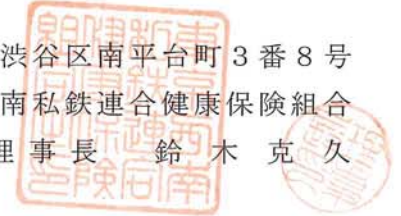


27西南健発第120-2号
公 告 第40-2号
平成28年3月1日

東京都渋谷区南平台町3番8号
東京西南私鉄連合健康保険組合
理事長 鈴木 克久



情報保護関連規程等の新設・変更・廃止について

このたび、下記のとおり「情報セキュリティ基本方針」、「システム等運用管理規程」および「機密文書管理規程」を新設、「個人情報保護管理規程」の変更、「電子計算機処理データ管理規程」を廃止しましたので、公告いたします。

記

東京西南私鉄連合健康保険組合の情報保護関連規程を次のとおり新設・変更・廃止する。

1. 新設

- ・情報セキュリティ基本方針
- ・システム等運用管理規程
- ・機密文書管理規程

上記について別添のとおり新設する。

附 則

この規程は、平成28年4月1日から施行する。

2. 変更

- ・個人情報保護管理規程

上記について別添「新旧条文対照表」のとおり変更する。

附 則

この規程は、平成28年4月1日から施行する。

3. 廃止

- ・電子計算機処理データ管理規程

上記について、平成28年3月31日で廃止する。

以 上

情報セキュリティ基本方針

(目的)

第 1 条 情報セキュリティ基本方針（以下「基本方針」という）は、東京西南私鉄連合健康保険組合（以下「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、個人情報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事を目的として制定する基本姿勢である。

(適用範囲)

第 2 条 基本方針は、役員、職員、契約社員、嘱託社員、出向社員、派遣社員、パート、ボランティア及び実習生等（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。

(個人情報)

第 3 条 個人情報とは、「個人情報の保護に関する法律」（平成15年5月30日・法律第57号。以下「法」という。）第2条第1項に定める特定の個人を識別することができるものをいい、紙に記載されたものであるか、写真・映像や音声であるか、電子計算機・光学式情報処理装置等のシステムにより処理されているかは問わない。

2 特定個人情報とは、「行政手続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。以下「番号法」という。）第2条第8項に定める個人番号をその内容に含む個人情報をいう。

(基本方針)

第 4 条 役職員は、個人情報に関し守秘義務を負うものとし、関連法令、通知及び関連規程を遵守するものとする。

2 組合は、個人情報保護に関する管理体制・管理運用方法・保存期間・役職員への教育・苦情相談窓口設置等の安全管理措置を講ずるものとする。

3 前項の安全管理措置は次の規程により組合会が定めるものとする。

(1) 個人情報保護管理規程

個人情報保護に関する基本的事項について定めるもの

(2) システム等運用管理規程

情報システム（組合において使用する全てのサーバー・PC等の電算機及び関連ソフトウェアをいう。以下同じ。）及び電子データ（全ての記録様式を含む。以下同じ）に関する具体的運用方法について定めるもの

(3) 機密文書管理規程

紙媒体に関する具体的運用方法について定めるもの

- 4 個人情報の漏えい等、事故発生時において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講じるものとする。

(基本方針及び関連規程の管理体制)

第 5 条 基本方針及び基本方針に基づく規程は、次に掲げる場合において改訂を行う等、組合会の責任において維持管理を行うものとする。

- (1) IT技術の発展との整合性を維持する必要がある場合
- (2) 社会環境の変化との整合性を維持する必要がある場合
- (3) 法令及び標準規格等との整合性を維持する必要がある場合

2 改訂された基本方針及び基本方針に基づく規程は、改訂後即時に役職員に向けて公開する。原則として、組合の外部に向けては公開しない。

(苦情・質問窓口の設置)

第 6 条 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を設ける。

(罰則)

第 7 条 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。

(監査及び是正措置)

第 8 条 個人情報の適正な保護を維持するために、毎年1回内部監査を実施する。なお、情報システム上の技術的対策等において、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等の措置を講ずるものとする。

- 2 前項の監査の結果、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. この方針は、平成28年4月1日より施行する。

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 本規程の適用対象は、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 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の取扱いについて、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を取扱う担当者として、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) 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) ウイ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、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、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する等、事故等発生の予防に努めるものとする。

(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 B C P 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」への準拠状況及び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条に定める本規程の適用対象に関する守秘義務を負う。

2 役職員等を採用するにあたり、雇用契約等締結時に前項の守秘義務契約を締結するものとする。

(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 守秘事項を含む業務委託契約を結ぶものとする。なお、契約の署名者は理事長とし、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項に定める監査への協力事項

(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、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、定期的または必要な都度、立ち入り監査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、必

要に応じて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、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以外の者をいう。以下同じ。）の立ち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) 組合の役職員が執務する場所または部屋を「執務室等」という。

(2) 個人情報保管されているサーバー及び記録媒体を設置または保管する場所または部屋を「サーバー室等」という。

2 部外者が執務室等またはサーバー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 データ保護管理者またはデータ保護担当者は、サーバー室等の出入口を常時施錠管理し、その入退室を記録・管理する。

4 サーバー室等への入退出は、データ保護管理者の承認を得て行うものとする。なお、部外者の入退出においてはその者の身分等について確認するものとする。

5 サーバー室等は、組合の役職員の常駐または防犯カメラによる常時監視し得る措置をとる等のセキュリティが保たれた管理領域とする。

6 データ保護管理者は、入退室の記録を確認して、問題が確認されたつど、適切な措置を講ずる。

(執務室等及びサーバー室等の安全管理)

第17条 データ保護管理者は、執務室等及びサーバー室等における火災、その他の災害、盗難に備えて、非常電源装置、無停電装置、自動消火装置、監視カメラ、入退制限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、情報システム等の正常稼働維持のため、執務室等及びサーバー室等の温度、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 サーバー等の記録機器及び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) 使用しない際は鍵のかかる保管庫に保管管理する。
 - (2) 執務室等またはサーバー室等を施錠し、施錠を記録・管理する。
- 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、5分以上使用しないことが見込まれるときは、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をするものとする。
- 3 サーバー等の記録機器及びPC等端末の廃棄及びレンタル・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) 情報を削除また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また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。

(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、「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（以下、「VPN」という）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、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、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の使用にあたっては、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 電子媒体の廃棄は、原則粉碎処理とする。
- 3 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。
- 4 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。
- 5 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作業前後に確認し、結果を記録に残すものとする。

(情報システム等の仕様書)

第22条 情報システム等について技術的対策の概要及び分担等を定めた仕様書を整備、管理するものとする。

- 2 仕様書は、所定の場所に格納して保管しなければならない。
- 3 仕様書を複製し又は外部に持ち出す場合には、理由等を附してデータ保護管理者の決裁を得なければならない。

(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る。
- (2) ウイ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、または他の外部媒体を接続する場合において、ウイ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。

(情報機器のリモートアクセス管理)

第24条 外部からアクセスを許容する情報機器（以下、「リモート端末」という）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。

(データ等の消去及び電子媒体の廃棄)

第25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、法令に定められているものの他は別に定めた保存期間の間保存・管理するものとする。

- 2 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。
- 3 保存期間経過後の消去及び廃棄方法について、破碎処理または熔融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。

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認証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また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。

(サーバー等記録機器の管理)

- 第27条 データ保護管理者は、サーバーへのアクセス状況・稼動状況を必要に応じて確認し、問題がある場合は、速やかに必要な処置を講ずるものとする。
- 2 データ保護管理者は、職務により定められた権限による情報アクセス範囲及び第26条に定めるアクセス権限とは別に管理者権限の付与に関する事項を定め、これに基づきハードウェア及びソフトウェアの設定を行うとともに、情報システム、情報への使用状況を監視するため、アクセスログを取得出来るものとする。
 - 3 異常なアクセスを検知したときは警告を発して、ネットワークを切断する等の対処をするものとする。
 - 4 情報のバックアップについて、定期的実施するとともに、バックアップ媒体については施錠可能なキャビネット、耐火金庫等に保管し、その所在を台帳等に記録する等適正な措置を実施するものとする。
 - 5 リスク対応（障害対策）について、第8条に定める措置により発生時の対

応等を定めるとともに、担当 SE 等と連携のうえ、復旧作業に努めるものとする。

(ネットワーク管理)

第28条 組合のLAN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。また、インターネット等のオープンなネットワークと物理的または論理的に遮断する等の安全管理措置を実施するものとする。

2 インターネットに接続している端末では、個人情報の取扱いは一切禁止とする。

3 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。

(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、必要に応じて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。

4 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カウント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) 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。

5 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29条 セキュリティパッチは、以下また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 ウイルス対策として、以下また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、端末にアンチウイ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イルスチェックを行ない、感染の有無を確認する。
- (3) アンチウイルスソフトは、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、ウイ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イルスチェックを行ない、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、配信型のアンチウイ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、データ保護管理者また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イルスサーバーにより取得し、情報システムのウイ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、ウイ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30条 法令で署名または記名・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

1. この規程は、平成28年4月1日より施行する。

機密文書管理規程

(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、当組合で取り扱う文書のうち、特に機密性の高い文書（以下「機密文書」という。）の適正な管理を図ることを目的とする。

(機密文書の定義)

第 2 条 機密文書とは、秘密保全の必要性が特に高く、当該文書が漏洩することによって、組合に甚大な損害や損失を与える恐れがある文書であって、機密度を規定する区分（以下、「機密区分」という。）を指定した文書と定義する。

(機密区分)

第 3 条 機密文書の機密区分は以下の通りとする。

- (1) 指定された者以外に開示してはならない機密文書を「極秘」と指定する。
- (2) 取扱い部署以外に開示してはならない機密文書を「秘密」と指定する。
- (3) 当組合の役職員以外に開示してはならない機密文書を「社外秘」と指定する。
- (4) 開示には、文書の移動、複写、編集等の文書の取扱いに関わる行為も含まれることとする。

(適用対象)

第 4 条 本規程の適用対象は以下の通りとする。

- (1) 当組合が作成及び編集した（情報システムから出力された帳票類を含む）文書
- (2) 申請・届出及び添付書類等の加入者及び事業主から受領した文書
- (3) 他の地方公共団体、医療保険者、その他の機関から入手した文書、又は情報を文書化したもの（メモを含む）

(個人情報の取扱い)

第 5 条 個人情報は、以下のような機密区分の指定に基づいて取扱うことと

する。

- (1) 特定個人情報が記入又は記載された文書は、機密区分として「極秘」を指定する。
 - (2) 個人情報（特定個人情報を除く）が記入又は記載された文書は、機密区分として「秘密」以上を指定する。
- 2 個人情報、又は特定個人情報の記入欄のある帳票、又は文書（以下、指定帳票という）において、個人情報、又は特定個人情報が記入されたものは、機密文書管理責任者の指定を得ずに前項の（1）（2）文書（「指定文書」という。以下同じ。）に準じて取り扱う。

（管理体制）

第 6 条 本規程の実施にかかる管理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、「機密文書管理責任者」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) 機密文書管理責任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「機密文書管理担当者」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は監事が実施するものとする。

（機密保持）

第 7 条 機密文書の開示を受けた役職員等（組合の指揮監督のもと、組合業務を遂行する者をいう。以下同じ。）は、知り得た機密情報を、関係する業務以外に使用してはならない。

- 2 機密文書の開示を受けた役職員等は、知り得た機密情報を、機密区分に基づく開示可能な範囲の者又は機密文書管理責任者が、業務上開示が必要と認めた者以外に開示、又は漏洩してはならない。
- 3 役職員等は、業務上必要な場合に限り、予め機密文書管理責任者に報告して、その指示に従って機密文書を最低必要部数に限って複写することができる。複写した文書を配布する場合は、連番を付与する等、配布先を特定可能とする措置を講ずる。また、使用終了後は原則として当該文書をすべて回収して破棄する。
- 4 役職員は、機密区分で開示が許可されていない役職員等がいる場所で機密

文書を取り扱う場合、機密文書から離れなければならない状況が発生した場合は、機密文書を施錠できる場所に保管してから離席する等の配慮をしなければならない。

- 5 役職員は、当組合外に機密文書を持ち出すことを原則禁止する。ただし、機密文書管理責任者が業務上、必要と認めた場合にはこの限りでない。

(機密文書の作成および指定)

第 8 条 機密文書の作成及び入手は、必要最低限に留める。

- 2 機密文書管理責任者は、指定帳票を除く、機密文書の内容を評価して、機密区分を指定する。
- 3 機密文書管理担当者は、機密文書について、開示可能な者の範囲及び開示期間等を定めて、機密文書管理責任者に報告する。
- 4 機密文書管理責任者は、報告を受けた機密文書に機密文書指定番号を付与等、機密区分が明確となる措置を実施する。

(機密文書の表示)

第 9 条 前条第 4 項の措置において、以下の事項を明確にするものとする。

- (1) 機密区分
 - (2) 機密文書指定番号
 - (3) 機密取扱期間
 - (4) 開示・使用範囲
- 2 指定帳票は、個別の文書について上記記載事項を省略することができる。

(機密文書の保管)

第 10 条 機密文書は、原則として、当該機密文書を作成、又は入手した部署で所在を明示して、法令の定めた保存期間、法令に定められているものの他は別に定めた保存期間の間保存・管理する。

- 2 保存期間が経過した文書において、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。
- 3 「極秘」、又は「秘密」が指定された機密文書は、保存・管理の状態が確認できるようにする。
- 4 「極秘」、又は「秘密」が指定された機密文書は、キャビネット等の施錠可能な保管庫に、常時施錠して保管・管理する。

5 機密文書の保管庫の施錠・開錠は、管理責任者、又は機密文書管理責任者が文書で指定した担当者が行う。

(機密文書の指定の変更、解除)

第11条 機密文書管理責任者は、機密文書の指定に変更事由が生じた場合、指定の変更、又は解除などの適切な措置を講じる。

(機密文書の引継ぎ)

第12条 人事異動、改組、業務委譲等によって機密文書を他部署に引継ぐ場合は、機密文書引継書を作成して、受領を明確にしなければならない。

(機密文書の廃棄)

第13条 保存期間が経過して廃棄すべき機密文書、又は使用後回収した複写した機密文書は、原則として、保管の所管部門において廃棄処分する。

2 廃棄する機密文書は、シュレッダー等で破碎処理また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。

(非常持出)

第14条 火災または天災等により、滅失毀損した場合、業務上著しく支障をきたす恐れのある機密文書は、専用の容器に入れ、「非常持出」の表示をする等、他の機密文書との区分けを明確にする。

2 「非常持出」の機密文書の保管場所は、火災盗難の予防並びに非常の際に搬出の容易なことを考慮して定める。

附 則

1. この規程は、平成28年4月1日より施行する。

新旧条文対照表

(個人情報保護管理規程)

新

旧

(目的)

第1条 本規程は、「個人情報の保護に関する法律」(平成15年5月30日・法律第57号。以下「法」という。)及び「行政手続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。以下「番号法」という。)、「健康保険組合等における個人情報の適切な取扱いのためのガイドラインについて」(平成16年12月27日保発第1227001号厚生労働省保険局長通知。以下「ガイドライン」という。)、「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」(以下「特定個人情報ガイドライン」という。)、「健康保険組合における個人情報保護の徹底について」(平成14年12月25日保保発第1225001号厚生労働省保険局保険課長通知。以下「保険課長通知」という。)に基づき、個人情報保護の重要性にかんがみ、東京西南私鉄連合健康保険組合(以下「組合」という。)における被保険者及びその被扶養者(以下「被保険者等」という。)等、組合が保有する個人情報の漏えい・滅失又はき損等(以下「漏えい等」という。)を防止し、個人情報保護の徹底を図ることを目的とする。

(個人情報の定義)

第2条 本規程による個人情報とは、法第2条第1項に定める特定の個人を識別することができるものをいい、紙に記載されたものであるか、写真・映像や音声であるか、電子計算機・光学式情報処理装置等のシステムにより処理されているかは問わない。また、この組合における個人情報は原則として別表1に掲げるものとする。

2 本規程による特定個人情報とは、番号法第2条第8項に定める個人番号をその内容に含む個人情報をいう。

3 死者に関する情報は、法の対象外であるが、ガイドラインに基づき、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。

4 前項にかかわらず、個人番号を含む死者に関する情報は生存する者に関する情報と同様に取扱うものとする。

(個人情報の利用目的の特定と公表等)

第3条 個人情報を取り扱うに当たって、その利用目的を別表2においてできる限り特定し、被保険者等本人にわかりやすい形で通知し、またはホームページ、組合・事業所掲示板への掲示、広報紙等で公表する。また、新たに個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を被保険者等本人に通知し、または前記手段等を用いて公表する。

2 組合は、あらかじめ本人の同意なく別表2により定める利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。ただし、利用目的と相当の関連性を有すると合理的に認められる場合は、本人に対し通知又は公表することにより変更できるものとする。

3 前項の規定は、次に掲げる場合については、適用しないものとする。

(1) 法令に基づく場合

(2) 人の生命、身体又は財産の保護のために必要であって、本人の同意を得ることが困難であるとき

(3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき

(4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することにより

(目的)

第1条 本規程は、「個人情報の保護に関する法律」(平成15年5月30日・法律第57号。以下「法」という。)及び「健康保険組合等における個人情報の適切な取扱いのためのガイドラインについて」(平成16年12月27日保発第1227001号厚生労働省保険局長通知。以下「ガイドライン」という。)「健康保険組合等における個人情報保護の徹底について」(平成14年12月25日保保発第1225001号厚生労働省保険局保険課長通知。以下「保険課長通知」という。)に基づき、個人情報保護の重要性にかんがみ、東京西南私鉄連合健康保険組合(以下「組合」という。)における被保険者及びその被扶養者(以下「被保険者等」という。)等、組合が保有する個人情報の漏えい・滅失又はき損等(以下「漏えい等」という。)を防止し、個人情報保護の徹底を図ることを目的とする。

(個人情報の定義)

第2条 本規程による個人情報とは、法第2条第1項に定める特定の個人を識別することができるものをいい、紙に記載されたものであるか、写真・映像や音声であるか、電子計算機・光学式情報処理装置等のシステムにより処理されているかは問わない。

2 死者に関する情報は、法の対象外であるが、ガイドラインに基づき、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。

(個人情報の利用目的の特定と公表等)

第3条 個人情報を取り扱うに当たって、その利用目的をできる限り特定し、被保険者等本人にわかりやすい形で通知し、またはホームページ、組合・事業所掲示板への掲示、広報紙等で公表する。また、新たに個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を被保険者等本人に通知し、または前記手段等を用いて公表する。

当該事務の遂行に支障を及ぼすおそれがあるとき

4 第1項の場合において、特定個人情報の利用目的は、番号法第9条に定める利用範囲において特定しなければならない。

5 第2項、第3項にかかわらず、特定個人情報については本人の同意有無にかかわらず、番号法第9条に定める範囲において特定した利用目的を超えて、取扱ってはならない。

(個人情報の第三者への提供の制限)

第4条 法第23条に定める第三者提供の除外事項等を除き、あらかじめ被保険者等本人の同意を得ないで、個人情報を提供してはならない。ただし、当該個人情報が特定個人情報である場合、本人の同意有無にかかわらず、番号法第19条に定める場合を除き、提供してはならない。

(個人情報の適正な取得及び正確性の確保)

第5条 偽りその他の不正の手段により個人情報を取得してはならない。また、利用目的の達成に必要な範囲内において、個人情報を正確かつ最新の内容に保つよう努めなければならない。

2 特定個人情報については、番号法第19条に定める場合を除き、収集又は保管してはならない。また、本人又は代理人から個人番号の提供を受けるときは、番号法第16条に定める本人確認の措置をとらなくてはならない。

(管理組織)

第6条 個人情報保護に関する管理組織として、個人情報取扱責任者及び個人情報保護管理担当者を設置するものとする。

2 前項に定めるもののほか、管理組織について必要な事項は、理事会において別に定める。

(個人情報取扱責任者及び個人情報保護管理担当者の責務等)

第7条 個人情報取扱責任者は、専務理事が就任するものとし、個人情報保護の徹底が図られるよう、各種安全対策の実施、組合の役職員等に対する教育訓練、外部委託業者の監督、個人情報に関する開示請求や苦情処理等を適切に行うなど個人情報保護に関して必要な措置の全般を管理し、理事長など役員とともに、その責任を負うものとする。

2 個人情報保護管理担当者は、常務理事が就任するものとし、個人情報取扱責任者の指揮のもと、前項に定める個人情報保護に関する必要な措置を実行するものとする。

(個人情報の管理)

第9条 被保険者等の個人情報が記載された文書等(帳票、電子データ等全ての記録様式を含む。以下同じ。)の保管場所については常時施錠し、その鍵の管理は、個人情報取扱責任者が行うものとする。また、個人情報取扱責任者は第7条に定める安全対策として、個人情報が記載、記録された文書等について整理及び保管状況を把握するとともに、電子計算機及び番号法第2条第1項第14号に定める情報提供ネットワークシステムへの接続環境の管理を適正に実施するものとする。

2 前項に定めるもののほか、被保険者等の個人情報への不当なアクセス並びに故意又は過失による虚偽入力、書換え及び消去を防止するため必要な事項に関しては、理事会において別に定める。

(個人情報の廃棄及び消去)

第11条 被保険者等の個人情報が記載された文書等の廃棄を行う場合は、個人情報取扱責任者の指示に従い、個人情報を読取不可能な状態にしなければならない。

2 電子計算機及び光学式情報処理装置の廃棄又は転売・譲渡等(リースの場合は返却)を行う場合は、個人情報取扱責任者の指示に従い、ハードディスク内のデータを復元不可能な状態にしなければならない

(個人情報の第三者への提供の制限)

第4条 法第23条に規定する第三者提供の除外事項等を除き、あらかじめ被保険者等本人の同意を得ないで、個人情報を提供してはならない。

(個人情報の適正な取得及び正確性の確保)

第5条 偽りその他の不正の手段により個人情報を取得してはならない。また、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければならない。

(管理組織)

第6条 組合に個人情報取扱責任者を置き、専務理事をもってこれに充てる。

2 前項に定めるもののほか、管理組織について必要な事項は、理事会において別に定める。

(個人情報取扱責任者の責務)

第7条 個人情報取扱責任者は、個人情報保護の徹底が図られるよう、各種安全対策の実施、組合の役職員に対する教育訓練、外部委託業者の監督、個人情報に関する開示請求や苦情処理等を適切に行い、理事長など役員とともに、その責任を負うものとする。また、個人情報保護に関して必要な事項の全般を管理すること。

(個人情報の管理)

第9条 被保険者等の個人情報が記載された文書等の保管場所については常時施錠し、その鍵の管理は、個人情報取扱責任者が行う。

2 前項に定めるもののほか、被保険者等の個人情報への不当なアクセス並びに故意又は過失による虚偽入力、書換え及び消去を防止するため必要な事項に関しては、理事会において別に定める。

(個人情報の廃棄及び消去)

第11条 被保険者等の個人情報が記載された文書等の廃棄を行う場合は、個人情報取扱責任者の指示に従い、個人情報を読取不可能な状態にしなければならない。

2 電子計算機及び光学式情報処理装置の廃棄又は転売・譲渡等(リースの場合は返却)を行う場合は、個人情報取扱責任者の指示に従い、ハードディスク内のデータを復元不可能な状態にしなければならない

い。

3 特定個人情報については、必要でなくなった場合かつ所管法令で定める保存期間を経過した場合、前二項に定める方法により、可及的速やかに廃棄又は消去しなければならない。

4 前三項に定めるもののほか、個人情報の廃棄及び消去のため必要な事項に関しては、理事会において別に定める。

(教育訓練)

第12条 個人情報取扱責任者は、役職員の採用及び組合会議員の就任に当たり、個人情報保護の重要性等について理解し遵守の徹底が図られるよう必要な研修、教育を実施するほか、随時、役職員及び組合会議員に対し、個人情報保護に関して必要な研修、教育を実施する。

2 前項に定める研修、教育を実施した場合、個人情報取扱責任者または個人情報保護管理担当者は、実施時期、場所、対象者及び内容を記録し保存するものとする。

(外部委託)

第14条 個人情報及び特定個人情報に関する処理は、次の各号に掲げる事項を契約書上に明記することを了承した業者に限り、外部委託することができる。

(1) 法令、関連通知及びガイドライン(当該個人情報が特定個人情報である場合には、特定個人情報ガイドラインを追加する)を遵守し、個人情報の保護に万全を期すこと。また、契約期間終了後においても同様であること。

(2) 被保険者等の個人情報を、組合の事業目的以外に利用しないこと。

(3) 被保険者等の個人情報の漏えい等が生じた場合には、契約を解除すること。

(4) 被保険者等の個人情報の漏えい等により損害が生じた場合には、損害賠償を行うこと。

(5) 組合の個人情報取扱責任者は、随時、委託契約に関する調査を行い、説明を求め及び報告を徴することができること。

(6) 個人情報取扱責任者から問題が指摘された場合には、速やかに必要な措置を行うこと。

(7) 組合との直接の契約関係を伴わない再委託を行わないこと。

(保有個人データの訂正及び利用停止等)

第16条 被保険者等本人から、個人データの内容が事実でないという理由によってデータの内容の訂正、追加又は削除(以下「訂正等」という。)を求められた場合、若しくは個人データが、特定した利用目的の達成に必要な範囲を超えて取扱われる、偽りその他不正の手段により取得される、また特定個人情報が番号法において限定的に明記された場合に違反して違法に第三者に提供されるなどの理由によって、データの利用の停止又は消去(以下「利用停止等」という。)を求められた場合、組合の「保有個人データ(診療報酬明細書等を除く)の開示・訂正・利用停止等に係る取扱要領」に則り処理を行う。

(個人情報相談窓口の設置)

第17条 個人情報の取扱いに関する相談や苦情の適切な処理を行うため、組合に個人情報相談窓口を設置する。

2 被保険者等から苦情等の申し出があった場合は、苦情等の内容を調査、確認のうえ個人情報取扱責任者に報告しなければならない。

い。

3 前二項に定めるもののほか、個人情報の廃棄及び消去のため必要な事項に関しては、理事会において別に定める。

(教育訓練)

第12条 個人情報取扱責任者は、役職員の採用に当たり、個人情報保護の重要性等について理解し遵守の徹底が図られるよう必要な研修を行うほか、随時、役職員及び組合会議員に対し、個人情報保護に関して必要な研修を行う。

(外部委託)

第14条 個人情報に関する処理は、次の各号に掲げる事項を契約書上に明記することを了承した業者に限り、外部委託することができる。

①保険課長通知を遵守し、個人情報の保護に万全を期すこと。また、契約期間終了後においても同様であること。

②被保険者等の個人情報を、組合の事業目的以外に利用しないこと。

③被保険者等の個人情報の漏えい等が生じた場合には、契約を解除すること。

④被保険者等の個人情報の漏えい等により損害が生じた場合には、損害賠償を行うこと。

⑤組合の個人情報取扱責任者は、随時、委託契約に関する調査を行い、説明を求め及び報告を徴することができること。

⑥個人情報取扱責任者から問題が指摘された場合には、速やかに必要な措置を行うこと。

⑦組合との直接の契約関係を伴わない再委託を行わないこと。

(保有個人データの訂正及び利用停止等)

第16条 被保険者等本人から、個人データの内容が事実でないという理由によってデータの内容の訂正、追加又は削除(以下「訂正等」という。)を求められた場合、若しくは個人データが、特定した利用目的の達成に必要な範囲を超えて取扱われる、また、偽りその他不正の手段により取得されるなどの理由によって、データの利用の停止又は消去(以下「利用停止等」という。)を求められた場合、組合の「保有個人データ(診療報酬明細書等を除く)の開示・訂正・利用停止等に係る取扱要領」に則り処理を行う。

(個人情報相談窓口の設置)

第17条 個人情報の取扱いに関する相談や苦情の適切な処理を行うため、組合に個人情報相談窓口を設置する。

別表1 健康保険組合等が保有する個人情報の例

個人情報の種類		個人情報の内容
被保険者	被保険者適用情報	記号・番号、氏名、生年月日、性別、資格取得日、資格喪失日、標準報酬月額、報酬実績、被扶養者の有無
	任意継続被保険者適用情報	記号・番号、氏名、生年月日、性別、資格取得日、資格喪失日、資格喪失時の標準報酬月額、被扶養者の有無
	被保険者レセプト情報	本人・家族区分、診療区分、保険者番号、記号・番号、給付割合、診療年月、府県コード、医療機関コード、氏名、性別、生年月日、特記事項、職務上の事由、医療機関の所在地および名称、診療科、傷病名、診療開始日、転帰、診療実日数、決定点数、公費点数、一部負担金額、患者負担金額、外来負担金額、入院負担金額、高額療養費金額、薬剤負担金額、薬剤負担金額公費分、食事療養日数、食事療養日数公費分、食事療養決定額、食事療養決定額公費分、食事療養標準負担額、食事療養標準負担額公費分、診療内容、画像（レセプト画像）
	被保険者健康診断情報	記号・番号、被保険者・被扶養者・事業所担当者氏名および住所、生年月日、電話番号、事業所名、事業所社員コード、受診費用、健診別給種コード、健診未実施項目、健診種目名、健診受診日、健診機関名、健診機関所在地、画像（レントゲン写真）、相談・指導内容、所見、保健師・看護師名、緊急薬・常備薬購入記録、疾病既往歴、家族既往歴
	被保険者現金給付情報	記号・番号、氏名、生年月日、住所、電話番号、振込口座、受診医療機関名、受診年月、傷病名、給与所得、基礎年金番号、年金額、医療費、装具装着日、装具購入費用、前年度所得（非課税者のみ）、移送費用、証明先医療機関名、労務不能期間、労務不能期間に受けた給与、労務不能期間の出勤状況、出産（予定）日、出生児数、出生児名、続柄、死亡年月日、死亡原因（病名）、除籍謄本記載内容、埋葬に要した費用（埋葬料のみ）、請求者住所・電話番号・振込口座
被保険者柔道整復情報	記号・番号、氏名、生年月日、施術柔道整復師名、柔道整復師登録番号、画像（申請書画像）、施術年月、施術金額、傷病名、柔道整復師の振込先口座	
被扶養者	被扶養者適用情報	氏名、生年月日、性別、被保険者との続柄、職業（学校名）、月平均収入額、同居別居の別
	被扶養者レセプト情報	被保険者レセプト情報と同じ
	被扶養者健康診断情報	被保険者健康診断情報と同じ
	被扶養者現金給付情報	氏名、生年月日、被保険者との続柄、振込口座、受診医療機関名、受診年月、傷病名、前年度所得（非課税者のみ）、医療費、装具装着日、装具購入費用、出産（予定）日、出生児数、出生児名、続柄、死亡年月日、死亡原因（病名）、除籍謄本記載内容
	被扶養者柔道整復情報	記号・番号、氏名、生年月日、施術柔道整復師名、柔道整復師登録番号、画像（申請書画像）、施術年月、施術金額、傷病名、柔道整復師の振込先口座、被扶養者氏名・生年月日、被保険者との続柄

上記のうち、適用及び現金給付情報において個人番号が付された情報については、特定個人情報として取扱うものとする。

別表2 健康保険組合の通常業務で想定される主な利用目的

1. 被保険者等に対する保険給付に必要な利用目的

【健康保険組合等の内部での利用に係る事例】

- ・保険給付及び付加給付の実施

【他の事業者等への情報提供を伴う事例】

- ・高額療養費及び一部負担金還元金等の自動払い
- ・海外療養費にかかる翻訳のための外部委託
- ・第三者行為に係る損保会社等への求償
- ・健保連の高額医療給付の共同事業

2. 保険料の徴収等に必要な利用目的

【健康保険組合等の内部での利用に係る事例】

- ・被保険者資格の確認並びに標準報酬月額及び標準賞与額の把握
- ・健康保険料の徴収
- ・被扶養者の認定
- ・健康保険被保険者証の発行

【他の事業者等への情報提供を伴う事例】

- ・被保険者等資格等のデータ処理の外部委託

3. 保健事業に必要な利用目的

【健康保険組合等の内部での利用に係る事例】

- ・健康の保持・増進のための健診、保健指導及び健康相談

【他の事業者等への情報提供を伴う事例】

- ・保健指導、健康相談に係る産業医への委託
- ・医療機関への健診の委託
- ・健診結果の事業者への提供
- ・被保険者等への医療費通知

4. 診療報酬の審査・支払に必要な利用目的

【健康保険組合等の内部での利用に係る事例】

- ・診療報酬明細書（レセプト）等の内容点検・審査

【他の事業者等への情報提供を伴う事例】

- ・レセプトデータの内容点検・審査の委託
- ・レセプトデータの電算処理のためのパンチ入力、画像取込み処理の委託

5. 健康保険組合の運営の安定化に必要な利用目的

【健康保険組合等の内部での利用に係る事例】

- ・医療費分析・疾病分析

【他の事業者等への情報提供を伴う事例】

- ・医療費分析及び医療費通知に係るデータ処理等の外部委託

6. その他

【健康保険組合等の内部での利用に係る事例】

- ・健康保険組合の管理運営業務のうち、業務の維持・改善のための基礎資料

【他の事業者等への情報提供を伴う事例】

- ・第三者求償事務において、保険会社・医療機関等への相談又は届出等

7. 特定個人情報

番号法第19条第7号において定められた他の医療保険者又は行政機関（以下「他機関」という。）との情報連携における利用目的

【組合の事務処理執行の為、他機関より情報を受ける場合】

- ・傷病手当金、高額療養費等保険給付審査事務にかかる給付情報等
- ・高齢受給者負担区分判定等にかかる課税・非課税情報
- ・被保険者資格取得事務にかかる他機関における資格情報
- ・被扶養者認定事務にかかる課税・非課税、住民票関係情報等

【他機関の事務執行の為、組合が情報を提供する場合】

- ・高額療養費、出産、葬祭関連給付等、他機関の給付事務にかかる組合における保険給付関連情報
- ・資格取得、被扶養者認定等、他機関の資格確認事務にかかる組合における資格取得、被扶養者資格関連情報