

特定個人情報保護評価書(重点項目評価書)

評価書番号	評価書名
1	出版健康保険組合における 適用、給付及び徴収関係事務 重点項目評価書

個人のプライバシー等の権利利益の保護の宣言

出版健康保険組合(以下「当組合」という。)は、適用、保険給付及び保険料等徴収関係事務において特定個人情報ファイルを取り扱うに当たり、その取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えい、その他の事態が発生するリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項

- ・特定個人情報を取り扱うことができる組合職員を限定し、他の職員や外部から特定個人情報にアクセスできないよう系統的に制御します。
- ・特定個人情報にアクセスしたとき、いつ・だれが・どこからアクセスをしたのか、システムで操作記録を自動的に残します。
- ・基幹システムと中間サーバー等をサーバー間接続することにより、電子記録媒体等で統合専用端末とのデータ授受を行う業務を減らして、電子記録媒体等への不正な複製や媒体の持出し、紛失等が生じるリスクを軽減しています。

評価実施機関名

出版健康保険組合

公表日

令和2年9月25日

項目一覧

I 基本情報
II 特定個人情報ファイルの概要
(別添1) 特定個人情報ファイル記録項目
III リスク対策
IV 開示請求、問合せ
V 評価実施手続
(別添2) 変更箇所

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	適用、給付及び徴収関係事務
②事務の内容	<p><制度内容> 当組合は健康保険法(大正11年法律第70号)並びに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年法律第27号。以下「番号法」という。)等に基づき、医療保険の運営の効率化、給付の内容及び費用の負担の適正化並びに加入者の健康の維持・増進、加入者が受ける医療の質の向上を図ることを目的としている。 その目的を達成するため当組合では、事業主と被保険者の代表による事業・運営計画の策定、保険料の徴収、保険給付、診療報酬明細書の内容審査、健康診査や体力づくり等の保健事業、加入者への広報活動、診療所や保養施設の運営等を行っている。 また、他の医療保険者等と共同して「被保険者等に係る情報の収集又は整理に関する事務」及び「被保険者等に係る情報の利用又は提供に関する事務」を社会保険診療報酬支払基金(以下「支払基金」という。)に委託することができる旨の規定が健康保険法に盛り込まれ、加入者の資格履歴情報と被保険者枝番の採番管理、地方公共団体等と情報提供ネットワークシステムを通じた情報照会・提供、加入者の本人確認に係る事務、その事務処理に必要な情報提供ネットワークシステムに接続する医療保険者等向け中間サーバー等(以下「中間サーバー等」という。)及び住民基本台帳ネットワークシステムに接続するためのサーバーの運用・管理を支払基金に一元的に委託することが可能になった。</p> <p>当組合の加入者は、全国の出版業等の①事業所の従業者である被保険者及びその被扶養者(一般加入者)、②事業所を退職するまで2ヶ月以上被保険者であった期間があり任意に継続加入を申し出た者及びその被扶養者(任意継続加入者)、③事業所を退職するまで20年以上又は40歳以降10年以上当組合の被保険者であった期間があり特例退職被保険者制度に加入を申し出た者及びその被扶養者(特例退職加入者)で、いずれも後期高齢者医療保険制度の適用年齢75歳に到達すると加入者の資格を喪失する。</p> <p><事務内容> 当組合が行う事務のうち、番号法別表第1の項番2「健康保険法による保険給付の支給、保健事業若しくは福祉事業の実施又は保険料等の徴収に関する事務であって主務省令で定める」事務について、加入者の個人番号等の特定個人情報を以下の範囲で利用する。 なお、健康保険事務に必要な事業所からの届出書の一部について、令和2年11月から事業所が電子データにしてオンラインでマイナポータル(社会保険・税手続オンライン・ワンストップサービス)経由で申請し、それをオンラインで当組合が受け付けすることが可能になる(※1)。</p> <p>1. 適用事務(加入者への保険給付や保険料徴収に当たって適用する資格関係情報等を取り扱う事務)</p> <p>(1)被保険者資格取得、資格喪失、被扶養者の異動等による資格の認定、資格関係情報変更の事務処理に係る個人番号の確認及び資格関係情報等の参照 (2)事業所又は加入者から個人番号が入手できない場合や個人番号又は基本4情報を確認する必要がある場合、住民基本台帳法第30条の9の規定に基づき支払基金を介して地方公共団体情報システム機構から個人番号や基本4情報を入力(※2) (3)平成29年5月以降、情報連携のために加入者の個人番号及び資格関係情報を中間サーバー等に登録して、被保険者枝番を取得し、資格喪失や異動等の資格関係情報に変更があった場合、中間サーバー等の登録情報を更新 (4)他の医療保険者等から異動してきた被保険者やその被扶養者の資格認定に当たり確認情報が必要な場合は、中間サーバー等内で従前に加入していた医療保険者等に情報照会し、資格喪失していることを確認、また、被扶養者の資格認定に必要な課税証明書や住民票等情報は、情報提供ネットワークシステムを利用して当該情報保有機関に情報照会し確認(※3) (5)健康保険被保険者証の再発行や高齢受給者証などの発行・管理事務に係る対象者の確認及び資格関係情報等の参照 (6)月額変更、算定、賞与等の標準報酬に係る届出書について資格関係情報等の参照</p> <p>(※1)マイナポータルは政府が運営するオンラインサービスで、マイナポータルに接続する当組合のオンラインネットワークは、従来から支払基金に接続して使用していたオンライン請求ネットワーク(以下「オンライン請求NW」という。)を利用する。なお、マイナポータルの運営主体は、申請データの中身を閲覧等できないようにシステム上制御されている。 (※2)地方公共団体情報システム機構からの個人番号入手や基本4情報入手は、支払基金経由で中間サーバー等を介して即時照会又はファイル一括照会する。 (※3)従前に加入していた医療保険者等への情報照会は被保険者枝番を用いて支払基金の中間サーバー等内で行い、情報提供ネットワークシステムを通じた当該情報保有機関への情報照会は、被保険者枝番を用いて支払基金の中間サーバー等を介して行う。</p>

5. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	<div style="text-align: right;"><選択肢></div> <div style="text-align: right;">1) 実施する</div> <div style="text-align: right;">2) 実施しない</div> <div style="text-align: right;">3) 未定</div> [実施する]
②法令上の根拠	<p>・番号法 第19条第7号(特定個人情報の提供の制限) (照会)別表第2 項番3 番号法別表第2の主務省令で定める事務及び情報を定める命令 第3条 (提供)別表第2 項番1、2、3、4、5、9、12、15、17、22、26、27、33、39、42、43、58、62、78、80、87、93、97、106、109、120 番号法別表第2の主務省令で定める事務及び情報を定める命令 第1条、第2条、第3条、第4条、第5条、第8条、第10条の2、第11条の2、第12条の3、第15条、第19条、第20条、第22条の2、第24条の2、第25条、第25条の2、第31条の2、第33条、第41条の2、第43条、第44条、第46条、第49条、第53条、第55条の2、第59条の3 (委託の根拠)・健康保険法 第205条の4 第1項及び第2項</p> <p>当組合は、健康保険法の規定に基づき、支払基金に情報提供ネットワークシステムを通じた情報照会・提供事務を委託する。情報提供ネットワークシステムを通じて取得した情報を保険給付の支給等の事務に活用するのは当組合であるが、情報提供ネットワークシステムに接続する主体は支払基金である。</p>
6. 評価実施機関における担当部署	
①部署	企画部
②所属長の役職名	企画部長
7. 他の評価実施機関	
なし	

II 特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
健康保険基幹情報ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	当組合の加入者である一般被保険者及び任意継続被保険者、特例退職被保険者とその被扶養者で、個人番号を有する者。
その必要性	当組合の事務を行う上で、加入者の資格や保険料の賦課・徴収、給付に関する情報を記録・管理する必要があるため。
④記録される項目	[100項目以上] <選択肢> 1) 10項目未満 2) 10項目以上50項目未満 3) 50項目以上100項目未満 4) 100項目以上
主な記録項目 ※	<ul style="list-style-type: none"> ・識別情報 [<input type="checkbox"/>] 個人番号 [<input type="checkbox"/>] 個人番号対応符号 [<input type="checkbox"/>] その他識別情報(内部番号) ・連絡先等情報 [<input type="checkbox"/>] 4情報(氏名、性別、生年月日、住所) [<input type="checkbox"/>] 連絡先(電話番号等) [<input type="checkbox"/>] その他住民票関係情報 ・業務関係情報 [<input type="checkbox"/>] 国税関係情報 [<input type="checkbox"/>] 地方税関係情報 [<input type="checkbox"/>] 健康・医療関係情報 [<input type="checkbox"/>] 医療保険関係情報 [<input type="checkbox"/>] 児童福祉・子育て関係情報 [<input type="checkbox"/>] 障害者福祉関係情報 [<input type="checkbox"/>] 生活保護・社会福祉関係情報 [<input type="checkbox"/>] 介護・高齢者福祉関係情報 [<input type="checkbox"/>] 雇用・労働関係情報 [<input type="checkbox"/>] 年金関係情報 [<input type="checkbox"/>] 学校・教育関係情報 [<input type="checkbox"/>] 災害関係情報 [<input type="checkbox"/>] その他 ()
その妥当性	<ul style="list-style-type: none"> ・個人番号: 対象者を正確に特定するために記録するもの。 ・その他識別情報(内部番号): 既存システムの識別番号を個人番号と紐付け、資格や保険料の賦課・徴収、給付に関する情報を管理するために記録するもの。 ・基本4情報、連絡先: 被保険者について、通知及び照会を行うために記録するもの。 ・医療保険関係情報: 保険料の賦課・徴収、給付に関する事務処理を行い、通知及び照会を行うために記録するもの。
全ての記録項目	別添1を参照。
⑤保有開始日	平成28年10月1日
⑥事務担当部署	業務部 適用課 業務部 給付課 大阪支部 業務課

3. 特定個人情報の入手・使用									
①入手元 ※	<input type="checkbox"/> 本人又は本人の代理人 <input type="checkbox"/> 評価実施機関内の他部署 () <input type="checkbox"/> 行政機関・独立行政法人等 (日本年金機構、日本私立学校振興・共済事業団) <input type="checkbox"/> 地方公共団体・地方独立行政法人 (市町村、後期高齢者医療広域連合) <input type="checkbox"/> 民間事業者 (加入事業所) <input type="checkbox"/> その他 (地方公共団体情報システム機構、国家公務員共済組合、国家公務員共済組合連合会、地方公務員共済組合、地方公務員災害補償基金、全国健康保険協会、国民健康保険組合、当組合以外の健康保険組合)								
②入手方法	<input type="checkbox"/> 紙 [<input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。)] [<input type="checkbox"/> フラッシュメモリ] <input type="checkbox"/> 電子メール [<input type="checkbox"/> 専用線] [<input type="checkbox"/> 庁内連携システム] <input type="checkbox"/> 情報提供ネットワークシステム <input type="checkbox"/> その他 (住民基本台帳ネットワークシステム、マイナポータル)								
③使用目的 ※	<p>I 基本情報「1. 特定個人情報ファイルを取り扱う事務 ②事務の内容」に記載した、</p> <ol style="list-style-type: none"> 加入者資格情報の更新管理、健康保険被保険者証等の発行・管理、異動・標準報酬関係届出書の資格情報確認 給付申請帳票の資格情報確認・審査、給付金計算及び限度額適用認定証等の発行・管理 保険料徴収や未納管理の事務処理で、個人番号を既存システムの識別番号と紐付けて必要な情報の検索・参照を行うことに使用する。 <p>また、資格認定事務で従前に加入していた医療保険者等の資格喪失情報が必要なときは従前の医療保険者等に情報照会を行い、被扶養者の資格認定や給付決定等の審査事務に他の情報保有機関の情報が必要なときは当該情報保有機関に情報照会を行い、取得した情報を被保険者枝番と紐付けた既存システムの識別番号で当該加入者の申請情報と照合・確認することに使用する。</p>								
④使用の主体	使用部署	業務部 適用課 業務部 給付課 大阪支部 業務課							
	使用者数	[10人以上50人未満] <table border="0" style="margin-left: 20px;"> <tr> <td colspan="2" style="text-align: center;"><選択肢></td> </tr> <tr> <td>1) 10人未満</td> <td>2) 10人以上50人未満</td> </tr> <tr> <td>3) 50人以上100人未満</td> <td>4) 100人以上500人未満</td> </tr> <tr> <td>5) 500人以上1,000人未満</td> <td>6) 1,000人以上</td> </tr> </table>	<選択肢>		1) 10人未満	2) 10人以上50人未満	3) 50人以上100人未満	4) 100人以上500人未満	5) 500人以上1,000人未満
<選択肢>									
1) 10人未満	2) 10人以上50人未満								
3) 50人以上100人未満	4) 100人以上500人未満								
5) 500人以上1,000人未満	6) 1,000人以上								
⑤使用方法	<p>I 基本情報「1. 特定個人情報ファイルを取り扱う事務 ②事務の内容」に記載した事務処理の、</p> <ol style="list-style-type: none"> 加入者資格情報の更新管理、健康保険被保険者証等の発行・管理、異動・標準報酬関係届出書の資格情報確認 給付申請帳票の資格情報確認・審査、給付金計算及び限度額適用認定証等の発行・管理の資格情報確認 保険料徴収の資格情報確認、保険料収納情報確認による未納管理で、個人番号を既存システムの識別番号と紐付け、必要な情報を健康保険基幹情報ファイルから検索・参照する。 <p>また、資格認定事務で従前に加入していた医療保険者等の資格喪失情報が必要なときは被保険者枝番を用いた照会データで中間サーバー等内で情報照会を行い、被扶養者の資格認定や給付決定等の審査事務に他の情報保有機関の情報が必要なときは被保険者枝番を用いた照会データを中間サーバー等で機関別符号を用いた照会データに変換し情報提供ネットワークシステムで情報照会を行い、取得した情報を被保険者枝番と紐付けた既存システムの識別番号で当該加入者の申請情報と照合・確認する。</p>								
	情報の突合	<ul style="list-style-type: none"> 個人番号が記載された届出書の受付・登録処理を行う際に、個人番号に紐付けられた既存システムの識別番号により基幹システムで管理している資格等の情報と突合することにより、正確な加入者の確認や業務データの審査・内容確認を行う。 異動により既存システムの識別番号が変更されているとき、異動前の資格情報項目と突合して同一人を名寄せし、必要な情報の履歴の参照を行う。 任意継続又は特例退職被保険者の加入処理を行う際に、それまで被保険者であった期間の資格情報項目と突合して同一人の名寄せをし、正確な審査を行うために加入期間や被扶養者等を参照・確認する。 資格認定事務で従前に加入していた医療保険者等の資格喪失情報が必要なときは被保険者枝番を用いた照会データで中間サーバー等内で情報照会を行い、被扶養者の資格認定や給付決定等の審査事務に他の情報保有機関の情報が必要なときは被保険者枝番を用いた照会データを中間サーバー等で機関別符号を用いた照会データに変換し情報提供ネットワークシステムで情報照会を行い、取得した情報を被保険者枝番と紐付けた既存システムの識別番号で当該加入者の申請情報と照合・確認する。 							
⑥使用開始日	平成28年10月1日								

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	[委託する] <選択肢> 1) 委託する 2) 委託しない (5) 件	
委託事項1	基幹システム導入、保守・改修、障害調査等	
①委託内容	基幹システムの導入・設定作業、定期保守・点検、障害調査や復旧等の作業	
②委託先における取扱者数	[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
③委託先名	公益財団法人日本生産性本部 ICT・ヘルスケア推進部	
再委託	④再委託の有無 ※	[再委託しない] <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項2	中間サーバー等における資格履歴管理事務	
①委託内容	個人番号を利用した加入者資格の履歴管理、被保険者枝番の採番管理、被保険者枝番と個人番号との紐付管理、及び資格履歴情報をオンライン資格確認等システムに登録	
②委託先における取扱者数	[50人以上100人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
③委託先名	支払基金	
再委託	④再委託の有無 ※	[再委託する] <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	委託先の支払基金から再委託先の商号又は名称、住所、再委託する理由、再委託する業務及び取り扱う特定個人情報の範囲、再委託先に係る業務の履行能力、再委託先への立入調査に係る要件、その他当組合が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図(委託先による再委託先に対する監督体制を含む。)の提出を受け、支払基金と再委託先が秘密保持に関する契約を締結していること等、再委託先における安全管理措置を確認し、決裁等必要な手続を経た上で、再委託を許諾する。(再委託先が更に再委託する場合も同様とする。)
	⑥再委託事項	中間サーバー等の運用・保守業務
委託事項3	中間サーバー等における情報提供ネットワークシステムを通じた情報照会・提供事務	
①委託内容	情報提供ネットワークシステムを使用した情報照会・情報提供、情報照会・情報提供を行うために必要となる機関別符号の取得及び管理	
②委託先における取扱者数	[50人以上100人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上	
③委託先名	支払基金	
再委託	④再委託の有無 ※	[再委託する] <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	委託先の支払基金から再委託先の商号又は名称、住所、再委託する理由、再委託する業務及び取り扱う特定個人情報の範囲、再委託先に係る業務の履行能力、再委託先への立入調査に係る要件、その他当組合が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図(委託先による再委託先に対する監督体制を含む。)の提出を受け、支払基金と再委託先が秘密保持に関する契約を締結していること等、再委託先における安全管理措置を確認し、決裁等必要な手続を経た上で、再委託を許諾する。(再委託先が更に再委託する場合も同様とする。)
	⑥再委託事項	中間サーバー等の運用・保守業務

委託事項4		中間サーバー等における本人確認事務
①委託内容		地方公共団体情報システム機構から住民基本台帳ネットワークシステムを使用した個人番号取得及び本人確認情報の取得
②委託先における取扱者数		[50人以上100人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
③委託先名		支払基金
再委託	④再委託の有無 ※	[再委託する] <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	委託先の支払基金から再委託先の商号又は名称、住所、再委託する理由、再委託する業務及び取り扱う特定個人情報の範囲、再委託先に係る業務の履行能力、再委託先への立入調査に係る要件、その他当組合が求める情報について記載した書面による再委託申請及び再委託に係る履行体制図(委託先による再委託先に対する監督体制を含む。)の提出を受け、支払基金と再委託先が秘密保持に関する契約を締結していること等、再委託先における安全管理措置を確認し、決裁等必要な手続を経た上で、再委託を許諾する。(再委託先が更に再委託する場合も同様とする。)
	⑥再委託事項	中間サーバー等の運用・保守業務
委託事項5		帳票類のデータ入力業務
①委託内容		資格取得届、算定届等の紙帳票からデータ入力によるデータファイル作成
②委託先における取扱者数		[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
③委託先名		株式会社 コンピュータービジネス
再委託	④再委託の有無 ※	[再委託しない] <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項6～10		

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	[<input checked="" type="checkbox"/>] 提供を行っている (26) 件 [<input type="checkbox"/>] 移転を行っている () 件 [<input type="checkbox"/>] 行っていない
提供先1	番号法第19条第7号 別表第2に定める各情報照会者 (別紙1「特定個人情報の提供先一覧」を参照)
①法令上の根拠	番号法第19条第7号 別表第2の各項 (別紙1「特定個人情報の提供先一覧」を参照)
②提供先における用途	番号法第19条第7号 別表第2に定める各事務 (別紙1「特定個人情報の提供先一覧」を参照)
③提供する情報	番号法第19条第7号 別表第2に定める各特定個人情報 (別紙1「特定個人情報の提供先一覧」を参照)
④提供する情報の対象となる本人の数	[10万人以上100万人未満] <div style="text-align: right;"> <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上 </div>
⑤提供する情報の対象となる本人の範囲	当組合の加入者である一般被保険者及び任意継続被保険者、特例退職被保険者とその被扶養者で、個人番号を有する者。
⑥提供方法	[<input checked="" type="checkbox"/>] 情報提供ネットワークシステム [<input type="checkbox"/>] 専用線 [<input type="checkbox"/>] 電子メール [<input type="checkbox"/>] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ [<input type="checkbox"/>] 紙 [<input type="checkbox"/>] その他 ()
⑦時期・頻度	情報提供ネットワークシステムを通じて他の情報保有機関からの情報提供の求めを受け付けた都度
提供先2～5	
提供先6～10	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[] <div style="text-align: right;"> <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上 </div>
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[<input type="checkbox"/>] 庁内連携システム [<input type="checkbox"/>] 専用線 [<input type="checkbox"/>] 電子メール [<input type="checkbox"/>] 電子記録媒体(フラッシュメモリを除く。) [<input type="checkbox"/>] フラッシュメモリ [<input type="checkbox"/>] 紙 [<input type="checkbox"/>] その他 ()
⑦時期・頻度	
移転先2～5	
移転先6～10	

6. 特定個人情報の保管・消去

保管場所 ※

○当組合のセキュリティ管理区域は「特定個人情報を取り扱う事務を実施する区画又は、特定個人情報を取り扱う情報システムを管理する区画」である。

○特定個人情報ファイルは「サーバー室」内のサーバーに保管し、個人番号が記載された届出書等の帳票類及び電子記録媒体もセキュリティ管理区域内に設置した保管庫に保管する。
なお、基幹システム専用端末や基幹システムに接続していない事務用PC、事務デスク内には一切保管・留置しないよう規制している。

【本部】

組合事務室：セキュリティドアによる立入りの制限、委託業者の訪問時の記録管理

セキュリティ管理区域：パーティションで包囲

サーバー室：セキュリティドアの施錠による立入りの制限、担当職員の入退室を記録管理

保管庫：管理者による施錠管理、入出庫の記録管理

【大阪支部】

組合事務室：セキュリティドア等による立入りの制限、委託業者の訪問時の記録管理

セキュリティ管理区域：パーティション等で包囲

保管庫：管理者による施錠管理、入出庫の記録管理

※電子申請された届出書データは、基幹システムで保管・管理する。

<中間サーバー等における措置>

①中間サーバー等の運用支援環境の設置場所は、取りまとめ機関が所有のサーバー環境(オンプレミス環境)の場合、セキュリティを確保したサーバー室に設置し、許可された者のみが入退室できる管理対象区域にて設置する。また、クラウド環境の場合、クラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。

②特定個人情報は、運用支援環境(情報提供サーバー)のデータベース内に保存され、バックアップもデータベース上に保存される。

7. 備考

なし

(別添1) 特定個人情報ファイル記録項目

健康保険基幹情報ファイル

※ 中間サーバー等に保存される「委託区画ファイル」、「副本区画ファイル」は、基幹システムで扱う特定個人情報ファイル(健康保険基幹情報ファイル)の副本であることから、一体のものとして評価を行っている。

【通用ファイル】

<加入者情報項目>	
証記号番号+枝番	
識別番号	
氏名	
カナ氏名	
性別	
生年月日	
加入区分(強制・任継・特退)	
本支部コード	
事業所コード	
続柄コード	
続柄枝番	
資格取得年月日	
取得理由	
資格喪失年月日	
喪失理由	
所属コード	
社員コード	
郵便番号	
住所	
電話番号	
喪失予定年月日	
改定年月	
改定区分	
標準報酬月額	
報酬実額	
賞与支払額	
賞与支払年月日	
<被保険者証項目>	
交付年月日-回収年月日	
有効開始年月日-終了年月日	
券面記載氏名、カナ氏名	
<高齢受給者証項目>	
交付年月日-回収年月日	
収入基準開始年月-終了年月日	
一部負担金割合	
<限度額適用認定証項目>	
交付年月日-回収年月日	
発効年月日-終了年月日	
適用区分	
長期入院該当年月日	
<特定疾病療養受療証項目>	
交付年月日-回収年月日	
発効年月日-終了年月日	
認定疾病区分	
自己負担限度額	
<一部負担金等免除証明項目>	
交付年月日-回収年月日	
免除開始年月日-終了年月日	
<特定疾患受給者項目>	
該当年月日-不該当年月日	
<公費項目>	
公費負担者番号	
該当年月日-不該当年月日	
<届出記録項目>	
氏名変更年月日	
産前産後休業開始年月日	
産前産後休業終了予定年月日	
産前産後休業終了年月日	
育児休業開始年月日	
育児休業終了予定年月日	
育児休業終了年月日	
法118条該当年月日-不該当年月日	
介護適用除外該当年月日	
介護適用除外非該当予定年月日	
介護適用除外非該当年月日	

【徴収ファイル】

<任意継続・特例退職保険料管理項目>	
識別番号	
前納区分(任継・特退)	
保険料収納記録(任継・特退)	
改定年月	
改定区分	
標準報酬月額	
【給付ファイル】	
<通用情報>	
識別番号	
<高額介護合算療養費項目>	
給付年度	
自己負担額計算対象年月日(自-至)	
自己負担額合計	
自己負担額高齢者分再掲	
<療養費(本人・家族)支給項目>	
診療の期間(自-至)	
診療の日数	
請求額	
支給額	
支給年月日	
<移送費(本人・家族)支給項目>	
移送期間(自-至)	
移送回数	
請求額	
支給額	
支給年月日	
<傷病手当金支給項目>	
療養のため休んだ(請求)期間(自-至)	
療養のため休んだ(請求)日数	
支給開始年月日	
支給額	
支給年月日	
支給日数	
支給期間(自-至)	
<埋葬料(費)(本人・家族)支給項目>	
死亡年月日	
埋葬年月日	
埋葬費用	
支給額	
支給年月日	
<出産育児一時金(本人・家族)支給項目>	
出産年月日	
生産児数	
死産児数	
支給額	
支給年月日	
<出産手当金支給項目>	
出産年月日	
出産のため休んだ(請求)期間(自-至)	
出産のため休んだ(請求)日数	
支給額	
支給年月日	
支給日数	
支給期間(自-至)	
<高額療養費(本人・家族)支給項目>	
診療の期間(自-至)	
診療の日数	
決定点数	
自己負担限度額	
支給額	
支給年月日	

【情報提供等記録項目】

処理番号
処理番号の枝番
事務名称
事務手続名称
情報照会者部署名称
情報提供者部署名称
提供の求めの日時
提供の日時
特定個人情報名称
不開示コード
過誤事由コード
被保険者枝番

【本人確認項目】

その他条件 履歴情報
その他条件 消除者
その他条件 異動事由
主たる照会条件
事務区分(住基法)
事務区分(番号法)
住所
住所(大字以降)
住民区分
個人番号
利用事由
変更状況
市町村コード
市町村名
性別
情報表示
氏名
氏名かな
照会対象期間終了 年月日
照会対象期間開始 年月日
照会対象期間(照会基準日)
生存状況
生年月日
異動事由
異動年月日
異動有無
要求レコード番号

【個人番号管理ファイル】

<個人番号管理テーブル>	
個人番号	
被保険者枝番	
識別番号	
理由コード	
理由	
郵便番号	
住所	
<個人番号記録>	
登録日	
変更日	
前個人番号	
削除日	
<「被保険者枝番」記録>	
登録日	
変更日	
削除日	

※個人番号と紐付ける
既存システムの「識別番号」

証記号番号+枝番・続柄コード・続柄枝番

特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置

【不適切な方法で入手が行われることを防止するための措置】

- 本人から個人番号を入手する場合の措置(郵送又は対面による入手)
 - ・機関誌や当組合Web等に、届出書の提出は郵送又は対面により組合に提出することを明示して周知を図り、それ以外の方法では入手を行わない。
 - ・郵送又は対面により個人番号を記載した届出書の受付をする際、番号法第16条(本人確認の措置)に則り本人確認書類を提出させて本人確認を行い、本人確認ができない場合は受け付けない。
- 加入事業所から個人番号を入手する場合の措置※
 - ・機関誌や当組合Web等で、事業所が被保険者から個人番号の提出を受ける際、番号法第16条(本人確認の措置)に則り本人確認を実施するよう収集要領に記載して周知し、これを求める。
 - ・届出書に事業所名、届出書作成者氏名の記載を求めて、真正性を確認する。
 - ・事業所が電子記録媒体で届出書を届け出る場合、取り決めたパスワード、暗号化処置をした媒体以外は受け付けない。
- ※電子申請された届出書の受け付け(入手)も上記と同様の措置をとる。また、電子申請データは、電子証明書又は法人認証基盤によって申請者(加入事業所等)の身元確認がされたデータをマイナポータルからオンライン請求NWを通じてのみ受け付ける。
- 地方公共団体情報システム機構から支払基金経由で機構保存本人確認情報をオンラインで入手する場合の措置
 - <中間サーバー等における措置>
 - ・個人番号の入手は統合専用端末を経由した方法でのみ行われるため、不適切な方法で入手が行われることはない。

【入手の際に特定個人情報が漏えい・紛失することを防止するための措置】

- 本人から個人番号を入手する場合の措置(郵送又は対面による入手)
 - ・特定個人情報が記載された届出書は管理簿に記載して保管庫に施錠保管する。また、届出書を使用後は文書保存管理規程に従って保管及び廃棄措置する。
- 加入事業所から個人番号を入手する場合の措置※
 - ・事業所から届けられた届出書は送付伝票と内容・数量を照合確認した上で、受付簿に登録する。
 - ・特定個人情報が記載された届出書は管理簿に記載して保管庫に施錠保管する。また、届出書を使用後は文書保存管理規程に従って保管及び廃棄措置をする。
 - ・事業所から入手した電子記録媒体は媒体管理簿に記載し、保管庫に施錠保管する。
 - ・電子記録媒体に記録されたデータは、事前にウイルスチェックを行い、読み込んだ件数を事業所に書類で知らせて相違ないか確認する。
 - ・保管する必要がない使用済の電子記録媒体は、工具又はメディアシュレッダーで物理的に破壊して廃棄し、廃棄記録を管理簿に記載する。
- ※電子申請された届出書の受け付け(入手)
 - ・事業所は、TSL/SSLによる暗号化でセキュリティを確保した届出データをマイナポータル経由で申請することとする。
 - ・当組合が、マイナポータル経由でオンライン請求NWにより届出データを受け付けし基幹システムに登録する処理等は、権限を付与された必要最小限の職員等だけが行えるようシステムの的に制御する。
 - ・なお、オンライン請求NWはIP-VPNによる閉鎖された通信回線で、通信内容の秘匿や盗聴防止の対応がされている。
- 入手した情報の登録・確認をする基幹システム専用端末における措置
 - ・基幹システム専用端末にはウイルス対策ソフトを導入してパターンファイルを随時更新しておく。
 - ・統合専用端末との情報授受については、操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読み出し等ができないようシステムの的に制御する。
 - ・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。
 - ・基幹システム専用端末はインターネット等外部ネットワークと隔離する。
 - ・特定個人情報にアクセスする権限が与えられていない職員等が専用端末を使用する場合、特定個人情報へのアクセスができないようシステムの的に制御する。
- 電子申請された届出書を受け付けるマイナポータル連携サーバー及びレセオン端末
 - ・マイナポータル連携サーバー及びレセオン端末にはファイアウォール、ウイルス対策ソフトを導入してパターンファイルを随時更新しておく。
 - ・マイナポータル連携サーバー及びレセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークやシステムとは分離する。
 - ・マイナポータル連携サーバー及びレセオン端末は、使用権限を付与された必要最小限の職員等だけが操作できるようシステムの的に制御する。
- 地方公共団体情報システム機構から支払基金経由で機構保存本人確認情報をオンラインで入手する場合の措置
 - <中間サーバー等における措置>
 - ・中間サーバー等と当組合の通信は、VPN等の技術を用いた専用線を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。

3. 特定個人情報の使用

リスク1: 目的を超えた紐付け、事務に必要なない情報との紐付けが行われるリスク

<p>リスクに対する措置の内容</p>	<p>【目的外の紐付けを防止するための措置】</p> <ul style="list-style-type: none"> ・基幹システムは、識別番号と個人番号を紐付けて管理し参照が可能であるが、個人番号を用いない事務処理においては、個人番号にアクセスできないようシステムの的に制御する。 ・特定個人情報ファイルを取り扱う事務に記載した事務においても、ログイン時には個人番号のアクセスや個人番号の入力、参照、表示等の紐付け機能を遮断した状態に設定されていて、必要がある場合のみアクセス権限がある職員等に限って設定を切り替え紐付けできるようシステムの的に制御する。 ・特定個人情報にアクセス権限のない職員等がシステム操作をする場合、いかなる方法によっても個人番号にアクセスできず、個人番号の参照、表示等、紐付けができないようシステムの的に制御する。 <p>【事務に必要なない情報との紐付けを防止するための措置】</p> <ul style="list-style-type: none"> ・特定個人情報ファイルを取り扱う事務に記載した事務以外は、いかなる方法によっても個人番号のアクセスや個人番号の入力、参照、表示等ができないようシステムの的に制御する。 ・特定個人情報にアクセス権限のない職員等がシステム操作する場合、全ての事務処理において個人番号にアクセスできず、個人番号の参照、表示等ができないようシステムの的に制御する。
<p>リスクへの対策は十分か</p>	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] <選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	<p>○基幹システムにおける措置※</p> <ul style="list-style-type: none"> ・全てのシステム利用者に発効するユーザID及び登録されたパスワードでログイン認証を行う。 ・共有のユーザIDは使用しないこととする。 ・全てのシステム利用者に、各人が取り扱うことができる事務の範囲及び個人番号取扱い権限(アクセス権限)の有無を決定し、ユーザIDと合わせて管理簿に記載、管理する。 ・アクセス権限が付与されたシステム利用者以外は個人番号を取り扱えないようシステム管理・制御機能に設定して、系統的に制御する。 ・アクセス権限を付与するシステム利用者は最小限に限定する。 ・パスワードに有効期間を設けて、定期的に変更するよう系統的に制御する。 ・退職や異動でシステム利用者でなくなった者のユーザIDは利用できないようシステム管理・制御機能から抹消する。 <p>※電子申請された届出書を受け付けし基幹システムに登録処理等を行う職員等のユーザID認証管理も、上記<基幹システムにおける措置>と同様に行う。 なお、マイナポータルにログインする当組合のユーザIDの管理は、健保連により行われる。</p> <p>○取りまとめ機関及び中間サーバー等における措置</p> <p><取りまとめ機関が定める当組合の運用における措置></p> <ul style="list-style-type: none"> ・中間サーバー等を利用する職員等を限定し、取り扱うことができる事務の範囲及び個人番号取扱い権限(アクセス権限)の有無を決定して、ユーザIDと合わせて管理簿に記載、管理する。 ・共用のユーザIDの使用を禁止する。 ・パスワードに設けられた有効期間に沿って、定期的に変更を行う。 ・退職や異動でシステム利用者でなくなった者のユーザIDは利用できないよう登録を抹消する。 <p><中間サーバー等における措置></p> <ul style="list-style-type: none"> ・統合専用端末又はサーバー間接続を利用したシステム操作や特定個人情報等へのアクセスを行う前にログイン操作を行い、操作者を認証するよう中間サーバー等で制御している。
その他の措置の内容	<p>【アクセス権限の発効・失効管理】</p> <p>○基幹システムにおける措置※</p> <ul style="list-style-type: none"> ・採用や異動等で適用、給付、徴収担当となる職員等には、担当となる日から有効なアクセス権限を、データ保護管理者の指示によりデータ保護担当者がシステム管理・制御機能に設定し、管理簿に記載する。 ・異動や退職等で担当から外れる職員等には、異動日や退職日をもって現在のアクセス権限が失効するよう、データ保護管理者の指示によりデータ保護担当者がシステム管理・制御機能の設定を変更し、管理簿に記載する。 <p>※電子申請された届出書を受け付けし基幹システムに登録処理等を行う職員等のアクセス権限の発効・失効管理も、上記<基幹システムにおける措置>と同様に行う。 なお、マイナポータルにログインする当組合のアクセス権限の発行・失効は、健保連に申請して行う。</p> <p>○取りまとめ機関及び中間サーバー等における措置</p> <p><取りまとめ機関が定める当組合の運用における措置></p> <ul style="list-style-type: none"> ・アクセス権限は、データ保護管理者が各職員等の担当事務分野とアクセス権限を決定し、基幹システムにおけるユーザ認証の管理やアクセス権限の発効・失効と同様に管理する。 <p>(1)発効管理</p> <ul style="list-style-type: none"> ・採用や異動等で中間サーバー等を利用する事務を担当する職員等には、担当となる日から有効なアクセス権限を、データ保護管理者の指示により登録し、管理簿に記載する。 <p>(2)失効管理</p> <ul style="list-style-type: none"> ・異動や退職等で担当から外れる職員等には、異動日や退職日をもって現在のアクセス権限が失効するよう、データ保護管理者の指示により登録を変更し、管理簿に記載する。 <p><中間サーバー等における措置></p> <p>当組合のデータ保護担当者が統合専用端末において以下の管理を行う。</p> <ul style="list-style-type: none"> ・IDは、ID付与権限をもったデータ保護担当者用IDと一般的なユーザIDがある。 ・支払基金が各医療保険者等のデータ保護担当者用IDに対して一般的なIDの付与権限を与えることにより、各医療保険者等においてデータ保護担当者が職員に対して一般的なユーザIDを付与することが可能となる。 ・指定日から職員IDを有効にしたり無効とするよう中間サーバー側で制御している。 ・パスワードを定期的に更新するよう中間サーバー側で制御している。 ・パスワードの最長有効期限を定めている。

	<p>【アクセス権限の管理】</p> <p>○基幹システムにおける措置※</p> <ul style="list-style-type: none"> ・ユーザID、アクセス権限の発効や更新は、データ保護担当者以外には行えないものとする。 ・データ保護担当者は、ユーザIDやアクセス権限の発効や更新を行う都度、データ保護管理者の確認を得て管理簿に記載し保管する。 ・データ保護担当者は随時、不要なユーザIDの残存や不必要なアクセス権限の付与等、管理簿の点検・見直しを行う。 ・パスワードに有効期間を設けて、定期的に変更するようシステム的に制御する。 <p>※電子申請された届出書を受け付けし基幹システムに登録処理等を行う職員等のアクセス権限の管理も、上記<基幹システムにおける措置>と同様に行う。</p> <p>なお、マイナポータルにログインする当組合のパスワードは、設けられた有効期間に沿って定期的に変更を行う。</p> <p>○取りまとめ機関及び中間サーバー等における措置</p> <p><取りまとめ機関が定める当組合の運用における措置></p> <ul style="list-style-type: none"> ・ユーザID、アクセス権限の登録や変更は、データ保護担当者以外には行えないものとする。 ・データ保護担当者は、ユーザIDやアクセス権限の登録や変更を行う都度、データ保護管理者の確認を得て管理簿に記載し保管する。 ・データ保護担当者は随時、不要なユーザIDの残存や不必要なアクセス権限の付与等、管理簿の点検・見直しを行う。 ・パスワードに設けられた有効期間に沿って、定期的に変更を行う。 <p><中間サーバー等における措置></p> <ul style="list-style-type: none"> ・該当する当組合の職員等に許可された業務メニューのみ表示するよう中間サーバー等で制御している。
<p>リスクへの対策は十分か</p>	<p>[十分である] <選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置

【従業者が事務外で使用することを防止する措置】

○基幹システムにおける措置

- ・アクセス権限がある職員等でも、I 基本情報「1. 特定個人情報ファイルを取り扱う事務」に記載した事務以外では個人番号や特定個人情報ファイルにアクセスできないようシステムの的に制御する。
- ・統合専用端末との情報授受については、操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システム専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステムの的に制御する。
- ・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。

小限の職員等だけが当該端末を操作できるようアクセス制御する。

- ・電子記録媒体等の管理簿と操作ログの突合等、定期的にチェックし、必要のないアクセスが行われていないか監視する。
- ・職員等に対して、特定個人情報の適切な取扱いを理解させることを目的として定期的に教育、研修を行う。

○電子申請された届出書の受け付けにおける措置

- ・電子申請された届出書を受け付けし基幹システムに登録処理等を行うのは、アクセス権限を付与された必要最小限の職員等に限定し、アクセス権限が付与された職員等でも限定された端末以外からは電子申請データにアクセスできないようシステムの的に制御する。
- ・電子申請データをフラッシュメモリに一時的に複写するときは、アクセス権限を付与された職員等が事前にデータ保護管理者の承認を得て、データ保護担当者がパスワード設定した媒体の使用を管理簿に記載して行い、処理に使用後速やかに媒体からデータを完全に消去して返却し、データ保護管理者はそれを確認する。

・電子申請データをレセオン端末に取得後、レセオン端末内の電子データは速やかに削除する。

- ・電子記録媒体等の管理簿と操作ログの突合等、定期的な操作ログのチェックや、職員等に対する教育、研修は上記<基幹システムにおける措置>と同様に行う。

○中間サーバー等における措置

- ・統合専用端末又はサーバー間接続を利用した情報照会依頼時等において、当組合の職員に許可された事務／事務手続のみ取り扱うことができるよう中間サーバー等で制御している。

【特定個人情報ファイルが不正に複製されることを防止する措置】

○基幹システムにおける措置

- ・統合専用端末との情報授受については、操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システム専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステムの的に制御する。

・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。

・電子記録媒体及びフラッシュメモリの利用記録等は媒体管理簿に記載し、保管庫に施錠保管する。

- ・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去した証明書類の提出や疑義が生じた際の立入調査等を条件にリース業者や廃棄業者に引渡し、証明書類で確認する。

条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を媒体管理簿に記載する。

・廃棄する電子記録媒体及びフラッシュメモリは工具又はメディアシュレッダーで物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載する。

- ・電子記録媒体等の管理簿と操作ログの突合等、定期的に操作ログをチェックし、データ抽出等の不正な持出しが行われていないか監視する。

○電子申請された届出書の受け付けにおける措置

・電子申請された届出書を受け付けし基幹システムに登録処理等を行うのは、アクセス権限を付与された必要最小限の職員等に限定し、アクセス権限が付与された職員等でも限定された端末以外からは電子申請データにアクセスできないようシステムの的に制御する。

・電子申請データをフラッシュメモリに一時的に複写するときは、アクセス権限を付与された職員等が事前にデータ保護管理者の承認を得て、データ保護担当者がパスワード設定した媒体の使用を管理簿に記載して行い、処理に使用後速やかに媒体からデータを完全に消去して返却し、データ保護管理者はそれを確認する。

・電子申請データをレセオン端末に取得後、レセオン端末内の電子データは速やかに削除する。

- ・電子記録媒体等の管理簿と操作ログの突合等、定期的な操作ログのチェックや、職員等に対する教育、研修は上記<基幹システムにおける措置>と同様に行う。

○取りまとめ機関及び中間サーバー等における措置

<取りまとめ機関が定める当組合の運用における措置>

委託区画ファイル、副本区画ファイル及び本人確認ファイルについては、以下の措置を講じる。

- ・中間サーバー等を利用して複製等のファイル操作が可能な職員等を最小限に限定する。
- ・電子記録媒体又はフラッシュメモリへの複製を行う場合、不必要な複製を制限するため事前に責任者の承認を得る。
- ・加入者の登録情報を確認する以外にファイルを複製しないよう、職員等に対し周知徹底する。

【特定個人情報の使用を記録し監視する措置】

○基幹システムにおける措置※

・個人番号の登録や更新、情報検索、個人番号を含むデータ表示機能等の使用及び特定個人情報ファイルへのアクセス等について、システム操作ログを自動的に記録する。

・操作ログには、処理年月日、時間、操作者等を記録する。

・操作ログは一定期間保管し、不正アクセスや事故が疑われるときに点検し追跡できるようにする。

・データ保護担当者は、定期的に又はセキュリティ上の問題が発生した際に、電子記録媒体等の管理簿と操作ログの突合等や操作ログを確認し、不正な運用が行われていないかを点検する。

※電子申請された届出書を受け付けし基幹システムに登録処理等を行う操作ログの記録も、上記<基幹システムにおける措置>と同様に行う。

○取りまとめ機関及び中間サーバー等における措置

<取りまとめ機関が定める当組合の運用における措置>

・中間サーバー等の使用について、データ保護担当者は、定期的に又はセキュリティ上の問題が発生した際に、操作ログを確認し、不正な運用が行われていないかを点検する。

<中間サーバー等における措置>

・特定個人情報ファイルを扱う統合専用端末又はサーバー間接続による操作履歴（操作ログ）を中間サーバー等で記録している。

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
リスク：委託先における不正な使用等のリスク		
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[定めている]	<選択肢> 1) 定めている 2) 定めていない
規定の内容	<ul style="list-style-type: none"> ・秘密保持義務。 ・データや書類の配送、授受、保管・管理方法。 ・特定個人情報ファイル取扱い場所の限定と明確化。 ・事業所内からの特定個人情報の持出しの禁止。 ・特定個人情報の目的外利用の禁止、複写・複製の禁止。 ・再委託の禁止。 ・漏えい、滅失、棄損、改ざん等の防止策の義務付け。 ・漏えい事案等が発生した場合の委託元への速やかな報告と委託先の責任。 ・委託契約終了後の特定個人情報の返却又は消去。 ・特定個人情報を取り扱う従業者の限定と明確化。 ・従業者に対する監督・教育。 ・委託先への監査、立入調査。 ・契約内容の遵守状況について報告の義務付け 等。 	
再委託先による特定個人情報ファイルの適切な取扱いの担保	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない
具体的な方法	<p>再委託契約に次の事項を盛り込むこととし、委託先による再委託先に対する必要かつ適切な監督のもと再委託先において安全管理措置が講じられていることを確認する。再委託先が更に委託する場合においても同様に取扱うものとする。</p> <ul style="list-style-type: none"> ・秘密保持義務。 ・データや書類の配送、授受、保管・管理方法。 ・特定個人情報ファイル取扱い場所の限定と明確化。 ・事業所内からの特定個人情報の持出しの禁止。 ・特定個人情報の目的外利用の禁止、複写・複製の禁止。 ・再委託の禁止。 ・漏えい、滅失、棄損、改ざん等の防止策の義務付け。 ・漏えい事案等が発生した場合の委託元への速やかな報告と委託先の責任。 ・委託契約終了後の特定個人情報の返却又は消去。 ・特定個人情報を取り扱う従業者の限定と明確化。 ・従業者に対する監督・教育。 ・委託先への監査、立入調査。 ・契約内容の遵守状況について報告の義務付け 等。 	
その他の措置の内容	<p>【特定個人情報ファイルの取扱いの記録】</p> <p>○当組合事務所に來て行う委託業務における措置</p> <ul style="list-style-type: none"> ・基幹システム専用端末を使用して行う業務は、当組合職員と同様に全ての操作ログを記録し一定期間保管して、セキュリティ上の問題が発生した際、又は必要なタイミングで操作ログのチェックを行う。 ・基幹システムの保守・点検等作業及び稼動確認テストを行う場合は当組合に事前に連絡し、作業内容の記録、報告を行わせ一定期間保管する。 <p>○委託先事業所で行う委託業務における措置(取りまとめ機関以外の委託先)</p> <p>次の記録を一定期間保管することを義務付け、不正な取扱いがされていないことを定期又は不定期に調査すること、また必要によって記録の提出や当組合が立入調査することを契約条件とする。</p> <ul style="list-style-type: none"> ・提供した書類や電子記録媒体の授受及び保管記録。 ・操作ログ及び作業内容記録。 ・消去又は廃棄の記録とその証明書類。 <p>○取りまとめ機関における措置</p> <p><取りまとめ機関で行う委託業務における措置></p> <ul style="list-style-type: none"> ・操作ログを中間サーバー等で記録している。 ・操作ログは、セキュリティ上の問題が発生した際、又は必要なタイミングでチェックを行う。 	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置

【特定個人情報の提供ルール】
 契約書において、再委託や第三者への提供を禁止している。
 ○委託先事業所で行う委託業務における措置（取りまとめ機関以外の委託先）
 ・特定個人情報の提供及び返却時に授受伝票と管理簿の記録をその都度点検し、双方で一定期間保存する。
 ・提供及び返却の際の搬送方法は、施錠可能なケースに格納し、委託先の従業者が持ち運ぶ又は荷物の追跡が可能な手段を用いて搬送することとする。
 ・電子記録媒体で提供及び返却する時は、当組合で認証した暗号化、パスワード設定を行うこととする。
 ・目的以外の使用、複写・複製を禁止し、必要と判断したときは委託契約に定める調査権に基づき、立入調査や報告を求める。
 ・返却を求めず消去や廃棄を指示した場合には、消去又は廃棄証明書を提出させる。
 ・契約書に特定個人情報ファイルの提供・使用について、安全管理や使用の記録作成等の義務を定め、当組合に随時報告又は必要に応じて当組合が立入調査する。

○取りまとめ機関で行う委託業務における措置
 ・契約書において当組合が保有する個人情報を第三者に漏らしてはならない旨を定めており、委託先から他者への特定個人情報の提供を認めていない。
 ・定期的に操作ログをチェックし、データ抽出等の不正な持出しが行われていないか監視する。
 ・提供情報は、業務委託完了時に全て返却又は消去する。

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。） [○] 提供・移転しない

リスク： 不正な提供・移転が行われるリスク

特定個人情報の提供・移転に関するルール	[<選択肢> 1) 定めている	2) 定めていない
ルールの内容及びルール遵守の確認方法			
その他の措置の内容			
リスクへの対策は十分か	[<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である

特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置

6. 情報提供ネットワークシステムとの接続 [] 接続しない(入手) [] 接続しない(提供)	
リスク1: 目的外の入手が行われるリスク	
リスクに対する措置の内容	<p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。 <中間サーバー等における措置> ①基幹システム専用端末を利用して情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可照会リスト(※)との照会を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。 つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。</p> <p>②支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバー等で記録しているため、不適切な統合専用端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。</p> <p>(※)番号法別表第2に基づき、事務手続ごとに情報照会者、情報提供者、照会・提供可能な特定個人情報リスト化したもの。</p>
リスクへの対策は十分か	<p>[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている</p>
リスク2: 不正な提供が行われるリスク	
リスクに対する措置の内容	<p>情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。 <中間サーバー等における措置> ①情報提供ネットワークシステムにおける照会許可照会リストを情報提供ネットワークシステムから入手し、中間サーバー等にも格納して、照会許可照会リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。</p> <p>②情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。</p> <p>③特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。</p> <p>④支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバー等で記録しているため、不適切な統合専用端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。</p>
リスクへの対策は十分か	<p>[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている</p>
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	
<p><統合専用端末と基幹システムとの間の情報授受に係るリスク対策></p> <ul style="list-style-type: none"> ・統合専用端末と基幹システムとの間の情報授受に係る業務を行う職員等を必要最小限に限定し、そのユーザIDとアクセス権限が付与された者以外が情報授受に係る業務ができないようシステムの的に制御する。 ・情報授受でフラッシュメモリへの複製を行う場合、不必要な複製を制限するため事前にデータ保護担当者の承認を得る。 ・フラッシュメモリの利用記録等は管理簿に記載し、保管庫に施錠保管する。 ・情報授受に用いるフラッシュメモリが使用ができる基幹システム専用端末を限定し、それ以外の基幹システム専用端末では使用できないようシステムの的に制御する。 ・フラッシュメモリを使用する場合はパスワード認証機能付きの媒体とし、データ保護担当者がパスワード設定した媒体以外は基幹システム専用端末及び統合専用端末で使用できないようシステムの的に制御する。 ・基幹システム専用端末及び統合専用端末の操作ログを記録し、データ保護担当者が定期的に又はセキュリティ上の問題が発生した際に、フラッシュメモリへの不必要な複製をチェックする。 ・統合専用端末は中間サーバー等以外とは接続せず、他の業務に兼用できないよう他のネットワークやシステムと分離する。 ・統合専用端末の使用後、ハードディスク等内の特定個人情報データは全て削除する。 ・フラッシュメモリではデータを保存せず、使用した都度、データを全て削除する。 <p><サーバー間接続の情報連携サーバーと基幹システムとの情報授受に係るリスク対策></p> <ul style="list-style-type: none"> ・情報授受に係る業務を行う職員等を必要最小限に限定し、そのユーザIDとアクセス権限が付与された者以外が情報授受に係る業務ができないようシステムの的に制御する。 ・情報授受の操作を行う基幹システム専用端末を限定し、それ以外の専用端末は使用できないようシステムの的に制御する。 ・情報連携サーバーは中間サーバー等及び基幹システム以外とは接続せず、他のネットワークやシステムと分離する。 ・情報連携サーバーにファイアウォールを設置して不正アクセスを防止し、ウイルス対策ソフトの導入及びパターンファイルの随時更新を行ってデータを保護する。 ・情報連携サーバーを使用した操作ログを記録し、データ保護担当者が定期的に又はセキュリティ上の問題が発生した際に、チェックする。 ・情報連携サーバーには一時的に情報を格納するだけで、情報授受が終了した時点でシステムで自動的に消去する。 	

情報提供ネットワークシステムに接続する際に支払基金が、以下の措置を講じている。

＜中間サーバー等における措置＞

- ①支払基金の職員が統合専用端末を利用して情報照会依頼及び情報照会結果の確認等を行う際、ログイン時の職員認証の他に、統合専用端末の操作履歴(操作ログ)を中間サーバー等で記録しているため、不適切な統合専用端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。
- ②情報連携においてのみ、情報提供用個人識別符号を用いることが中間サーバー等にて担保されており、不正な名寄せが行われるリスクに対応している。
- ③中間サーバー等と情報提供ネットワークシステムとの間は、高度なセキュリティを維持した厚生労働省統合ネットワークを利用することにより、安全性を確保している。
- ④中間サーバー等と医療保険者等の通信は、VPN等の技術を用いた専用線を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。
- ⑤中間サーバー等では、特定個人情報を管理するデータベースを医療保険者等ごとに区分管理(アクセス制御)しており、中間サーバー等を利用する医療保険者等であっても他の医療保険者等が管理する情報には一切アクセスできない。

7. 特定個人情報の保管・消去	
リスク： 特定個人情報の漏えい・滅失・毀損リスク	
①事故発生時手順の策定・周知	[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
②過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし] <選択肢> 1) 発生あり 2) 発生なし
その内容	
再発防止策の内容	
	<p>【物理的対策】</p> <p><セキュリティ管理区域(特定個人情報を取り扱う事務を実施する区画又は、特定個人情報を取り扱う情報システムを管理する区画)における措置></p> <ul style="list-style-type: none"> ・入退室記録管理 ・消火設備、煙感知器等の設置 ・無停電電源装置(UPS)の付設 ・サーバラックの施錠 ・サーバ及び基幹システム専用端末をインターネット等外部ネットワークと隔離等により、リスクを回避する。 <p><中間サーバー等における措置></p> <ul style="list-style-type: none"> ・運用支援環境は、クラウド事業者が保有・管理する環境(日本国内)に設置し、クラウド事業者による設置場所への入退室記録管理及び施錠管理をすることでリスクを回避する。 ・クラウド環境にアクセスできる運用・保守拠点では、電子錠による入退室制限等の物理的なアクセス制御手段により、許可された利用者のみが入退室できるようにする。また、監視カメラ等による入退室及び室内映像の収集ができ、入退室の記録を取得可能とする。 <p>【技術的対策】</p> <p><基幹システムにおける措置></p> <ul style="list-style-type: none"> ・ウイルス対策ソフトの導入、パターンファイルの随時更新 ・統合専用端末との情報授受については、操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する。それ以外の基幹システム専用端末においては、特定個人情報ファイルについて端末への保存や電子記録媒体及びフラッシュメモリへの書込み及び読出し等ができないようシステムの的に制御 ・サーバー間接続に係る情報連携サーバーを介した情報授受は操作を行う基幹システム専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御 ・情報連携サーバーには一時的に情報を格納し、情報授受が終了した時点でシステムで自動的に消去 ・基幹システム専用端末は、他の情報系端末等に兼用しない ・サーバ及び基幹システム専用端末はインターネット等外部ネットワークに接続できないよう分離等により、リスクを回避する。 <p><電子申請された届出書の受け付けにおける措置></p> <ul style="list-style-type: none"> ・マイナポータルに接続するオンライン請求NWは、通信内容の秘匿や盗聴防止がされたIP-VPNによる閉鎖された通信回線を使用する。

<p>その他の措置の内容</p>	<ul style="list-style-type: none"> ・マイナポータル内部において、オンライン請求NWの接続先と事業主の接続先は論理的に分離されている。 ・電子申請された届出書を受け付けし基幹システムに登録処理等を行うのは、アクセス権限を付与された必要最小限の職員等だけに限定したアクセス制御をし、アクセス権限が付与された職員等でも限定された端末以外からは電子申請データにアクセスできないようシステム的に制御する。 ・マイナポータル連携サーバー及びレセオン端末はオンライン請求NWにだけ接続し、それ以外のネットワークとは接続できないよう分離する。 ・マイナポータル連携サーバー及びレセオン端末にはファイアウォールの設定やウイルス対策ソフトを導入しパターンファイルを随時更新する。 <p>等により、リスクを回避する。</p> <p><取りまとめ機関が定める当組合の運用における措置></p> <ul style="list-style-type: none"> ・統合専用端末及び情報連携サーバーはインターネットに接続できないよう分離 ・統合専用端末及び情報連携サーバーは中間サーバー等以外のシステムに兼用できないよう分離等により、リスクを回避する。 <p><中間サーバー等における措置></p> <ol style="list-style-type: none"> ①運用支援環境において保有する特定個人情報インターネットに流出することを防止するため、中間サーバー等はインターネットには接続できないようシステム面の措置を講じている。 ②運用支援環境では、セキュリティ対策を実施するクラウドマネージドサービス(クラウド事業者により運用管理まで含めた形で提供されるサービス)等を活用し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ③クラウドマネージドサービスの利用にあたっては、クラウド事業者は個人番号を内容に含む電子データを取り扱わない契約とし、クラウド事業者が個人番号等にアクセスできないように、アクセス制御を行う。 ④運用支援環境では、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤導入しているOS及びミドルウェアについて、必要なセキュリティパッチの適用を行う。 ⑥中間サーバー等と当組合の通信は、VPN等の技術を用いた専用線を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。 ⑦運用支援環境とオンライン資格確認等システムとの通信は、個人番号が送信されないように、厚生労働省が定めたインターフェース仕様に沿って、決められたデータ項目のみ提供するようにシステム的に制御されている。 ⑧オンライン資格確認等システム側から運用支援環境へはアクセスしないよう制御(情報を提供した際の処理結果電文は除く。)する。
<p>リスクへの対策は十分か</p>	<p>[十分である]</p> <p><選択肢></p> <p>1) 特に力を入れている 2) 十分である</p> <p>3) 課題が残されている</p>

特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置

【特定個人情報ファイルの保管期間】

- ・基幹システムに保存する個人番号については、当組合の「システム等運用管理規程」に規定された 保存期間に基づき、資格喪失後10年間保管する。
- ・電子申請された届出書データは決済処理が終了するまでの間、基幹システムで保管・管理する。決済処理をした届出書データ等は、当組合の「文書保存規程」及び「システム等運用管理規程」に定められた期間、基幹システムで保管する。
- ・中間サーバー等内の委託区画ファイルに保存される情報については、オンライン資格確認等(システムで資格履歴)を必要とする期間(10年間)、また、副本区画ファイルに保存される情報については、加入者が当組合で資格を喪失した時点から、照会条件として指定される範囲及び情報連携で副本を提供する可能性のある年(最長5年間)まで保管する。
- ・情報提供等記録項目については、7年間保管する。
- ・本人確認項目については、個人番号を利用するために一時的に格納されるものであるためその保管期間は1年を超えることはない。

【特定個人情報が古いまま保管され続けることを防止する措置】

<基幹システムにおける措置>

- ・被扶養者については年1回、現況確認により情報の更新を実施する。
- ・当組合の機関誌、Webページ等で加入者や事業所に異動・変更を速やかに届出るよう周知を図る。

<取りまとめ機関が定める当組合の運用における措置>

- ・加入者の資格情報等の新規登録又は情報の更新があった際は、速やかに中間サーバー等の委託区画又は副本区画の情報を登録・更新する。

【特定個人情報が消去されずにいつまでも存在することを防止する措置】

<基幹システムにおける措置>

- ・喪失日から保管期間が経過した加入者を定期的に基幹システムで検出し、個人番号を完全消去する。
- ・その他、基幹システム内に保管したデータファイル等は、保管期間が終了したものを定期的に基幹システムで検出し、基幹システムの消去機能を使って完全に消去する。
- ・電子記録媒体にデータファイル等を保管した場合は、保管期間が終了したものを定期的に管理簿で点検し、電子記録媒体を工具又はメディアシュレッダーで物理的に破壊して廃棄する。

※上記の消去又は廃棄を行った場合、管理簿に消去又は廃棄の記録を記載する。

<電子申請された届出書における措置>

- ・電子申請データをレセオン端末に取得後、レセオン端末内の電子申請データは速やかに削除する。
- ・フラッシュメモリでレセオン端末と基幹システム間の電子データの授受を行ったときは、処理に使用後速やかに媒体からデータを消去する。
- ・基幹システム内に保管した電子申請データは、上記<基幹システムにおける措置>の通り保管期間の終了後に消去又は廃棄も記載する。

<取りまとめ機関が定める当組合の運用における措置>

- ・資格審査時に中間サーバー等の運用支援環境(委託区画)に特定個人情報を登録する。資格審査の結果、資格を得られない場合には、運用支援環境(委託区画)に登録した特定個人情報を消去する。

【運用上のルールによる措置】

- ・プリンタ、FAX等の出力用紙の放置禁止の徹底
- ・保存期間が過ぎた特定個人情報の記載された用紙(届出書や帳票類)はシュレッダーで粉砕して破棄
- ・溶解処分業者による保存満了分文書廃棄の実施(処分方法や廃棄証明書発行等の委託契約条件の見直しによる確実な廃棄の実施)
- ・書類又は電子記録媒体の搬送時の所在追跡可能な手段の実施
- ・執務用デスク周辺の整理整頓及び退社時の施錠の実施
- ・離席時のスクリーンセーバー又はシャットダウン
- ・PC等のリース機器返却又は機器を廃棄する場合、HDDのデータを復元不可能に完全消去又は物理的に破壊した証明書類の提出や疑義が生じた際の立入調査等を条件にリース業者や廃棄業者に引渡し、証明書類で処置を確認
- ・条件に見合う適切な業者がない場合は、当組合でデータ消去ソフトを導入して完全消去を実施し、廃棄記録を媒体管理簿に記載
- ・廃棄する電子記録媒体及びフラッシュメモリは、工具又はメディアシュレッダーで物理的に破壊して廃棄し、廃棄記録を媒体管理簿に記載
- ・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。

【特定個人情報の漏えい事案等が発生した場合の対応】

「特定個人情報の漏えいその他の特定個人情報の安全の確保に係る重大な事態の報告に関する規則(平成27年特定個人情報保護委員会規則第5号)」及び「事業者における特定個人情報の漏えい事案等が発生した場合の対応について(平成27年特定個人情報保護委員会告示第2号)」に基づき、次の対応を行う。

- (1)事業所内の責任ある立場の者に直ちに報告するとともに、被害の拡大を防止する。
 - (2)事実関係を調査し、番号法違反又は番号法違反のおそれが把握できた場合には、その原因究明を行う。
 - (3)上記(2)で把握した事実関係による影響の範囲を特定する。
 - (4)上記(2)で究明した原因を踏まえ、再発防止策を検討し、速やかに実施する。
 - (5)事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係等について、速やかに本人に連絡又は本人が容易に知り得る状態に置く。
 - (6)事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、事実関係及び再発防止策について、速やかに公表する。
 - (7)番号法違反の事案又は番号法違反のおそれのある事案を把握した場合には、事実関係及び再発防止策等について、速やかに本告示等に基づく報告先に報告する。
- ただし、重大事態に該当する事案又はそのおそれのある事案が発覚した時点で、直ちにその旨を個人情報保護委員会に報告し、その後、重大事態に該当する事案は、本規則の規定に従って個人情報保護委員会に報告する。

8. 監査	
実施の有無	[<input type="checkbox"/>] 自己点検 [<input type="checkbox"/>] 内部監査 [<input type="checkbox"/>] 外部監査
9. 従業者に対する教育・啓発	
従業者に対する教育・啓発	[<input type="checkbox"/> 十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
具体的な方法	<p>【教育・啓発】</p> <ul style="list-style-type: none"> ・職員等の採用・就任時に、特定個人情報管理規定の教育を行う。 ・最低毎年1回、特定個人情報取扱いの教育を行う。 ・教育実施後、理解度の把握や啓発を図るため、テストやレポート提出を行う。 ・事故が発生した場合、その原因、影響、再発防止策等を全職員等に周知する。 ・リスク回避の方策や改善案等を職員等に考えさせ提案させる。 ・適当な外部機関の教育、研修プログラムがあれば交代で参加させる。 ・派遣職員については、契約時の派遣先による当組合の契約における特定個人情報の取扱いの周知徹底を行い、当組合に在職中は職員等と同等に上記のような教育・啓発に参加させて教育する。 <p><取りまとめ機関が定める当組合の運用における措置></p> <ul style="list-style-type: none"> ・情報提供ネットワークシステム運用主体や厚生労働省、取りまとめ機関等が医療保険者等向けに実施する教育・研修、訓練等に当組合の職員を参加させる。 ・運用管理規程(医療保険者等向け)の「5.1 教育」に則り、情報提供ネットワークシステム運用主体が提供する教育計画及び取りまとめ機関が提供する教育・研修資料を基に毎年教育計画を作成して実施する。 ・教育実施後、受講者のQ&A対応や理解度向上を目的としたフォローアップ対応を適宜行う。 ・受講者の意見等を踏まえた上で教育内容の改善を検討すると共に、収集した意見等の集計結果をレポートにまとめ、取りまとめ機関に提供する。 <p>【違反行為の措置】</p> <ul style="list-style-type: none"> ・違反行為が組合内外に与える影響の重大性に応じて、戒告、減給、停職、解雇等の処分を行う。 ・違反行為による損害賠償を請求することがある。 ・これらの措置、処分について就業規則に定め、周知する。
10. その他のリスク対策	
なし	

IV 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒101-8304 東京都千代田区神田駿河台1-7 出版健康保険組合 業務部適用課 TEL03-3292-5005 業務部給付課 TEL03-3292-5006 〒540-0012 大阪市中央区谷町1-7-4 出版健康保険組合大阪支部 業務課 TEL06-6944-4300
②請求方法	当組合所定の様式による書面で、特定個人情報の開示・訂正・利用停止請求を受け付ける。 ・様式1: 保有個人データ開示請求書 ・様式2: 保有個人データ開示依頼書 ・様式3: 保有個人データ訂正・利用停止等届出書
③法令による特別の手続	なし
④個人情報ファイル簿への不記載等	なし
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	〒101-8304 東京都千代田区神田駿河台1-7 出版健康保険組合 企画部 TEL03-3292-5009 〒540-0012 大阪市中央区谷町1-7-4 出版健康保険組合大阪支部 総務課 TEL06-6944-4300
②対応方法	・問合せ受付時に受付票を起票し、内容及び対応、経過等について記録を残す。 ・重要度や緊急度のランク付けを行い、対応する担当者や回答期限を設定する。 ・情報漏えい等の重大な事案に関する問合せは、理事長へ報告の上、対応を決定する。

V 評価実施手続

1. 基礎項目評価	
①実施日	令和2年9月16日
②しきい値判断結果	[基礎項目評価及び重点項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び重点項目評価の実施が義務付けられる 2) 基礎項目評価の実施が義務付けられる(任意に重点項目評価を実施) 3) 特定個人情報保護評価の実施が義務付けられない(任意に重点項目評価を実施)
2. 国民・住民等からの意見の聴取【任意】	
①方法	
②実施日・期間	
③主な意見の内容	
3. 第三者点検【任意】	
①実施日	
②方法	
③結果	

(別添2)変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年11月21日	Ⅱ-4-委託事項5-②	空欄	2)10人以上50人未満	事後	委託先を決定したことにより委託先取扱者数を記載したもので、重要な変更にあらず。
平成28年11月21日	Ⅱ-4-委託事項5-③	未定	株式会社 コンピュータービジネス	事後	委託先を決定したことにより委託先名を記載したもので、重要な変更にあらず。
平成29年9月6日	I-6-②所属長	井川 達也	矢嶋 浩	事後	重要な変更にあたらぬ所属長氏名の変更
平成30年9月3日	I 1.特定個人情報ファイルを取り扱う事務において使用するシステム ②事務の内容	1. 適用事務 (1)平成28年10月から、資格を有する……。 (※1)地方公共団体情報システム機構からの個人番号取得は、平成28年10月から平成29年3月の間は電子記録媒体で行い、平成29年4月以降は中間サーバー等を介して即時照会又はファイル一括照会する。……	(1)を全文削除。 (※1)を次の様に変更。 地方公共団体情報システム機構からの個人番号入手や基本4情報入手は、支払基金経由で中間サーバー等を介して即時照会又はファイル一括照会する。	事後	平成29年3月で(1)の事務、及び地方公共団体情報システム機構から電子記録媒体での個人番号取得が終了。取扱上のリスク軽減で、重要な変更にあらず。
平成30年9月3日	I 5.情報提供ネットワークシステムによる情報連携 ②法令上の根拠	・番号法 第19条第7号 (提供)別表第2 項番1、2、……200	・番号法 第19条第7号 (提供)別表第2 項番1、2、……119	事後	番号法改正により項番変更
平成30年9月3日	Ⅲ 2.特定個人情報の入手リスク:目的外の入手が行われるリスク 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置	○地方公共団体情報システム機構から支払基金経由で機構保存本人確認情報を電子記録媒体で入手する場合の措置	この項目を全文削除	事後	平成29年3月末で電子記録媒体による入手が終了。取扱上のリスク軽減で、重要な変更にあらず。
平成30年9月3日	Ⅲ 9.従業員に対する教育・啓発	・中間サーバー等の……統合専用端末導入前に研修を行う。	・厚労省、取りまとめ機関等が実施する教育・研修への参加 ・取りまとめ機関が提供する資料より毎年教育計画を作成、実施 ・受講者の意見等をまとめ、取りまとめ機関に提供	事後	平成29年4月に統合専用端末が導入され、導入前研修の終了により、取りまとめ機関が定める運用管理規程の「教育」に書換え。

令和2年2月20日	I 2. 特定個人情報ファイル を取り扱う事務において 使用するシステム [システム1] ②システムの機能	(※)「識別番号」は、既存システムで被保険者及び被扶養者を特定するために当組合で発番した一意の番号で、事業所コード、証記号番号+枝番及び続柄コード、従業員番号及び扶養番号である。 (「証記号番号+枝番」は、オンライン資格確認等の実施に対応して従来からの「証記号番号」に個人を識別する2桁の番号(枝番)を、令和2年度から付加するものである。以下、「証記号番号+枝番」について同じ。)	事前	「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正であるが、事前に提出
令和2年2月20日	同 [システム1] ③他のシステムとの接続	その他のシステム名(レセプトシステム、レセプト情報管理システム、レセプト管理・分析システム、調査報告システム、月報システム)	その他のシステム名に「中間サーバー等」を追記	事前 サーバー間接続方式を採用する重要な変更で、事前に提出
令和2年2月20日	同 [システム2] ②システムの機能	(1)資格履歴管理事務に係る機能 新規加入者の基本4情報(又はその一部)、資格情報(個人番号含む。)を中間サーバー等に登録する。	(1)資格履歴管理事務に係る機能 (i)資格履歴管理 新規加入者の基本4情報(又はその一部)、資格情報(個人番号を含む。)及び各種証情報を中間サーバー等に登録する。 (ii)オンライン資格確認等システムへの資格情報の提供 個人番号を除いた資格履歴ファイルをオンライン資格確認等システムに提供する。	事前 「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正であるが、事前に提出
令和2年2月20日	同 [システム2] ③他のシステムとの接続		その他のシステム名に「基幹システム、オンライン資格確認等システム」を記載	事前 サーバー間接続方式を採用する重要な変更で、事前に提出 「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正であるが、事前に提出
令和2年2月20日	II 4. 特定個人情報ファイル の取扱いの委託 委託事項2 ①委託内容	個人番号を利用した加入者資格の履歴管理、被保険者枝番の採番管理、被保険者枝番と個人番号との紐付管理	個人番号を利用した加入者資格の履歴管理、被保険者枝番の採番管理、被保険者枝番と個人番号との紐付管理、及び資格履歴情報をオンライン資格確認等システムに登録	事前 「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正であるが、事前に提出

令和2年2月20日	II 6. 特定個人情報の保管・消去 保管場所	<中間サーバー等における措置> ・中間サーバー等は、支払基金のデータセンターに設置しており、許可された者のみが入退室できる管理対象区域に設置する。	<中間サーバー等における措置> ①中間サーバー等の運用支援環境の設置場所は、取りまとめ機関が所有のサーバー環境(オンプレミス環境)の場合、セキュリティを確保したサーバー室に設置し、許可された者のみが入退室できる管理対象区域にて設置する。また、クラウド環境の場合、クラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。 ②特定個人情報は、運用支援環境(情報提供サーバー)のデータベース内に保存され、バックアップもデータベース上に保存される。	事前	同上
令和2年2月20日	II (別添1)特定個人情報ファイル記録項目	<加入者情報項目> 証記号、証番号	<加入者情報項目> 証記号番号+枝番 <被保険者証項目><高齢受給者証項目> <限度額適用認定証項目><特定疾病療養受療証項目>等に項目名の追加、修正	事前	同上
令和2年2月20日	III 2. 特定個人情報の入手 特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く)におけるその他のリスク及びそのリスクに対する措置		【入手の際に特定個人情報が漏えい・紛失することを防止するための措置】に、 『サーバー間接続に係る情報連携サーバーとの情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する』ことを追記	事前	サーバー間接続方式を採用する重要な変更で、事前に提出
令和2年2月20日	III 3. 特定個人情報の使用 特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		【従業者が事務外で使用することを防止する措置】と【特定個人情報ファイルが不正に複製されることを防止する措置】に、 『サーバー間接続に係る情報連携サーバーとの情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する』ことを追記 【特定個人情報の使用を記録し監視する措置】に、 『サーバー間接続による操作履歴を記録する』ことを追記	事前	同上

令和2年2月20日	Ⅲ 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		『サーバー間接続に係る情報連携サーバーと基幹システムとの情報授受に係るリスク対策』を追記	事前	同上
令和2年2月20日	Ⅲ 7. 特定個人情報の保管・消去 リスク: 特定個人情報の漏えい・滅失・毀損リスク その他の措置の内容	【物理的対策】 ＜中間サーバー等における措置＞ ・中間サーバー等を支払基金のデータセンターに設置し、設置場所への入退室記録管理、監視カメラによる監視及び施錠管理をすることでリスクを回避する。	【物理的対策】 ＜中間サーバー等における措置＞ ・運用支援環境は、クラウド事業者が保有・管理する環境(日本国内)に設置し、クラウド事業者による設置場所への入退室記録管理及び施錠管理をすることでリスクを回避する。 ・クラウド環境にアクセスできる運用・保守拠点では、電子錠による入退室制限等の物理的なアクセス制御手段により、許可された利用者のみが入退室できるようにする。また、監視カメラ等による入退室及び室内映像の収集ができ、入退室の記録を取得可能とする。	事前	「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正であるが、事前に提出
令和2年2月20日	同 その他の措置の内容		【技術的対策】に、 『サーバー間接続に係る情報連携サーバーとの情報授受は操作を行う専用端末を限定し、アクセス権限を付与された最小限の職員等だけが当該端末を操作できるようアクセス制御する』ことと、 『情報連携サーバー内の情報は自動削除され残らない』ことを追記	事前	サーバー間接続方式を採用する重要な変更で、事前に提出

令和2年2月20日	同 その他の措置の内容	<p>【技術的対策】 <中間サーバー等における措置> ①中間サーバー等において保有する特定個人情報インターネットに流出することを防止するため、中間サーバー等はインターネットには接続できないようシステム面の措置を講じている。 ②中間サーバー等ではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ③中間サーバー等では、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ④導入しているOS及びミドルウェアについて、必要なセキュリティパッチの適用を行う。 ⑤中間サーバー等と当組合の通信は、VPN等の技術を用いた専用線を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。</p>	<p>【技術的対策】 <中間サーバー等における措置> ①運用支援環境において保有する特定個人情報インターネットに流出することを防止するため、中間サーバー等はインターネットには接続できないようシステム面の措置を講じている。 ②運用支援環境では、セキュリティ対策を実施するクラウドマネージドサービス(クラウド事業者により運用管理まで含めた形で提供されるサービス)等を活用し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ③クラウドマネージドサービスの利用にあたっては、クラウド事業者は個人番号を内容に含む電子データを取り扱わない契約とし、クラウド事業者が個人番号等にアクセスできないように、アクセス制御を行う。 ④運用支援環境では、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤導入しているOS及びミドルウェアについて、必要なセキュリティパッチの適用を行う。 ⑥中間サーバー等と当組合の通信は、VPN等の技術を用いた専用線を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をしている。 ⑦運用支援環境とオンライン資格確認等システムとの通信は、個人番号が送信されないように、厚生労働省が定めたインターフェース仕様に沿って、決められたデータ項目のみ提供するようにシステム的に制御されている。 ⑧オンライン資格確認等システム側から運用支援環境へはアクセスしないよう制御(情報を提供した際の処理結果電文は除く。)する。</p>	事前	「オンライン資格確認等」の実施に伴うもので、当組合が行う事務、リスク対策等に重要な変更が生じない修正であるが、事前に提出
令和2年2月20日	I 5. 情報提供ネットワークシステムによる情報連携 ②法令上の根拠	・番号法 第19条第7号(特定個人情報の提供の制限) (提供)別表第2 項番1、2、3……119	(提供)別表第2のうち、項番119を120に変更。	事後	番号法改正で項番号が変更されただけの軽微な変更で、事後(改正後)に提出
令和2年9月25日	評価書全般 (Ⅲ2.特定個人情報の入手、Ⅲ.3特定個人情報の使用、Ⅲ.7特定個人情報の保管・消去等)		電子申請による届出書の入手経路の追加に伴う追記等 (特定個人情報の入手に関するリスク対策の追記等)	事前	電子申請に係る重要な変更

<p>令和2年9月25日</p>	<p>Ⅲ 3. 特定個人情報の使用</p> <p>特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置</p> <p>Ⅲ 6. 情報提供ネットワークシステムとの接続</p> <p>情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置</p> <p>Ⅲ 7. 特定個人情報の保管・消去</p> <p>特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置</p>		<p>電子記録媒体等の保管・管理等についての追記等</p>	<p>事後</p>	<p>リスク管理の記述について事後補正</p>
<p>令和2年9月25日</p>	<p>I 5. 情報提供ネットワークシステムによる情報連携</p> <p>②法令上の根拠</p>	<p>(提供)別表第2 項番1、2、3、4、5、9、12、15、17、22、26、27、33、39、42、43、58、62、78、80、87、93、97、106、109、120</p> <p>番号法別表第2の主務省令で定める事務及び情報を定める命令 第1条、第2条、第3条、第4条、第5条、第8条、第19条、第20条、第25条、第33条、第43条、第44条、第46条、第49条、第53条</p>	<p>(提供)別表第2 項番1、2、3、4、5、9、12、15、17、22、26、27、33、39、42、43、58、62、78、80、87、93、97、106、109、120</p> <p>番号法別表第2の主務省令で定める事務及び情報を定める命令 第1条、第2条、第3条、第4条、第5条、第8条、第10条の2、第11条の2、第12条の3、第15条、第19条、第20条、第22条の2、第24条の2、第25条、第25条の2、第31条の2、第33条、第41条の2、第43条、第44条、第46条、第49条、第53条、第55条の2、第59条の3</p>	<p>事後</p>	<p>条項の記載漏れ等を見直した結果で、事後変更</p>