システム等運用管理規程

第１章（総則）

（目的）

第１条　システム等運用管理規程（以下「規程」という）は、レゾナック健康保険組合（以下、「組合」という）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、組合の業務を取り扱うシステム（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　規程の適用対象は、組合における全ての情報システム及び個人情報又は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または情報（記録様式、媒体の種類を問わない。以下「データ」または「情報」という。）並びに情報システム設計書、オペレーション手順書、プログラム説明書及びコードブック等（以下「情報システム等の仕様書」という。）とする。

第２章（組織的な対策）

（管理運営体制）

第３条　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)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)規程の適正な実施にかかる点検の実施者として「情報システム点検責任者」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)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の取扱について、適正かつ円滑な運用を図る。

(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の取扱についての苦情対応窓口を設置する。

(4)点検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を取扱う担当者として、当該取扱が必要となる業務ごとに「事務担当者」を定め、アクセス権限を付与する。

(6)情報システム及びデータについて不正利用が行われた場合、また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。

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)情報システム等への「事務担当者」の登録並びに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)情報システム等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情報システム等の運用状況を報告する。

(7)情報システム等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　情報システム点検責任者は、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の取扱にかかる点検を事務監査とあわせて実施し、その結果について監査報告(通知)書をもってデータ保護管理者に報告する。

(2)点検の実施においては、点検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)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)システム等の異常を発見した場合、速やかにデータ保護管理者また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また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（ログアウトまたはスクリーンロック等)。

(11)ウィルスに感染又はその恐れを発見した場合、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また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、著作権また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、点検報告、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程度、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行うとともに、必要な都度、規程の見直しについて審議するものとする。

(1)点検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、事故発生の事実及び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

には、全業務を中断し個人情報取扱責任者の指示を受けるものとする。

（点検）

第９条　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」への準拠状況及び情報システムの運用状況及びデータの取扱について、第４条第３項に定める点検を受けなければならない。

２　データ保護管理者は、情報システム点検責任者から点検結果の報告を受け、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、臨時点検を情報システム点検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、直接また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。

（守秘契約）

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。）は在職中のみならず、退職後においても業務中に知り得た個人情報等第２条に定める規程の適用対象に関する守秘義務を負う。

２　　組合は、役職員が法令通知、基本方針及び関連規程等に違反して、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、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。

（業務委託契約）

第１２条　組合業務を外部委託する場合においては、以下の処置を実施するものとする。

2　守秘事項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　第２項に定める契約に、次に示す事項を規定し、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)個人情報の安全管理に関する事項

(2)事業所内からの個人情報の持出しの禁止

(3)個人情報の目的外利用の禁止

(4)再委託に関する事項

(5)個人情報の取扱状況に関する委託者への報告の内容及び頻度及び第６項に定める点検への協力事項

(6)契約内容が遵守されていることを委託者が確認できる事項

(7)契約内容が遵守されなかった場合の処置

(8)事件・事故が発生した場合の報告・連絡に関する事項

(9)漏えい事案等が発生した場合の委託先の責任に関する事項

(10)一連の委託業務終了後に関する事項（終了報告、確実に情報を消去する等）

(11)確実に削除又は破棄したことを証明書等により確認できる事項

(12)保守要員のアカウント情報の管理に関する事項（適切に管理することを求める）

(13)従業者に対する監督・教育

4　再委託は原則として禁止するものとし、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、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等の保守・改修・管理を委託する等により、役職員以外の者（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、データ保護管理者また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、作業者・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、定期的または必要な都度、立ち入り点検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、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、役職員に対し個人情報保護管理規程に基づき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、情報システムの取り扱いについてマニュアルを整備し、事務担当者に周知のうえ、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、定期的に情報システムの取り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。

第 4 章（物理的安全管理措置）

（個人情報を取り扱う区域の管理）

第１６条　組合は管理区域及び取扱区域を明確にし、それぞれの区域に対し次の各号に従い以下の措置を講じる。

（１）管理区域への入退出管理及び管理区域へ持ち込む機器及び電子媒体の制限を行うものとする。

（２）取扱区域は可能な限り壁または間仕切り等を設置し、事務担当者以外の往来が少ない場所への座席配置や後ろから覗き見される可能性の低い場所への座席配置等をするなど座席配置を工夫するものとする。

（電子媒体及び端末等の安全管理）

第１７条　組合は管理区域及び取扱区域における個人情報を取扱う機器、電子媒体及び書類等について、次のいずれかの対策により盗難防止措置を講じる。

（１）使用しない際は、施錠できるキャビネット・書庫等に保管管理する

（２）特定個人情報を取り扱うシステムが、機器のみで運用されている場合は、セキュリティワイヤー等で固定する

（３）端末等の利用に際しては、離席時など、特定の時間使用しなかった場合はパスワード付スクリーンロック・自動ログオフ機能等を設定する

（電子媒体等の持ち出し管理）

第１８条　電子媒体等の持ち出しに関して持ち出し対象となる電子媒体等を規定し、それ以外の電子媒体等の持ち出しを禁止する。

２．持ち出し対象となる情報については、暗号化・パスワードの設定等、紛失・盗難等を防ぐための安全な方策を講ずるものとする。

（データ等の消去及び電子媒体等の廃棄）

第１９条　　データ及びデータが収録された電子媒体については、法令の定めた保存期間の間、保存・管理するものとする。ただし、法令の定めがない場合については、以下の期間、保存・管理するものとする。

（１）情報システム等で保有するデータについては5年

（２）電子媒体に収録されたデータについては3年（文書保存規程を準用）

（３）電子申請にかかる届出書データ、届出データおよび添付文書については3年

（４）（１）のバックアップを目的としたデータについては10年

２．保存期間経過後の消去および廃棄方法について、破砕処理または溶解処理する等、復元不可能な状態にしなければならない。なお、消去及び廃棄した場合、その経過を記録・管理するものとする。

３．保存期間が経過したデータ及び電子媒体において、引き続き保存する必要があるものについては、改めて保存期間を定めて保存・管理するものとする。

４．個人情報を記した電子媒体の廃棄に当たっては、安全かつ確実に行われることを、データ保護管理者が確認する

５．行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（平成２５年５月３１日・法律第２７号）第２条第５項に定める個人情報（情報システム等で保有するものに限る）については、第１項に定める期間に関わらず資格喪失又は扶養削除の日から１０年間とする。

（情報機器のリモートアクセス管理）

第２０条　　外部からアクセスを許容する情報機器については、以下の内容を別に定めるものとする。

（１）リモート端末及びリモートアクセス要件

（２）リモート端末がリモートアクセス要件を保持していることを確認する手順

（３）情報システムに不正な侵入等の攻撃を防止する技術的対策

２．データ保護管理者は、リモート端末がリモートアクセス要件を保持していることを定期的に確認するものとする。

第 5 章（技術的安全管理措置）

（アクセス権限等）

第２１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、を実施するものとする。

（アクセス者の識別と認証）

第２２条　　個人情報を取り扱う情報システムは、ユーザーＩＤ、パスワード、磁気・

ＩＣカード等の識別方法により、事務担当者が正当なアクセス権を有する者であることを識別した結果に基づき認証するものとする。

（特定個人情報へのアクセス制御）

第２３条　特定個人情報等へのアクセス制御は以下のとおりとする。

（１）個人番号と紐づけてアクセスできる情報の範囲をアクセス制御により限定する。

（２）特定個人情報ファイルを取り扱う情報システムをアクセス制御により限定する。

（３）ユーザーID に付与するアクセス件により、特定個人情報ファイルを取扱う情報システムを使用できるものを事務担当者に限定する。

（外部からの不正アクセス等の防止）

第２４条　組合は、以下の各方法により、情報システムを外部からの不正アクセス又

は不正ソフトウェアから保護するものとする。

（１）情報システムと外部ネットワークとの接続箇所に、ファイアーウォール等を設置し、不正アクセスを遮断する方法。

（２）情報システム及び機器にセキュリティ対策ソフトウェア等を導入する方法。

（３）導入したセキュリティ対策ソフトウェア等により入出力データにおける不正ソフトウェアの有無を確認する方法。

（４）機器やソフトウェア等に標準装備されている自動更新機能等の活用によりソフトウェア等を最新状態とする方法。

（５）ログ等の分析を定期的に行い、不正アクセス等を検知する方法。

（情報漏えいの防止）

第２５条　組合は、個人情報をインターネット等により外部に送信する場合、通信経路における情報漏えい等及び情報システムに保存されている個人情報の情報漏えい等を防止するものとする。

（１）通信経路における情報漏えい等の防止策として通信経路の暗号化を行う。

（２）情報システムに保存されている個人情報の情報漏えい等の防止策として、データの暗号化又はパスワードによる保護を行う。

附　　則　この規程は、平成２８年３月１日より施行する。

平成２８年８月１日に一部変更

令和　４年９月１日に第１９条を一部変更