ない事情等により委託先事業者が再委託を行う場合は、当組合による再委託の許諾を要件とする。この場合、再委託先において、委託先と同等の個人情報保護に関する対策及び契約がなされていることを条件とし、組合との業務委託の契約書に再委託での安全管理に関する事項を加えるものとする。

5 組合の情報システムの保守・改修・管理を委託する等により、役職員等以外の者(保守要員という。以下同じ。)が組合内で作業する場合において、データ保護管理者又はデータ保護担当者は、以下の確認を実施する。

(1) 保守要員用のアカウントの確認(保守要員個人の専用アカウントを使用すること)。

(2) 保守作業等の情報システムに直接アクセスする作業の際には、作業員、作業内容及び作業結果の確認(原則として日単位)。

(3) 清掃等、直接情報システムにアクセスしない作業の場合の定期的なチェック。

(4) 保守契約における個人情報保護の徹底。

(5) 保守作業の安全性についてログによる確認。

- 6 委託先（再委託先を含む。）における法令、契約等に基づく個人情報保護にかかる措置の遵守状況を確認する為、定期的又は必要な都度、立ち入り監査又は立ち入り監査における確認項目と同等の項目を書面にて確認する等の合理的な方法による確認を実施するものとする。

### 第3章（人的な対策）

#### （教育の実施）

第13条 データ保護管理者及びデータ保護担当者は、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意識面及び技術面の向上を目的として、役職員等に対し必要かつ適切な監督及び継続的な教育を行うものとする。

#### （マニュアルの整備）

第14条 データ保護管理者及びデータ保護担当者は、情報システムの取扱いについてマニュアルを整備し、事務担当者に周知の上、常に利用可能な状態におくものとする。

#### （研修）

第15条 データ保護管理者及びデータ保護担当者は、事務担当者に対し、定期的に情報及び情報機器の持出しにかかる運用方法を含む情報システムの取扱い及びプライバシー保護に関する研修を行うものとする。この場合において、研修時のテキスト、出席者リストを残し経過及び内容を明確にするものとする。

### 第4章（物理的な対策）

#### （入退出管理）

第16条 部外者（原則として組合の役職員等以外の者をいう。以下同じ。）の立入りを制限する必要がある物理的な領域を以下のように定義する。

- （1）組合の役職員等が執務する場所又は部屋を「執務室等」という。
- 2 部外者が執務室等に立ち入る場合、入退室記録の作成、同伴等の管理を実施する。
- 3 データ保護管理者は、入退室の記録を定期的に確認して、問題が確認されたつど、適切な措置を講ずる。

#### （執務室等の安全管理）

第17条 データ保護管理者は、執務室等における火災、その他の災害、盗難に備えて、自動消火装置などによる必要な保安処置を講じなければならない。

- 2 データ保護管理者は、情報システムの正常稼働維持のため、執務室等の温度、湿度等の環境を適切に保持するものとする。

(記録機器及び端末の安全管理)

第18条 記録機器及びPC等の端末は、以下のいずれかの対策により盗難防止措置を講ずるものとする。

- (1) 執務室等を施錠し、施錠を記録・管理する。
  - (2) 盗難防止用ワイヤーロックで固定する。
- 2 PC等端末の使用に際しては、部外者の通る方に画面を向けず、窃視防止フィルムを貼るなどの、窃視防止に努めるとともに、離席時など、特定の時間(5分以内)使用しなかった場合は、なりすましによる使用を防ぐため、パスワード付きスクリーンロック、又は自動ログオフ機能を設定するものとする。
- 3 記録機器及びPC等端末の廃棄並びにレンタル・リース切れによる返却等に当たっては、以下の手続きを行った上で当該処理を行うものとする。
    - (1) ハードディスク等の既存情報を上書処理により書き換え、情報の完全消去を行った上で当該措置を行う。
    - (2) 情報を削除又は廃棄した記録を保管管理する。
  - 4 前項に定める情報の消去又は廃棄処理を外部業者に委託する場合は、情報を完全消去した証明書を受領し、証明書を保管管理するものとする。

(組合内ネットワーク管理)

第19条 情報システムのネットワーク(以下、「組合内LAN」という。)は、インターネット、仮想プライベートネットワーク等の当組合の外部と情報交換ができるネットワークとは技術的な安全対策を適用した上で接続するものとする。

- 2 事務担当者は、組合内LANに端末を接続する場合、データ保護管理者の承認を得なければならない。
- 3 事務担当者が私有(組合が支給したもの以外をいう。)のPCを持ち込み、組合内LANに接続することは、原則禁止とする。ただし、業務上やむを得ず接続を要する場合は、データ保護管理者の承認を得て行うこととする。この場合、PCの使用に当たっては、本規程を準用するものとする。
- 4 委託先等の部外者が情報システム等保守のためPC等を持ち込んで組合内LANに接続する場合、データ保護管理者の承認を得なければならない。

(外部機関との情報交換)

第20条 医療保険者、保守会社、通信事業者、運用委託業者等の外部機関と情報を交換する場合、相手外部機関との間で、責任分界点や責任の所在を契約書等で明確にするものとする。ただし、法令等で情報交換が必要な外部機関と接続する場合は、この限りではない。

- 2 データ保護管理者は、外部機関と情報を交換する場合、リスク分析を行い、安全に運用されるように技術的対策を講ずるものとする。
- 3 リスク分析及びその技術的対策の内容を文書化して、維持・管理し、外部機関との情報交換が適切に実施されているかを定期的に確認するものとする。

(電子媒体の管理)

第21条 データ保護管理者が特に許可した場合を除き、情報のバックアップ業務以外には外部記憶媒体へのデータ等の複写を禁止するものとする。

- 2 個人情報を記録した可搬型記録媒体（FD、CD-ROM、DVD、USBメモリ等）は、施錠できるキャビネットに保管し、その所在を台帳に記録し、管理する。
- 3 個人情報を可搬型記録媒体で授受する場合は、授受の記録を残すものとする。

第22条 削除

(情報及び情報機器の持出し管理)

第23条 情報及び情報機器の持出しに関してリスク分析を実施し、持出し対象となる情報及び情報機器を規定し、それ以外の情報及び情報機器の持出しを禁止するものとする。

- 2 持出し対象となる情報及び情報機器をまとめて、利用者に公開するものとする。
- 3 持出し対象となる情報及び情報機器の持出しについては、情報の暗号化、ファイル交換ソフトのインストール禁止の実施及び次の措置を講ずるとともに、データ保護管理者の承認等を条件とする。

(1) 起動パスワードを設定する。起動パスワードは、推定しやすいものは避け、また定期的に変更する。

(2) ウィルス対策ソフトをインストールする。

(3) 別途定めたもの以外のアプリケーションはインストールしない。

(4) 持出した情報機器をネットワークに接続、又は他の外部媒体を接続する場合において、ウィルス対策ソフトやパーソナルファイアウォール等により情報漏えい及び改ざん等防止対策を講ずる。

(5) データ保護管理者は、情報が格納された可搬媒体及び情報機器の所在について台帳

に記録し、その内容を定期的にチェックし、所在状況を把握する。

4 盗難、紛失時は、以下のように対処することとする。

- (1) 持出した情報及び情報機器の盗難、紛失時には、速やかにデータ保護管理者に届け出る。
- (2) 届出を受け付けたデータ保護管理者は、その情報及び情報機器の重要度に従って対応する。

## 第24条 削除

(電子媒体の廃棄)

第25条 保存期間経過後の消去及び廃棄方法については、原則として粉碎処理又は溶融処理する等復元不可能な状態にしなければならない。

2 データ保護管理者は、個人情報記録した電子媒体を廃棄するときは、廃棄が安全かつ確実に行われることを作業の前後に確認し、その経過を記録・管理するものとする。

## 第5章 (技術的な対策)

(アクセス権限等)

第26条 データ保護管理者は、第4条第1項第5号に定めるアクセス権限について、役職員等の採用時、異動時、退職時に合わせ、速やかに利用者の認証情報の登録、変更、削除及び認証情報の発行処置を実施するものとする。

2 データ保護管理者は、情報システム等の使用について利用者等の申請により、情報システムへのアクセス権限を審査し、ID・パスワードの設定等本人確認のための措置を実施のうえ、利用者登録を実施する。利用者登録実施後、利用者の認証に必要なデバイス又は認証情報を利用者へ交付する。

3 利用者には、原則として利用者権限を付与し、管理者権限は付与しない。

(外部ネットワーク管理)

第27条 基幹業務システムの端末は、法に定める場合を除き、他の法人格のある外部機関と共用しないものとする。

2 インターネットの利用について、以下の条件の下で管理するものとする。

- (1) インターネット利用は、業務上必要な場合に限られ、私的利用は禁止とする。情報

及びソフトウェア等のダウンロード、インストール等が業務上必要なインターネットサイトは、原則ホワイトリストで指定して通信先を限定する。

(2) データ保護管理者は、ホームページを含む不正アクセスや改ざんの防止のため、インターネットに係る各サーバー、ルータ等に適切な管理策等の処置を講じ、ファイアウォール及びプロキシサーバーを設置する等、許可された通信以外の通信を遮断する措置を実施するとともに、通信の状況を記録し、定期的（月1回以上）に通信状況を確認する。

(3) 当組合の情報を、ホームページを用いてインターネットへ公開、又は公開情報を変更・削除する場合は、データ保護管理者の承認を得なければならない。

(4) データ保護管理者は、ホームページの利用状況を監視し、不正アクセスやホームページの改ざんの有無を確認し、問題がある場合は、適切な処置（予防・是正）を講ずる。

### 3 電子メールの利用について、以下の条件の下で管理するものとする。

(1) メールアカウントはデータ保護管理者が発行し、役職員の退職時には当該役職員のメールアドレスを速やかに削除する。

(2) 電子メールの私的利用は、禁止とする。

(3) 受信メールの自動転送については、組織外へのメール転送を原則禁止とする。ただし、業務の遂行のために予め許された指定メールアドレスへの転送は、信頼のおける転送方法をもって実施する場合のみ可能とする。

(4) 個人情報を含む情報を電子メールで送信する場合、個人情報を含む情報に暗号化処置等を講ずるなど、情報の安全性に留意して、ファイルとして添付して送信することとする。この場合、復号用パスワードは別に送信し、紛失又は誤送に備える。

(5) 電子メールに個人情報が含まれる場合は、必要で無くなった都度、速やかに削除することとする。

### 4 無線LANの利用について、通信の暗号化の実施、アクセスポイントの適宜確認等の不正アクセス対策を実施するものとする。

(ウイルス対策等)

第28条 セキュリティパッチは、以下の手順又は以下に準じた手順に基づいて適用するものとする。

(1) 情報システムのサーバー及び端末には、ベンダーからの保証がない限り、原則として修正プログラムは適用しない。

(2) インターネットへの接続を許可された端末については、オペレーティングシステム

やパッケージソフト等のパッチなどの修正プログラムがメーカーより発行された場合、既存システムの影響を考慮してデータ保護管理者の指示に基づいて実施する。

- 2 ウィルス対策として、以下の措置又は以下に準じた措置を実施するものとする。
  - (1) 悪意のあるソフトウェア等から保護するため、全てのサーバー、端末にアンチウィルスソフトを導入し、パターンファイルは常に最新のものを使用する。
  - (2) 定期的にソフトウェア等のウィルスチェックを行い、感染の有無を確認する。
  - (3) アンチウィルスソフトは、常に稼働させておくこととする。
  - (4) 業務上許された情報取得分については、ウィルスチェックを行い、問題のないことを確認後に使用する。
  - (5) 電子メールサーバーは、すべての着信メールについてウィルスチェックを行い、感染の有無を確認する。
  - (6) ネットワークに接続するサーバーと端末は、配信型のアンチウィルスソフトの利用を可能とし、パターンファイルの更新は自動更新で行う。
  - (7) ネットワークに接続していないPCは、データ保護管理者又はデータ保護担当者が常に更新情報の入手に努め、最新パターンファイルを入手し更新する。
  - (8) インターネットに接続していない組合内LANは、最新のパターンファイルを、インターネットに接続したウィルスサーバーにより取得し、情報システムのウィルスサーバーに手動で更新・配信する。
  - (9) 電子媒体の使用時においては、ウィルス等の不正なソフトウェアの混入がないか事前に確認しなければならない。

(電子署名・タイムスタンプ)

第29条 法令で署名又は記名・押印が義務付けられた文書等において、記名・押印を電子署名に代える場合、以下の条件を満たす電子署名を行う。

- (1) 厚生労働省の定める準拠性監査基準を満たす保健医療福祉分野PKI 認証局もしくは認定特定認証事業者等の発行する電子証明書を用いて電子署名を施す。
  - (2) 電子署名を含む文書全体にタイムスタンプを付与する。
  - (3) 上記タイムスタンプを付与する時点で有効な電子証明書を用いる。
- 2 データ保護管理者は、電子的に受領した文書に電子署名が有る場合の、署名検証手順を定める。具体的には、電子署名が有効である間に、電子署名の検証に必要な情報（関連する電子証明書や失効情報等）を収集し、署名対象文書と署名値とともにその全体に対してタイムスタンプを付与する等の対策を実施する。

附 則

この規程は、平成28年4月1日より施行する。

附 則

この規程は、平成28年8月1日より施行する。

附 則

この規程は、平成30年2月6日より施行する。

附 則

この規程は、令和2年11月17日より施行する。

附 則

この規程は、令和4年4月1日より施行する。

附 則

この規程は、令和5年8月1日より施行する。