

# ジェイティービー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) 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、当該取扱が必要となる業務ごとに「事務担当者」を任免し、アクセス権限を付与する。
- (6) 情報システムのベンダーの基幹システムにおいては、特定個人情報に関わる各種アクセスログについてレポーティング機能を搭載する。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) 離席する際の窃視防止対策として、スクリーンセーバーを設定する。
- (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。なお、ベンダーの基幹系システム利用に関わる通信は専用回線を採用しており、ファイアウォール、IDS(不正検知システム)等による、不正アクセスの遮断・検知に加え、セキュリティパッチ適用による脆弱性対策、ウィルス対策を実施している。
- (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受けるとともに、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、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** ベンダーの基幹系システムについては、非常時の備え情報摂取、情報改竄、業務妨害、情報漏えい、自然災害（局所/広域）、障害について、予防措置と事後対策を定義し、対策を実施している。

- 2 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。
- 3 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、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) 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）

(12) 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。
- 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、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。

### 第4章（物理的な対策）

（入退出管理）

**第14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及び記録媒体を保管する場所を「執務室等」という。
- 2 基幹系システムはベンダーのシステムを使用しているが、サーバーは健保内ではなくベンダー所有のサーバーが多摩市内にある。

- 3 部外者が執務室等に立ち入る場合、入退出記録の作成、同伴等の管理を実施する。  
(定期的に入退出する清掃業者は対象外とする)。
- 4 執務室等は組合員が常駐することとする。
- 5 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。

(執務室等及びサーバー室等の安全管理)

**第15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、入退制限装置による保安処置を講じる。

(PC 端末の安全管理)

**第16条** PC 等の端末は、以下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 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。
- 3 PC 等端末の廃棄は、外部業者に委託している。また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17条** 組合の LAN は JTB グループの基幹ネットワークを利用している。

- 2 事務担当者が私有（組合が支給したもの以外をいう。）の PC を持込み、LAN に接続することは、原則禁止とする。

(外部機関との情報交換)

**第18条** 委託しているベンダーによる外部機関（社会保険診療報酬支払基金、健保連、保健事業実施業者等）との情報交換については、当健保との契約に基づき実施している。併せて、外部機関との情報交換においては、ベンダーが契約のうえ、仮想プライベートネットワーク、若しくは専用回線を用いた上で、通信を暗号化して行っている。当健保における外部機関との情報交換は、契約に基づき安全に運用されるよう対策を講じている。



- 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。

(電子媒体の管理)

**第19条** ベンダーの基幹系システムについては、バックアップ業務以外に外部記憶媒体へのデータ複写は実施していない。データ保護管理者が特に許可した場合を除き、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20条** 情報システムの仕様書は、ベンダーが厳重に管理している。

- 2 システムマニュアルについては、PC内のベンダーのサポートページに最新版を掲載している。

(情報機器のリモートアクセス管理)

**第21条** ベンダーからリモートアクセスする場合は、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22条** 情報システム等で保有するデータ及びに収録されたデータについては、法令の定めた保存期間保存・管理するものとする。但し、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)ベンダーの基幹系システム又は電子媒体で保有するレセプトデータは6年保存後、廃棄する。
  - (2)当健保保有の電子媒体に収録されたデータについては委託業者にて2月、及び8月に廃棄する。但し、それぞれの廃棄月前の直近2ヶ月は直近の廃棄月ではなく次の廃棄月に廃棄する。
  - (3)(1)のバックアップを目的としたデータについては、個人番号は10日間、週次データは1週間、遠隔地バックアップ（大阪）は1ヶ月間保存後廃棄する。
  - (4)電子申請に係る届出書データ及び添付文書については2年間保存後廃棄する。
- 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。
  - 4 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8項に定める個人番号データ（情報システム等で保有するものに限り）については、第1項に定める期間を資格喪失又は扶養削除の日から3年間とする。

## 第5章（技術的な対策）

（アクセス権限等）

- 第23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に交付する。

（サーバー等記録機器の管理）

- 第24条** ベンダーの基幹系システムのサーバー機器については、アクセス状況・稼働状況の常時監視、バックアップの自動化、適正な管理、障害発生時の報告体制、対応手順の整備を行っている。

- 2 ベンダー以外の母体企業のシステム及び健保内の LAN については、JTB グループ本社総務部と連携し指示を仰ぎ対応するものとする。

(ネットワーク管理)

**第25条** 組合の LAN は、JTB グループの基幹ネットワークを利用しており、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 インターネットについては JTB グループの基幹ネットワークを利用している。
- 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) 電子メールは母体企業が導入の Google Apps (G メール) を使用している。メールアドレスは母体企業の JTB グループ本社総務部に申請し、設定・削除を依頼している。
  - (2) 電子メールの私的利用は、禁止とする。
  - (3) 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理等を講ずるなど、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、紛失または誤送に備える。
  - (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。

(ウィルス対策等)

**第26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) ベンダーの基幹システムのサーバー機器のうち必要な機器は、適宜・適切な頻度でセキュリティパッチ、アンチウィルスソフト（パターンファイル含む）を適用している。
  - (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、母体企業が管理している。
- 2 ウィルス対策として、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ない、感染の有無を確認する。
  - (3) アンチウィルスソフトは、常に稼動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) 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27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となる情報（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 7 月 26 日から施行する。
- 2. 第 22 条 1 項 (4) を追加（令和 2 年 11 月 1 日から適用する）
- 3. 第 22 条の(1)の文言を訂正し、令和 4 年 4 月 1 日から施行する。