

特定個人情報保護評価書(全項目評価書)

評価書番号	評価書名
12	国民健康保険法による保険給付等に関する事務 全項目評価書

個人のプライバシー等の権利利益の保護の宣言

広島市は、国民健康保険法による保険給付等に関する事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイル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を発生させ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

評価実施機関名

広島市長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

令和8年3月24日

項目一覧

I 基本情報
(別添1) 事務の内容
II 特定個人情報ファイルの概要
(別添2) 特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
(別添3) 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	国民健康保険法による保険給付等に関する事務						
②事務の内容 ※	<p>国民健康保険法による保険給付の支給又は保険料の徴収に関する次の事務</p> <ol style="list-style-type: none"> 1. 保険給付及び保険料賦課に必要な資格情報を管理し、被保険者証等の交付を行う被保険者資格管理事務 2. 被保険者の所得の把握、保険料賦課、保険料減免等を行う保険料賦課管理事務 3. 高額療養費等の保険給付を行う給付管理事務 4. 保険料の収納、還付、充当等及び滞納者への督促状の送付を行う保険料収納管理事務 5. 保険料の滞納整理等を行う保険料滞納管理事務 <p>「医療保険制度の適正かつ効率的な運営を図るための健康保険法等の一部を改正する法律」によりオンライン資格確認のしくみの導入を行うとされたことと、当該しくみのような、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または整理に関する事務」及び「被保険者等に係る情報の利用または提供に関する事務」を「国民健康保険団体連合会(以下「国保連合会」という。)または社会保険診療報酬支払基金(以下「支払基金」という。)(以下「支払基金等」という。)に委託することができる旨の規定が国民健康保険法に盛り込まれていることを踏まえ、オンライン資格確認等システムへの資格情報の提供に係る加入者等の資格履歴情報の管理、機関別符号の取得、及び一部の情報提供について共同して支払基金等に委託することとし、国保連合会から再委託を受けた国民健康保険中央会(以下「国保中央会」という。)及び支払基金(以下「取りまとめ機関」という。)が、医療保険者等向け中間サーバー等の運営を共同して行う。</p> <p><オンライン資格確認等システム稼働に向けた準備としての資格履歴管理事務、機関別符号の取得等事務(以下「オンライン資格確認の準備業務」という。)></p> <ul style="list-style-type: none"> ・オンライン資格確認等システムで被保険者等の資格情報を利用するために、国保連合会から委託を受けた国保中央会が、本市からの委託を受けて「医療保険者等向け中間サーバー等における資格履歴管理事務」を行うために、本市から被保険者及び世帯構成員の個人情報を出し、国保連合会を経由して医療保険者等向け中間サーバー等へ被保険者資格情報の提供を行う。 ・オンライン資格確認等システムで被保険者等の資格情報を利用するために、支払基金が、本市からの委託を受けて「医療保険者等向け中間サーバー等における機関別符号取得等事務」を行うために、情報提供等記録開示システムの自己情報表示業務機能を利用して、本市から提供した被保険者資格情報とオンライン資格確認等システムで管理している情報とを紐付けるために機関別符号の取得並びに紐付け情報の提供を行う。 						
③対象人数	<p>[30万人以上]</p> <p><選択肢></p> <table> <tr> <td>1) 1,000人未満</td> <td>2) 1,000人以上1万人未満</td> </tr> <tr> <td>3) 1万人以上10万人未満</td> <td>4) 10万人以上30万人未満</td> </tr> <tr> <td>5) 30万人以上</td> <td></td> </tr> </table>	1) 1,000人未満	2) 1,000人以上1万人未満	3) 1万人以上10万人未満	4) 10万人以上30万人未満	5) 30万人以上	
1) 1,000人未満	2) 1,000人以上1万人未満						
3) 1万人以上10万人未満	4) 10万人以上30万人未満						
5) 30万人以上							

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

①システムの名称	国民健康保険システム								
②システムの機能	<ol style="list-style-type: none"> 1. 被保険者資格管理機能 資格の取得、喪失などの情報を管理し、被保険者証等の発行を行う機能 2. 保険料賦課管理機能 市税システムから提供を受けるなどして所得情報を管理し、保険料を賦課し、保険料の減免などを行う機能 3. 給付管理機能 被保険者の所得情報より、保険給付に必要な所得区分を判定し、高額療養費等の保険給付を行う機能 4. 保険料収納管理機能 保険料の収納情報を管理し、還付、充当等及び滞納者への督促状の発行を行う機能 								
③他のシステムとの接続	<table> <tr> <td>[] 情報提供ネットワークシステム</td> <td>[○] 庁内連携システム</td> </tr> <tr> <td>[] 住民基本台帳ネットワークシステム</td> <td>[] 既存住民基本台帳システム</td> </tr> <tr> <td>[○] 宛名システム等</td> <td>[] 税務システム</td> </tr> <tr> <td>[] その他 ()</td> <td></td> </tr> </table>	[] 情報提供ネットワークシステム	[○] 庁内連携システム	[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム	[○] 宛名システム等	[] 税務システム	[] その他 ()	
[] 情報提供ネットワークシステム	[○] 庁内連携システム								
[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム								
[○] 宛名システム等	[] 税務システム								
[] その他 ()									

システム2～5

システム2

①システムの名称	滞納管理システム
----------	----------

②システムの機能	国民健康保険法による保険料の徴収に関する電算処理機能 ・滞納者の滞納状況の管理 ・滞納者との折衝記録の管理 ・滞納整理関係帳票、納付書等の作成 ・統計情報の管理								
③他のシステムとの接続	<table border="0"> <tr> <td>[] 情報提供ネットワークシステム</td> <td>[<input checked="" type="checkbox"/>] 庁内連携システム</td> </tr> <tr> <td>[] 住民基本台帳ネットワークシステム</td> <td>[] 既存住民基本台帳システム</td> </tr> <tr> <td>[] 宛名システム等</td> <td>[<input checked="" type="checkbox"/>] 税務システム</td> </tr> <tr> <td>[] その他 (</td> <td>)</td> </tr> </table>	[] 情報提供ネットワークシステム	[<input checked="" type="checkbox"/>] 庁内連携システム	[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム	[] 宛名システム等	[<input checked="" type="checkbox"/>] 税務システム	[] その他 ()
[] 情報提供ネットワークシステム	[<input checked="" type="checkbox"/>] 庁内連携システム								
[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム								
[] 宛名システム等	[<input checked="" type="checkbox"/>] 税務システム								
[] その他 ()								

システム3

①システムの名称	共通基盤(庁内連携システム、宛名システム及び申請管理システムに相当)								
②システムの機能	<ol style="list-style-type: none"> ポータル機能 ICカードによる利用者認証、権限管理及び業務システムの起動を行う機能。 システム間連携制御機能 共通基盤と業務システム間及び異なる業務システム間のデータ連携を行う機能。 運用管理機能 システム監視、稼働記録(ログ)管理、ウイルス対策及びデータのバックアップを行う機能。 団体内統合宛名機能 個人番号と団体内統合宛名番号とを紐付けて管理する機能。団体内統合宛名番号が未登録の個人番号については、新規に団体内統合宛名番号を割り当てる。 中間サーバー連携機能 中間サーバーと共通基盤間のデータ連携を行い、中間サーバーへの情報照会要求の送信及び照会結果の受信並びに特定個人情報の副本の登録を行う機能。 ぴったりサービス対応機能 サービス検索・電子申請機能と共通基盤間のデータ連携を行い、サービス検索・電子申請機能への申請データ取得要求及び返信のあった申請データの取得並びに申請データ処理状況の登録を行う。取得した申請データは、「2. システム間連携制御機能」により住民記録システムからマイナンバーカードに搭載されている利用者証明用電子証明書のシリアル番号と住記宛名番号が紐づいた情報を取得し、申請データに含まれるシリアル番号を住記宛名番号へ変換し、住記宛名番号及び団体内統合宛名番号を申請データに紐づけてデータベースに保管するとともに、申請データを業務システムに連携する機能。 								
③他のシステムとの接続	<table border="0"> <tr> <td>[] 情報提供ネットワークシステム</td> <td>[] 庁内連携システム</td> </tr> <tr> <td>[] 住民基本台帳ネットワークシステム</td> <td>[<input checked="" type="checkbox"/>] 既存住民基本台帳システム</td> </tr> <tr> <td>[] 宛名システム等</td> <td>[<input checked="" type="checkbox"/>] 税務システム</td> </tr> <tr> <td>[<input checked="" type="checkbox"/>] その他 (</td> <td>中間サーバー、国民健康保険システム、介護保険システム、福祉情報システム、財務会計システム、人事・給与システム、サービス検索・電子申請機能)</td> </tr> </table>	[] 情報提供ネットワークシステム	[] 庁内連携システム	[] 住民基本台帳ネットワークシステム	[<input checked="" type="checkbox"/>] 既存住民基本台帳システム	[] 宛名システム等	[<input checked="" type="checkbox"/>] 税務システム	[<input checked="" type="checkbox"/>] その他 (中間サーバー、国民健康保険システム、介護保険システム、福祉情報システム、財務会計システム、人事・給与システム、サービス検索・電子申請機能)
[] 情報提供ネットワークシステム	[] 庁内連携システム								
[] 住民基本台帳ネットワークシステム	[<input checked="" type="checkbox"/>] 既存住民基本台帳システム								
[] 宛名システム等	[<input checked="" type="checkbox"/>] 税務システム								
[<input checked="" type="checkbox"/>] その他 (中間サーバー、国民健康保険システム、介護保険システム、福祉情報システム、財務会計システム、人事・給与システム、サービス検索・電子申請機能)								

システム4

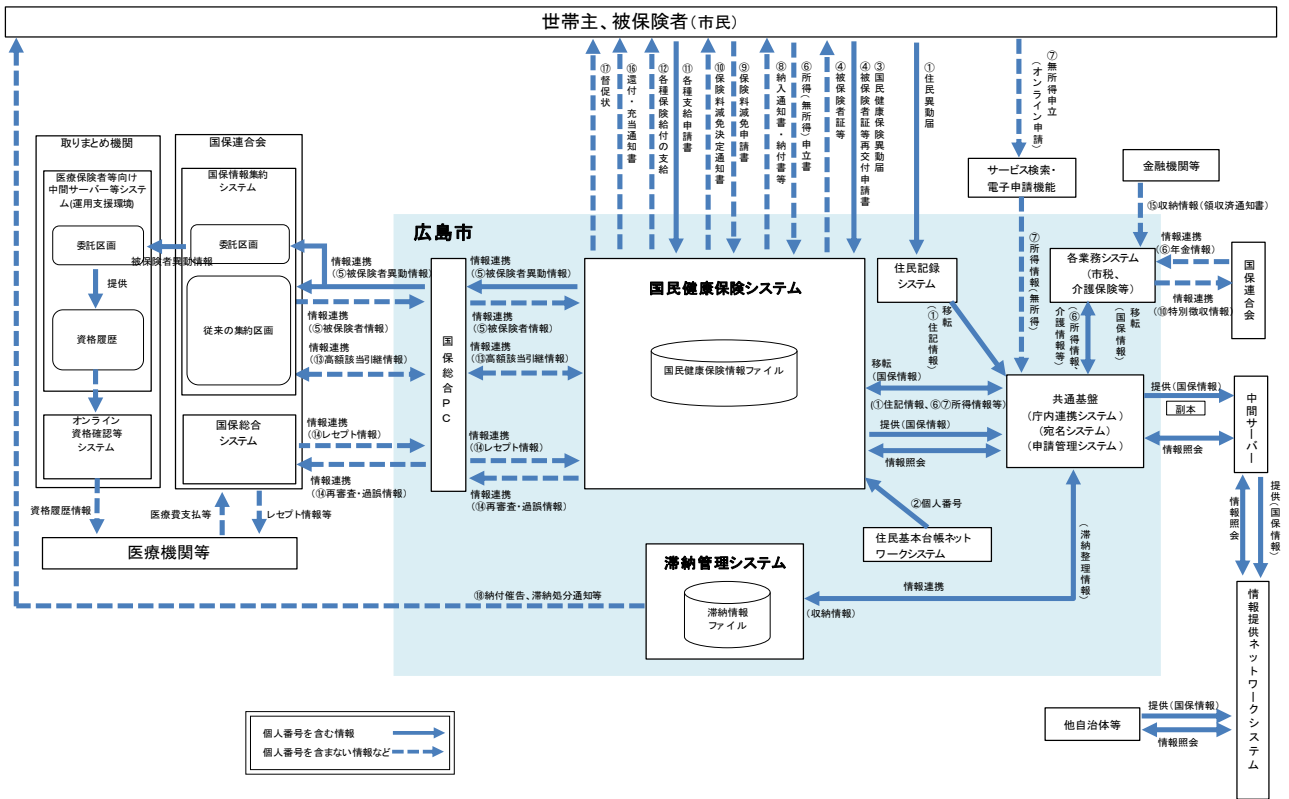
①システムの名称	中間サーバー
	<ol style="list-style-type: none"> 符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 情報照会機能 情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報の情報照会及び情報提供受領を行う機能。 情報提供機能 情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報の提供を行う機能。 既存システム接続機能 中間サーバーと既存システム、団体内統合宛名システム及び住基システムとの間で情報照会内容、情報提供内容、特定個人情報、符号取得のための情報等について連携する機能。

<p>②システムの機能</p>	<p>「医療保険者等向け中間サーバー等」は、医療保険者等全体または医療保険制度横断で資格管理等を行う際に必要となるシステムであり、(1)資格履歴管理事務に係る機能、(2)情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能、(3)地方公共団体情報システム機構に対して住民基本台帳ネットワークシステムを通じて機構保存本人確認情報の提供を求める機能(以下「本人確認事務に係る機能」という。)を有する。 医療保険者等向け中間サーバー等は、取りまとめ機関が運営する。</p> <p>なお、市区町村国保に関しては、情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能のうち情報照会及び情報提供、本人確認事務に係る機能については、「地方公共団体における情報連携プラットフォームに係る中間サーバー(自治体中間サーバー)」を利用するため、「医療保険者等向け中間サーバー等」では、情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能のうち情報照会及び情報提供、本人確認事務に係る機能は行わない。</p> <p>(1)資格履歴管理事務に係る機能 (i)資格履歴管理(評価対象) ・医療保険者等が、加入者等の基本4情報(又はその一部)、資格情報及び各種証情報(個人番号含む。)を委託区画に登録する。 ・運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する(※1)。 (ii)オンライン資格確認等システムへの資格情報の提供(個人番号を用いないため評価対象外) ・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。 ※1 当該機能については支払基金が特定個人情報保護評価を実施するため当評価の対象外。</p> <p>(2)情報提供ネットワークシステムを通じた情報照会・提供事務に係る機能 (i)機関別符号取得(※2)(評価対象外) ・医療保険者等からの符号取得要求を受領後、システムの自動処理により、符号取得要求ファイルを生成し、情報提供サーバーに転送する。 ・支払基金職員が情報提供サーバーアプリケーションを操作することで、情報提供ネットワークシステムから機関別符号を取得し、機関別符号ファイルに格納する。 (ii)情報照会及び(iii)情報提供(副本情報)(実施しないため評価対象外) ・市区町村国保による情報提供(副本情報)は、「地方公共団体における情報連携プラットフォームに係る中間サーバー(自治体中間サーバー)」を経由して情報提供ネットワークシステムと接続するため、医療保険者等向け中間サーバー等では行わない。 (iv)情報提供(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)(※2)(評価対象外) ・マイナポータルからの自己情報開示の求めを受け付け、システムの自動処理により、運用支援環境において被保険者等を特定し、資格履歴ファイルからオンライン資格確認等システムで管理している情報と紐付けるために使用する情報(個人番号は含まない。)を提供する。 ※2 当該機能については支払基金が特定個人情報保護評価を実施するため当評価の対象外。</p> <p>(3)本人確認事務に係る機能 (i)個人番号取得及び(ii)基本4情報取得(実施しないため評価対象外) ・市区町村国保による情報提供(副本情報)は、「地方公共団体における情報連携プラットフォームに係る中間サーバー(自治体中間サーバー)」を経由して情報提供ネットワークシステムと接続するため、医療保険者等向け中間サーバー等では行わない。</p>
<p>③他のシステムとの接続</p>	<p>[] 情報提供ネットワークシステム [] 庁内連携システム [] 住民基本台帳ネットワークシステム [] 既存住民基本台帳システム [] 宛名システム等 [] 税務システム [] その他 ()</p>

システム8									
①システムの名称	サービス検索・電子申請機能								
②システムの機能	<ul style="list-style-type: none"> ・【住民向け機能】自らが受けることができるサービスをオンラインで検索及び申請ができる機能 ・【地方公共団体向け機能】住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能 								
③他のシステムとの接続	<table border="0"> <tr> <td>[] 情報提供ネットワークシステム</td> <td>[<input checked="" type="checkbox"/>] 庁内連携システム</td> </tr> <tr> <td>[] 住民基本台帳ネットワークシステム</td> <td>[] 既存住民基本台帳システム</td> </tr> <tr> <td>[<input checked="" type="checkbox"/>] 宛名システム等</td> <td>[] 税務システム</td> </tr> <tr> <td>[] その他 ()</td> <td></td> </tr> </table>	[] 情報提供ネットワークシステム	[<input checked="" type="checkbox"/>] 庁内連携システム	[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム	[<input checked="" type="checkbox"/>] 宛名システム等	[] 税務システム	[] その他 ()	
[] 情報提供ネットワークシステム	[<input checked="" type="checkbox"/>] 庁内連携システム								
[] 住民基本台帳ネットワークシステム	[] 既存住民基本台帳システム								
[<input checked="" type="checkbox"/>] 宛名システム等	[] 税務システム								
[] その他 ()									
3. 特定個人情報ファイル名									
国民健康保険情報ファイル、滞納情報ファイル									
4. 特定個人情報ファイルを取り扱う理由									
①事務実施上の必要性	<p>1. 国民健康保険情報ファイル</p> <ul style="list-style-type: none"> ・本市国民健康保険に加入する前の医療保険者の資格情報を正確に取得する等により、被保険者資格管理事務を公平・公正に行うため ・転入前市町村から被保険者の所得情報を正確に取得する等により、保険料賦課管理事務を公平・公正に行うため ・他保険者の給付情報を正確に取得する等により、給付管理事務を公平・公正に行うため ・保険料の収納状況を適正に管理することにより、被保険者間の負担の公平を図るため <p>2. 滞納情報ファイル</p> <ul style="list-style-type: none"> ・保険料の滞納状況を適正に管理することにより、保険料の収納を確保し、被保険者間の負担の公平を図るため <p><オンライン資格確認の準備業務></p> <ul style="list-style-type: none"> ・オンライン資格確認で被保険者等の資格情報を利用するためには、医療保険者等向け中間サーバー等において、医療保険者等の加入者等の履歴情報を正確に管理する必要があり、その履歴情報の生成の際には、同一人であることを正確に把握するために個人番号を用いることから、特定個人情報として国民健康保険関連情報ファイルを保有する。 								
②実現が期待されるメリット	<ul style="list-style-type: none"> ・本市国民健康保険に加入する前の医療保険者より資格情報を取得することにより、被保険者資格管理事務の効率化が図られる。 ・転入前市町村から被保険者の所得情報を取得することにより、文書による照会がなくなり保険料賦課管理事務及び給付管理事務の効率化が図られる。 ・他保険者の給付情報を取得することにより、本市国民健康保険との間の給付調整の効率化が図られる。 <p><オンライン資格確認の準備業務></p> <ul style="list-style-type: none"> ・オンライン資格確認等システムを通して、資格喪失後の受診に伴う事務コスト等の解消、高額療養費限度額適用認定証等の発行業務等の削減、被保険者番号の入力自動化による返戻レセプトの削減、後続開発システムとの連携による保健医療データ活用のしくみを実現する。 								
5. 個人番号の利用 ※									
法令上の根拠	<p>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(以下「番号利用法」という。)第9条第1項、番号利用法別表の44の項、番号利用法別表の主務省令で定める事務を定める命令第24条、番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条</p> <p><オンライン資格確認の準備業務></p> <ul style="list-style-type: none"> ・番号利用法 第9条第1項(利用範囲)別表 項番44 ・番号利用法別表の主務省令で定める事務を定める命令 第24条 ・国民健康保険法 第113条の3 第1項及び第2項 								
6. 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	<table border="0"> <tr> <td>[実施する]</td> <td> <p><選択肢></p> <p>1) 実施する</p> <p>2) 実施しない</p> <p>3) 未定</p> </td> </tr> </table>	[実施する]	<p><選択肢></p> <p>1) 実施する</p> <p>2) 実施しない</p> <p>3) 未定</p>						
[実施する]	<p><選択肢></p> <p>1) 実施する</p> <p>2) 実施しない</p> <p>3) 未定</p>								

<p>②法令上の根拠</p>	<p>【情報照会の根拠】 番号利用法第19条第8号に基づく主務省令第2条の表 69の項、70の項、71の項 番号利用法別表の主務省令で定める事務を定める命令 第24条</p> <p>【情報提供の根拠】 番号利用法第19条第8号に基づく主務省令第2条の表 2の項、3の項、6の項、13の項、16の項、19の項、27の項、38の項、42の項、48の項、56の項、65の項、69の項、83の項、87の項、111の項、115の項、125の項、131の項、137の項、141の項、145の項、158の項、161の項、164の項、165の項、166の項、173の項</p> <p><オンライン資格確認の準備業務> ・番号利用法 附則第6条第4項（利用目的:情報連携のためではなくオンライン資格確認の準備として機関別符号を取得する等） ・国民健康保険法 第113条の3 第1項及び第2項</p>
<p>7. 評価実施機関における担当部署</p>	
<p>①部署</p>	<p>健康福祉局保健部保険年金課</p>
<p>②所属長の役職名</p>	<p>保険年金課長</p>
<p>8. 他の評価実施機関</p>	
<p>なし</p>	

(別添1) 事務の内容



(備考)

【被保険者資格管理に関する事務】

- ①住民異動による資格取得・喪失、氏名変更、世帯変更等の届出の受理、確認を行う。
- ②届出書等に記載された個人番号について、必要に応じて個人番号の真正性の確認を行う。
- ③被用者保険等の喪失による資格取得、被用者保険等への加入に伴う資格喪失届の受理、確認を行う。
- ④被保険者証、高齢受給者証等の交付申請受理、確認及び交付を行う。
- ⑤都道府県単位で資格管理を行うため、被保険者情報の連携を行う。(別紙「1. 資格継続業務」参照)
また、オンライン資格確認等システムで被保険者の資格情報を利用するため、国保総合(国保集約)システム経由で、医療保険者等向け中間サーバー等システムの委託区画へ、被保険者異動情報の登録を行う。(別紙「3. オンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者異動情報の提供」参照)

【保険料賦課管理に関する事務】

- ⑥保険料の算定等のための所得(年金情報を含む。)を把握する。無所得の申立ては、窓口や郵送での書類の受入のほか、サービス検索・電子申請機能での受領により行う。
- ⑦サービス検索・電子申請機能により申請された電子申請データを申請管理システムにより受領
- ⑧保険料の賦課を行う。
- ⑨保険料の減免の申請受理、決定を行う。
- ⑩年金の特別徴収情報を提供する。

【給付管理に関する事務】

- ⑪各保険給付の申請受理、確認を行う。
- ⑫保険給付申請の内容を審査し、世帯の所得状況に応じた支給を行う。
- ⑬高額療養費の高額該当回数の引き継ぎ確認を行う。(別紙「2. 高額該当の引き継ぎ業務」参照)
- ⑭国保連合会からレセプト情報を受領し、再審査・過誤の確認を行う。

【保険料収納管理に関する事務】

- ⑮保険料の納付状況について、金融機関等からの領収済通知書等により確認する。
- ⑯保険料の過納付や誤納付について、超過額を還付又は充当し、世帯主に通知する。
- ⑰保険料を納期限までに完納しない場合は、世帯主に督促状を送付する。

【保険料滞納管理に関する事務】

- ⑱督促状を送付後も保険料を完納しない場合は、広島市市税等お知らせセンターから世帯主に電話による納付勧奨等を行う。また、職員による滞納整理を開始する。

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	
1. 国民健康保険情報ファイル	
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 ※	・本市の国民健康保険被保険者及びその世帯主 ・過去に上記に該当していた者で、国民健康保険法第5条に該当しなくなった、又は国民健康保険法第6条に該当することとなったことにより被保険者資格を喪失した者及びその世帯主
その必要性	保険料の賦課、徴収等及び保険給付を公平・公正に行うため
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"/>] 5情報(氏名、氏名の振り仮名、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	<ol style="list-style-type: none"> 1. 識別情報 ・個人番号:対象者を正確に特定するために保有(参照)する。 ・その他識別情報(内部番号):本市において、個人を一意に識別するために独自の識別番号を保有する。 2. 連絡先等情報 ・5情報:被保険者証、保険料の納入通知書等の印字等、事務で必要とする氏名、住所等を管理するために保有する。 ・連絡先:本人への連絡等のため保有する。 ・その他住民票関係情報:世帯主と被保険者の関係を示す続柄等を保有する。 3. 業務関係情報 ・地方税関係情報:保険料の算定、高額療養費の支給等を行うための所得情報を保有する。 ・医療保険関係情報:本事務を運用するための国民健康保険情報を保有する。 ・生活保護・社会福祉関係情報:市外の施設に入所したが引き続き本市の国民健康保険に加入する住所地特例に係る入所施設等の情報を保有する。 ・介護・高齢者福祉関係情報:高額介護合算療養費の支給を行うための介護保険情報を保有する。 ・雇用・労働関係情報:非自発的失業者に係る雇用保険情報を保有する。 ・年金関係情報:年金から特別徴収により保険料を徴収するための年金関係情報を保有する。
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年10月
⑥事務担当部署	健康福祉局保健部保険年金課、各區市民部保険年金課及び出張所、財政局収納対策部各課

3. 特定個人情報の入手・使用	
①入手元 ※	<p>[<input type="checkbox"/>] 本人又は本人の代理人</p> <p>[<input type="checkbox"/>] 評価実施機関内の他部署 (企画総務局区政課、財政局税務部市民税課、健康福祉局高齢福祉部介護保険課)</p> <p>[<input type="checkbox"/>] 行政機関・独立行政法人等 (厚生労働省、地方公共団体情報システム機構)</p> <p>[<input type="checkbox"/>] 地方公共団体・地方独立行政法人 (他地方公共団体)</p> <p>[<input type="checkbox"/>] 民間事業者 ()</p> <p>[<input type="checkbox"/>] その他 (他医療保険者、広島県国民健康保険団体連合会)</p>
②入手方法	<p>[<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</p> <p>[<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</p> <p>[<input type="checkbox"/>] 情報提供ネットワークシステム</p> <p>[<input type="checkbox"/>] その他 (市税システム端末の直接操作、サービス検索・電子申請機能、申請管理システム)</p>
③入手の時期・頻度	<p>1. 識別情報 新規取得又は変更が発生した都度入手する。</p> <p>2. 連絡先等情報 新規取得又は変更が発生した都度入手する。</p> <p>3. 業務関係情報 ・地方税関係情報:新規取得又は変更が発生した都度入手する。 ・医療保険関係情報:新規取得又は変更が発生した都度入手する。 ・生活保護・社会福祉関係情報:新規取得又は変更が発生した都度入手する。 ・介護・高齢者福祉関係情報:月1回 ・雇用・労働関係情報:新規取得又は変更が発生した都度入手する。 ・年金関係情報:月1回</p> <p>※国保連合会から入手する資格継続業務に係る被保険者情報(国民健康保険に関する都道府県単位の被保険者資格情報)、高額該当の引き継ぎ業務に係る引き継ぎ情報(継続候補世帯リスト、継続世帯確定リスト等転出地市区町村から転入地市区町村へ高額該当情報を引き継ぐための情報)は次のとおり。</p> <p>・被保険者情報:平成30年4月以後に、日1回 ・引き継ぎ情報:平成30年4月以後に、月1回</p>
④入手に係る妥当性	<p><国保連合会からの入手> 国民健康保険に関して、被保険者資格等の管理を都道府県単位で実施する必要があり、個人番号利用事務の一部を国保連合会に委託しているため、本市が保険給付の支給、保険料の徴収または保健事業等を実施するためには、国保連合会から当該情報を入手する必要がある。 なお、入手する情報は、本市分の被保険者、擬制世帯主、過去に被保険者であった者、過去に擬制世帯主であった者のみであり、当該事務において必要な範囲内の情報である。</p> <p>1. 入手の時期・頻度の妥当性 ・資格継続業務 ・被保険者情報:国保総合(国保集約)システム上で管理している被保険者資格を、住民基本台帳に記載する必要があり、日次で連携を行うことで住民票の記載事項の正確性を確保する。 ・高額該当の引き継ぎ業務 ・引き継ぎ情報:高額療養費制度は、医療機関等での支払額が、暦月で一定額を超えた場合にその超過額を支給する制度のため月次計算を行うが、その計算前に月次で連携を行うことで、支給の正確性を確保する。</p> <p>2. 入手方法の妥当性 ・入手は専用線を用いて行うが、信頼性、安定性の高い通信環境が実現でき、さらに通信内容の暗号化とあわせて通信内容の漏えいや盗聴に対するリスクが低く、頻繁に通信が必要な場合には通所の通信回線である公衆網を使うよりも低コストとなることが期待できる。</p> <p><その他入手に関する妥当性> 公平・公正な保険料の賦課、徴収等及び保険給付を行うためには、世帯主及び被保険者の住民票関係情報、所得情報、介護保険情報等を正確に把握しなければならない。 住民から直接入手する以外の個人情報は住民の2度手間とならぬよう、関係部署・機関から入手している。その頻度・時期については(正確性を期するため)提供元の事務サイクルに合わせている。ただし、住民の利益に資するためには、国民健康保険事務において必要なタイミングに必要な情報が入手できるようにする必要があるのであるため、関係先と協議し、可能な範囲で迅速な入手に努めている。</p>

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 (6) 件
委託事項1	国民健康保険システムの運用・保守業務
①委託内容	国民健康保険システムの運用及び保守業務(ハードウェア保守、ソフトウェア保守、バッチ・オンライン運用管理、障害対応及び小規模なシステム改修)
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
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
対象となる本人の範囲 ※	・本市の国民健康保険被保険者及びその世帯主 ・過去に上記に該当していた者で、国民健康保険法第5条に該当しなくなった、又は国民健康保険法第6条に該当することとなったことにより被保険者資格を喪失した者及びその世帯主
その妥当性	バッチ・オンライン運用管理、障害対応等においては、システムで保有するすべてのデータを取り扱うため、特定個人情報ファイルの全体の取扱いを委託することが妥当である。
③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
④委託先への特定個人情報ファイルの提供方法	[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<input checked="" type="radio"/>] その他 (システムの直接操作)
⑤委託先名の確認方法	広島市ホームページの調達情報公開システムにより、委託先名を公表している。
⑥委託先名	日本電気株式会社 中国支社
再委託	
⑦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
⑧再委託の許諾方法	契約書において、「委託業務の全部又は一部を第三者に請け負わせ、若しくは委任してはならない。ただし、あらかじめ書面により甲(発注者)の承認を得た場合は、当該委託業務の一部を第三者に請け負わせ、又は委任することができる。」としており、受注者から再委託等承諾申請書の提出があり、内容を審査したところ適正であると認められたため、承諾している。
⑨再委託事項	ハードウェア保守、ソフトウェア保守、バッチ・オンライン運用管理、障害対応及び小規模なシステム改修の各業務における作業

委託事項2		共通基盤の運用・保守業務
①委託内容		共通基盤に関する運用・保守業務(バックアップ取得、システムの稼働状況の監視、障害・異常発生時の確認及び復旧、自動実行ジョブスケジュールの設定・実行確認等)
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	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
	対象となる本人の範囲 ※	・本市の国民健康保険被保険者及びその世帯主 ・過去に上記に該当していた者で、国民健康保険法第5条に該当しなくなった、又は国民健康保険法第6条に該当することとなったことにより被保険者資格を喪失した者及びその世帯主
	その妥当性	バックアップ取得、システム障害・異常発生時の対応においては、システムで保有するすべてのデータを取り扱うため、特定個人情報ファイルの全体の取扱いを委託することが妥当である。
③委託先における取扱者数		[10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
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<input checked="" type="radio"/>] その他 (システムの直接操作)
⑤委託先名の確認方法		広島市ホームページの調達情報公開システムにより、委託先名を公表している。
⑥委託先名		株式会社日立製作所
再委託	⑦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
	⑧再委託の許諾方法	委託契約書において、「委託業務の全部又は一部を第三者に委任し、若しくは請け負わせてはならない。ただし、あらかじめ書面により甲の承諾を得た場合は、当該業務の一部を第三者に委任し、又は請け負わせることができる。」としており、受託者から再委託承諾申請書の提出があり、内容を審査したところ適正であると認められたため、承諾している。
	⑨再委託事項	共通基盤の運用・保守業務のうち、システムの稼働状況の監視、障害・異常発生時の確認、自動実行ジョブスケジュールの実行確認等

委託事項3		資格継続業務、高額該当回数の引き継ぎ業務に関する市町村保険者事務共同処理業務
①委託内容		<p>・療養給付の審査・支払に付随する業務として、都道府県単位で管理することとなる資格取得年月日や喪失年月日の管理(資格継続業務)と、同一都道府県内で転居があった場合における高額療養費の該当回数を通算するための同一世帯判定に必要な情報等の管理(高額該当の引き継ぎ業務)を委託する(国保情報集約システムを使用する)。</p> <p>・なお、個人番号を用いるのは、資格継続業務と高額該当の引き継ぎ業務(国保総合(国保集約)システム)のみであり、国民健康保険の療養給付等の審査・支払業務そのものには、個人番号を用いない。</p> <p>・オンライン資格確認等システムで被保険者等の資格情報を利用するため、国保連合会は、市区町村より受領した被保険者資格異動に関するデータを編集し、「医療保険者等向け中間サーバー等」へ送信、登録を行う。</p>
②取扱いを委託する特定個人情報ファイルの範囲		<p>[特定個人情報ファイルの全体]</p> <p><選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部</p>
対象となる本人の数		<p>[10万人以上100万人未満]</p> <p><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</p>
対象となる本人の範囲 ※		<p>・被保険者(*): 広島県の区域内に住所を有する者で、他の医療保険制度の被保険者でない者のうち、本市に住所を有する者</p> <p>・擬制世帯主: 被保険者が属する住民基本台帳上の世帯主のうち、国民健康保険の被保険者でない者(例: 国保に加入している世帯員がいるが、その世帯の世帯主は社会保険に加入している場合に、この国保に未加入の世帯主を「擬制世帯主」という。)</p> <p>・過去に被保険者であった者および過去に擬制世帯主であった者</p> <p>* 国民健康保険法第5条から第6条に基づく被保険者のうち、本市に加入資格が適用される者をいう</p>
その妥当性		<p>・被保険者の情報は、国民健康保険に関する事務の基礎情報であるため管理する必要がある。</p> <p>・医療費の自己負担限度額が非課税区分に該当するかどうかを判定する際には、擬制世帯主の住民税課税状況を含んで判定をするため、被保険者のみでなく、擬制世帯主の情報も必要である。</p> <p>・療養給付の審査・支払に関する業務等を行う上で、被保険者とその被保険者が属する世帯の世帯主(擬制世帯主)に関する所得等の情報を管理する必要がある。</p> <p>・「国民健康保険法(昭和33年法律第192号)」第110条によって保険給付を受ける権利は、2年間有効、「地方自治法(昭和22年法律第67号)第236条1項」によって不当利得の返還を受ける権利は5年間有効とされているため、過去の特定個人情報についても管理する必要がある。</p> <p>・なお、個人番号を用いるのは、資格継続業務と高額該当の引き継ぎ業務およびオンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者資格情報の提供(国保総合(国保集約)システム)のみであり、国民健康保険の療養給付等の審査・支払業務そのものには、個人番号を用いない。</p>
③委託先における取扱者数		<p>[10人以上50人未満]</p> <p><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</p>
④委託先への特定個人情報ファイルの提供方法		<p>[<input checked="" type="checkbox"/>] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。)</p> <p>[] フラッシュメモリ [] 紙</p> <p>[] その他 ()</p>
⑤委託先名の確認方法		広島市ホームページの調達情報公開システムにより、委託先名を公表している。
⑥委託先名		広島県国民健康保険団体連合会
⑦再委託の有無 ※		<p>[再委託する]</p> <p><選択肢> 1) 再委託する 2) 再委託しない</p>
再委託		
⑧再委託の許諾方法		契約書において、「委託業務の全部又は一部を第三者に委任し、若しくは請け負わせてはならない。ただし、あらかじめ書面により甲(発注者)の承諾を得た場合は、当該業務の一部を第三者に委任し、又は請け負わせることができる。」としており、受注者から再委託承諾申請書の提出があり、内容を審査したところ適正であると認められたため、承諾している。
⑨再委託事項		資格継続業務、高額該当回数の引き継ぎ業務で使用する国保総合(国保集約)システムに関する運用業務の一部(バッチ処理パラメータの入力/バッチ処置の実行/バックアップデータの取得と保管/システム障害発生時の復旧支援作業/各種マスターメンテナンス/外字作成・登録)など。

委託事項4		医療保険者等向け中間サーバー等における資格履歴管理事務
①委託内容		オンライン資格確認のための準備として、医療保険者等向け中間サーバー等において、個人番号を利用した被保険者資格の履歴管理、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などを行う。
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	<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
	対象となる本人の範囲 ※	・被保険者(*): 広島県の区域内に住所を有する者で、他の医療保険制度の被保険者でない者のうち、本市に住所を有する者 ・擬制世帯主: 被保険者が属する住民基本台帳上の世帯主のうち、国民健康保険の被保険者でない者(例: 国保に加入している世帯員がいるが、その世帯の世帯主は社会保険に加入している場合に、この国保に未加入の世帯主を「擬制世帯主」という。) ・過去に被保険者であった者および過去に擬制世帯主であった者 * 国民健康保険法第5条から第6条に基づく被保険者のうち、本市に加入資格が適用される者をいう
	その妥当性	オンライン資格確認等システムで被保険者等の資格情報を利用するために、加入者の資格履歴情報の管理を行う。
③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
④委託先への特定個人情報ファイルの提供方法		[<input type="radio"/>] 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 ()
⑤委託先名の確認方法		広島市ホームページの調達情報公開システムにより、委託先名を公表する。
⑥委託先名		広島県国民健康保険団体連合会 (広島県国民健康保険団体連合会は、国保中央会に再委託する)
再委託	⑦再委託の有無 ※	[<input type="checkbox"/> 再委託する] <選択肢> 1) 再委託する 2) 再委託しない
	⑧再委託の許諾方法	委託先の広島県国保連合会から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、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、再委託先への立ち入り調査に係る要件、その他当市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、広島県国保連合会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。) 運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、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ことになるため、クラウド事業者は、次を満たすものとする。 ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上および運用上のセキュリティ(OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化etc)をどのように確保したかを書面にて示した上で、許諾を得ること。
	⑨再委託事項	医療保険者等向け中間サーバー等における資格履歴管理事務 (国保中央会から再々委託する「医療保険者等向け中間サーバー等の運用・保守業務」を含む)

委託事項6	国保総合(国保集約)システムに係るアプリケーション保守業務及びシステム運用事務	
①委託内容	国保総合(国保集約)システムに係るアプリケーション保守業務(アプリケーション改修、データパッチ実施等)及びシステム運用事務(バックアップ取得、システム障害等発生時のデータ復旧等)	
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	対象となる本人の数	<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
	対象となる本人の範囲 ※	・被保険者(*): 都道府県の区域内に住所を有する者で、他の医療保険制度の被保険者でない者のうち、当市に住所を有する者 ・擬制世帯主: 被保険者が属する住民基本台帳上の世帯主のうち、国民健康保険の被保険者でない者 (例: 国保に加入している世帯員がいるが、その世帯の世帯主は社会保険に加入している場合に、この国保に未加入の世帯主を「擬制世帯主」という。) ・過去に被保険者であった者および過去に擬制世帯主であった者 * 国民健康保険法第5条から第6条に基づく被保険者のうち、当市に加入資格が適用される者をいう
その妥当性	・被保険者の情報は、国民健康保険に関する事務の基礎情報であるため管理する必要がある。 ・医療費の自己負担限度額が非課税区分に該当するかどうかを判定する際には、擬制世帯主の住民税課税状況を含んで判定をするため、被保険者のみでなく、擬制世帯主の情報も必要である。 ・療養給付の審査・支払に関する業務等を行う上で、被保険者とその被保険者が属する世帯の世帯主(擬制世帯主)に関する所得等の情報を管理する必要がある。 ・「国民健康保険法(昭和33年法律第192号)」第110条によって保険給付を受ける権利は、2年間で有効、「地方自治法(昭和22年法律第67号)第236条1項」によって不当利得の返還を受ける権利は5年間で有効とされているため、過去の特定個人情報についても管理する必要がある。 ・なお、個人番号を用いるのは、資格継続業務と高額該当の引き継ぎ業務およびオンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者資格情報の提供(国保総合(国保集約)システム)のみであり、国民健康保険の療養給付等の審査・支払業務そのものには、個人番号を用いない。	
③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
④委託先への特定個人情報ファイルの提供方法	[<input checked="" 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 ()	
⑤委託先名の確認方法	広島市ホームページの調達情報公開システムにより、委託先名を公表する。	
⑥委託先名	広島県国民健康保険団体連合会 (広島県国民健康保険団体連合会は、国保中央会に再委託する)	

再委託	⑦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
	⑧再委託の許諾方法	<p>委託先の広島県国民健康保険団体連合会から再委託先の商号又は名称、住所、再委託する理由、再委託する業務の範囲、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、再委託先への立ち入り調査に係る要件、その他当市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、広島県国民健康保険団体連合会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。)</p> <p>国保総合(国保集約)システムを、クラウド事業者が保有・管理する環境に設置する場合、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ことになるため、クラウド事業者は、次を満たすものとする。</p> <ul style="list-style-type: none"> ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 ・クラウド事業者が提供するクラウドサービスは、政府情報システムのためのセキュリティ評価制度(ISMAP)に基づくクラウドサービスリストに掲載されているものとする。 <p>国保総合(国保集約)システムを、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上および運用上のセキュリティ(OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化etc)をどのように確保したかを書面にて示した上で、許諾を得ること。</p>	
	⑨再委託事項	国保総合(国保集約)システムに係るアプリケーション保守業務及びシステム運用事務の全て	

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 (28) 件 [<input checked="" type="checkbox"/>] 移転を行っている (13) 件 [] 行っていない
提供先1	別紙1に掲げる情報照会者(番号利用法第19条第8号に基づく主務省令第2条の表に定める情報照会者)
①法令上の根拠	番号利用法第19条第8号
②提供先における用途	別紙1に掲げる事務
③提供する情報	医療に関する給付の支給又は保険料の徴収に関する情報であって主務省令で定めるもの
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	・本市の国民健康保険被保険者及びその世帯主 ・過去に上記に該当していた者で、国民健康保険法第5条に該当しなくなった、又は国民健康保険法第6条に該当することとなったことにより被保険者資格を喪失した者及びその世帯主
⑥提供方法	[<input checked="" type="checkbox"/>] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	随時
移転先1	財政局税務部市民税課、各市税事務所
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条
②移転先における用途	個人市民税の課税に関する事務
③移転する情報	国民健康保険料の納付に関する情報
④移転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移転する情報の対象となる本人の範囲	国民健康保険料の納付義務者
⑥移転方法	[<input checked="" type="checkbox"/>] 庁内連携システム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	年1回
移転先2	財政局税務部市民税課
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条
②移転先における用途	個人市民税の課税に関する事務
③移転する情報	地方税法第321条の7の2第1項に規定する特別徴収対象年金所得者の判定に必要となる国民健康保険料の年金天引き(特別徴収)に関する情報

移転先5	健康福祉局高齢福祉部介護保険課、各区厚生部福祉課	
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条	
②移転先における用途	介護保険要支援・要介護認定に関する事務、介護保険給付の支給に関する事務	
③移転する情報	国民健康保険被保険者の資格に関する情報	
④移転する情報の対象となる本人の数	[1万人以上10万人未満]	<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
⑤移転する情報の対象となる本人の範囲	国民健康保険被保険者	
⑥移転方法	<input checked="" type="checkbox"/> 庁内連携システム <input type="checkbox"/> 電子メール <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> その他 ()	<input type="checkbox"/> 専用線 <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> 紙
⑦時期・頻度	随時	
移転先6	健康福祉局高齢福祉部介護保険課、各区厚生部福祉課	
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条	
②移転先における用途	高額医療合算介護(介護予防)サービス費の支給	
③移転する情報	高額医療合算介護(介護予防)サービス費の算定に関する情報	
④移転する情報の対象となる本人の数	[1万人未満]	<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
⑤移転する情報の対象となる本人の範囲	高額介護合算療養費の支給申請者	
⑥移転方法	<input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 電子メール <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> その他 ()	<input type="checkbox"/> 専用線 <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input checked="" type="checkbox"/> 紙
⑦時期・頻度	随時	
移転先7	健康福祉局障害福祉部障害自立支援課、各区厚生部福祉課	
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条	
②移転先における用途	障害者の日常生活及び社会生活を総合的に支援するための法律による自立支援給付の支給に関する事務	
③移転する情報	国民健康保険被保険者の資格に関する情報	
④移転する情報の対象となる本人の数	[1万人未満]	<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

移転先10	健康福祉局精神保健福祉センター、各区厚生部福祉課	
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条	
②移転先における用途	自立支援医療費(精神通院)の支給認定	
③移転する情報	国民健康保険被保険者の資格に関する情報	
④移転する情報の対象となる本人の数	[1万人以上10万人未満]	<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
⑤移転する情報の対象となる本人の範囲	国民健康保険被保険者及び被保険者資格喪失者のうち自立支援医療費(精神通院)の支給認定申請者	
⑥移転方法	<input checked="" type="checkbox"/> 庁内連携システム <input type="checkbox"/> 電子メール <input type="checkbox"/> フラッシュメモリ <input type="checkbox"/> その他 ()	<input type="checkbox"/> 専用線 <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> 紙
⑦時期・頻度	随時	
移転先11	健康福祉局保健部健康推進課	
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条	
②移転先における用途	予防接種法による給付の支給に関する事務	
③移転する情報	国民健康保険の給付に関する情報	
④移転する情報の対象となる本人の数	[1万人未満]	<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
⑤移転する情報の対象となる本人の範囲	予防接種による健康被害を受けた者であって、国民健康保険の給付を受けた者	
⑥移転方法	<input type="checkbox"/> 庁内連携システム <input type="checkbox"/> 電子メール <input checked="" type="checkbox"/> フラッシュメモリ <input type="checkbox"/> その他 ()	<input type="checkbox"/> 専用線 <input type="checkbox"/> 電子記録媒体(フラッシュメモリを除く。) <input type="checkbox"/> 紙
⑦時期・頻度	必要に応じて。	

移転先12	健康福祉局保健部健康推進課
①法令上の根拠	番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条
②移転先における用途	感染症の予防及び感染症の患者に対する医療に関する法律による入院の費用負担に関する事務
③移転する情報	国民健康保険の給付に関する情報
④移転する情報の対象となる本人の数	[1万人未満] <small><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</small>
⑤移転する情報の対象となる本人の範囲	感染症の予防及び感染症の患者に対する医療に関する法律に基づく入院勧告又は措置された者のうち、国民健康保険の給付を受けた者
⑥移転方法	[] 庁内連携システム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [<input checked="" type="checkbox"/>] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	必要に応じて。
移転先13	企画総務局区政課、各区市民部市民課及び出張所
①法令上の根拠	住民基本台帳法第7条第10号
②移転先における用途	住民基本台帳に関する事務
③移転する情報	国民健康保険被保険者の資格に関する情報
④移転する情報の対象となる本人の数	[10万人以上100万人未満] <small><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</small>
⑤移転する情報の対象となる本人の範囲	・本市の国民健康保険被保険者 ・過去に上記に該当していた者で、国民健康保険法第5条に該当しなくなった、又は国民健康保険法第6条に該当することとなったことにより被保険者資格を喪失した者
⑥移転方法	[<input checked="" type="checkbox"/>] 庁内連携システム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()

⑦時期・頻度	随時												
6. 特定個人情報の保管・消去													
①保管場所 ※	<p><広島市における措置></p> <ul style="list-style-type: none"> ・特定個人情報は本市データセンター内に設置したサーバーのデータベース内に保管する。 ・データセンターでは、以下の3か所の入口において入退管理を行う。 <ol style="list-style-type: none"> 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 <p>上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証(指紋)の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。</p> <p>また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること(共連れ)を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。</p> <ul style="list-style-type: none"> ・サーバーは事務で使用するシステムごとのサーバーラック内に設置され、施錠される。サーバーラックは事前にサーバーの使用許可を得た者以外の者が開錠することはできない。 ・データセンター内(サーバー室内を含む)には監視カメラを設置するほか、24時間365日警備員が常駐し、定期的に巡回を行う。 ・データセンターから情報記録媒体の持ち出しを行う場合、事前に本市担当職員が押印した情報記録媒体等持出承認書をデータセンターに持参し、退館する際に警備員に提出することとしている。 ・データセンターから退館する際、警備員による手荷物検査を行い、情報記録媒体等持出承認書に記載のない情報記録媒体を保持していた場合、データセンターからの持ち出しはできない。 ・特定個人情報を含むサーバー内のデータのバックアップテープはデータセンター内の耐火金庫に保管されるほか、大規模災害時の復旧に備えてデータセンターから300km以上離れた場所に分散保管される。 ・特定個人情報が記録された電子記録媒体及び紙媒体は、鍵付保管庫等で保管している。 <p><中間サーバー・プラットフォームにおける措置></p> <p>①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。</p> <ul style="list-style-type: none"> ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 <p>②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間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。</p>												
②保管期間	<p><選択肢></p> <table border="0"> <tr> <td>1) 1年未満</td> <td>2) 1年</td> <td>3) 2年</td> </tr> <tr> <td>4) 3年</td> <td>5) 4年</td> <td>6) 5年</td> </tr> <tr> <td>7) 6年以上10年未満</td> <td>8) 10年以上20年未満</td> <td>9) 20年以上</td> </tr> <tr> <td colspan="3">10) 定められていない</td> </tr> </table> <p>[5年]</p> <p>その妥当性</p> <ul style="list-style-type: none"> ・被保険者資格情報は、被保険者資格を取得している間は消去せず、喪失後も5年間保管している。 ・保険料賦課情報は、当該年度に係る保険料の賦課決定(更正)の期間である5年間保管している。 ・給付情報は、保険給付を受けた日から5年間保管している。 ・保険料収納情報は、保険料が完納されるまでは消去せず、完納後も5年間保管している。 	1) 1年未満	2) 1年	3) 2年	4) 3年	5) 4年	6) 5年	7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上	10) 定められていない		
1) 1年未満	2) 1年	3) 2年											
4) 3年	5) 4年	6) 5年											
7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上											
10) 定められていない													

<p>③ 消去方法</p>	<p><広島市における措置></p> <ul style="list-style-type: none"> ・情報セキュリティ実施手順や広島市文書取扱規程により、情報消去の責任者や手続、方法等保存期間経過後の消去時の取扱いを定めている。 ・保管期間経過後、特定個人情報が保存された記録媒体に対して委託業者が一定回数以上の無作為な書き込みを行った上で、媒体そのものを物理的に破壊することで当該媒体に記録された特定個人情報を消去し、消去した情報、媒体、日付等を記録する。また、データ消去証明書の提出を求め、必要に応じて立ち入り検査を実施している。 ・届出書等の紙媒体については、広島市文書取扱規程により、保管期間経過後、溶解処理を行っている。 <p><中間サーバー・プラットフォームにおける措置></p> <ol style="list-style-type: none"> ① 特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ② クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度 (ISMAP) に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③ 中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。
<p>7. 備考</p>	

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	
2. 滞納情報ファイル	
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 ※	保険料の滞納者等
その必要性	保険料の滞納状況の管理を適正に行い、保険料の収納を確保し、被保険者間の負担の公平を図る必要がある。
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"/>] 5情報(氏名、氏名の振り仮名、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	1. 識別情報 ・個人番号:対象者を正確に特定するために保有(参照)する。 ・その他識別情報(内部番号):本市において、個人を一意に識別するために独自の識別番号を保有する。 2. 連絡先等情報 ・5情報:保険料の納付催告書の印字等、事務で必要とする氏名、住所等を管理するために保有する。 ・連絡先:本人への連絡等のため保有する。 ・その他住民票関係情報:世帯主と被保険者の関係を示す続柄等を保有する。 3. 業務関係情報 ・医療保険関係情報:本事務を運用するための国民健康保険情報を保有する。
全ての記録項目	別添2を参照。
⑤保有開始日	平成27年10月
⑥事務担当部署	財政局税務部税制課及び収納対策部各課

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 checked="" 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 () <input type="checkbox"/> 地方公共団体・地方独立行政法人 () <input type="checkbox"/> 民間事業者 () <input type="checkbox"/> その他 ()
②入手方法	<input type="checkbox"/> 紙 [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ <input type="checkbox"/> 電子メール [] 専用線 [<input checked="" 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 ()
③入手の時期・頻度	1. 識別情報 新規取得又は変更が発生した都度入手する。 2. 連絡先等情報 新規取得又は変更が発生した都度入手する。
④入手に係る妥当性	保険料の滞納状況の管理を適正に行い、被保険者間の保険料負担の公平を図るためには、保険料の収納状況を正確に把握しなければならない。 住民から直接入手する以外の個人情報は住民の2度手間とならぬよう、関係部署・機関から入手している。その頻度・時期については(正確性を期するため)提供元の事務サイクルに合わせている。ただし、住民の利益に資するためには、国民健康保険事務において必要なタイミングに必要な情報が入手できるようにする必要があるので、関係先と協議し、可能な範囲で迅速な入手に努めている。

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 (3) 件	
委託事項1	市税システム(滞納管理システム)の運用・保守業務	
①委託内容	滞納管理システムの運用及び保守業務(ハードウェア保守、ソフトウェア保守、バッチ・オンライン運用管理、障害対応及び小規模なシステム改修)	
②取扱いを委託する特定個人情報ファイルの範囲	[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
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	
対象となる本人の範囲 ※	保険料の滞納者等	
その妥当性	バッチ・オンライン運用管理、障害対応等においては、システムで保有するすべてのデータを取り扱うため、特定個人情報ファイルの全体の取扱いを委託することが妥当である。	
③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	
④委託先への特定個人情報ファイルの提供方法	[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<input checked="" type="radio"/>] その他 (システムの直接操作)	
⑤委託先名の確認方法	広島市ホームページの調達情報公開システムにより、委託先名を公表している。	
⑥委託先名	日本電気株式会社 中国支社	
再委託	⑦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
	⑧再委託の許諾方法	契約書において、「委託業務の全部又は一部を第三者に委任し、若しくは請け負わせてはならない。ただし、あらかじめ書面により甲(発注者)の承諾を得た場合は、当該業務の一部を第三者に委任し、又は請け負わせることができる。」としており、受注者から再委託等承諾申請書の提出があり、内容を審査したところ適正であると認められたため、承諾している。
	⑨再委託事項	ハードウェア保守、ソフトウェア保守、バッチ・オンライン運用管理、障害対応及び小規模なシステム改修の各業務における作業

委託事項2		共通基盤の運用・保守業務
①委託内容		共通基盤に関する運用・保守業務(バックアップ取得、システムの稼働状況の監視、障害・異常発生時の確認及び復旧、自動実行ジョブスケジュールの設定・実行確認等)
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] <選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部
	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
	対象となる本人の範囲 ※	・本市の国民健康保険被保険者及びその世帯主 ・過去に上記に該当していた者で、国民健康保険法第5条に該当しなくなった、又は国民健康保険法第6条に該当することとなったことにより被保険者資格を喪失した者及びその世帯主
	その妥当性	バックアップ取得、システム障害・異常発生時の対応においては、システムで保有するすべてのデータを取り扱うため、特定個人情報ファイルの全体の取扱いを委託することが妥当である。
③委託先における取扱者数		[10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
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [<input checked="" type="radio"/>] その他 (システムの直接操作)
⑤委託先名の確認方法		広島市ホームページの調達情報公開システムにより、委託先名を公表している。
⑥委託先名		株式会社日立製作所
再委託	⑦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
	⑧再委託の許諾方法	委託契約書において、「委託業務の全部又は一部を第三者に委任し、若しくは請け負わせてはならない。ただし、あらかじめ書面により甲の承諾を得た場合は、当該業務の一部を第三者に委任し、又は請け負わせることができる。」としており、受託者から再委託承諾申請書の提出があり、内容を審査したところ適正であると認められたため、承諾している。
	⑨再委託事項	共通基盤の運用・保守業務のうち、システムの稼働状況の監視、障害・異常発生時の確認、自動実行ジョブスケジュールの実行確認等

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	[] 提供を行っている () 件 [] 移転を行っている () 件 [○] 行っていない
----------	---

6. 特定個人情報の保管・消去

①保管場所 ※		<p><広島市における措置></p> <ul style="list-style-type: none"> ・特定個人情報は本市データセンター内に設置したサーバーのデータベース内に保管する。 ・データセンターでは、以下の3か所の入口において入退管理を行う。 <ol style="list-style-type: none"> 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 <p>上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証(指紋)の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。</p> <p>また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること(共連れ)を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。</p> <ul style="list-style-type: none"> ・サーバーは事務で使用するシステムごとのサーバーラック内に設置され、施錠される。サーバーラックは事前にサーバーの使用許可を得た者以外の者が開錠することはできない。 ・データセンター内(サーバー室内を含む)には監視カメラを設置するほか、24時間365日警備員が常駐し、定期的に巡回を行う。 ・データセンターから情報記録媒体の持ち出しを行う場合、事前に本市担当職員が押印した情報記録媒体等持出承認書をデータセンターに持参し、退館する際に警備員に提出することとしている。 ・データセンターから退館する際、警備員による手荷物検査を行い、情報記録媒体等持出承認書に記載のない情報記録媒体を保持していた場合、データセンターからの持ち出しはできない。 ・特定個人情報を含むサーバー内のデータのバックアップテープはデータセンター内の耐火金庫に保管されるほか、大規模災害時の復旧に備えてデータセンターから300km以上離れた場所に分散保管される。 ・特定個人情報が記録された電子記録媒体及び紙媒体は、鍵付保管庫等で保管している。 <p><中間サーバー・プラットフォームにおける措置></p> <p>①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。</p> <ul style="list-style-type: none"> ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 <p>②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間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。</p>											
	②保管期間	<p>期間</p> <p>[定められていない]</p> <p><選択肢></p> <table border="0"> <tr> <td>1) 1年未満</td> <td>2) 1年</td> <td>3) 2年</td> </tr> <tr> <td>4) 3年</td> <td>5) 4年</td> <td>6) 5年</td> </tr> <tr> <td>7) 6年以上10年未満</td> <td>8) 10年以上20年未満</td> <td>9) 20年以上</td> </tr> <tr> <td>10) 定められていない</td> <td></td> <td></td> </tr> </table> <p>その妥当性</p> <p>当該年度に係る保険料の賦課決定(更正)の期間を5年としていることから、保険料が完納されるまでは消去せず、完納後も5年間保管している。</p>	1) 1年未満	2) 1年	3) 2年	4) 3年	5) 4年	6) 5年	7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上	10) 定められていない	
1) 1年未満	2) 1年	3) 2年											
4) 3年	5) 4年	6) 5年											
7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上											
10) 定められていない													

③ 消去方法	<p><広島市における措置></p> <ul style="list-style-type: none">・情報セキュリティ実施手順や広島市文書取扱規程により、情報消去の責任者や手続、方法等保存期間経過後の消去時の取扱いを定めている。・保管期間経過後、特定個人情報が保存された記録媒体に対して委託業者が一定回数以上の無作為な書き込みを行った上で、媒体そのものを物理的に破壊することで当該媒体に記録された特定個人情報を消去し、消去した情報、媒体、日付等を記録する。また、データ消去証明書の提出を求め、必要に応じて立ち入り検査を実施している。・届出書等の紙媒体については、広島市文書取扱規程により、保管期間経過後、溶解処理を行っている。 <p><中間サーバー・プラットフォームにおける措置></p> <ol style="list-style-type: none">①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度 (ISMAP) に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。
	<p>7. 備考</p>

(別添2) 特定個人情報ファイル記録項目

【1. 国民健康保険情報ファイル】

1.被保険者番号、2.国保世帯番号、3.国保主宛名番号、4.国保主個人番号、滞納者対策情報(5.滞納レベル、6.対策内容、7.特別事情情報、8.弁明書情報、9.滞納額減少情報、10.調定額、11.納付額)、12.宛名番号、13.個人番号、14.資格取得日、15.資格取得事由、16.資格喪失日、17.資格喪失事由、18.退職情報、19.加入保険情報、20.修学情報、21.遠隔地施設情報、22.住所地特例情報、23.失業情報、24.特定同一世帯所属者情報、25.旧被扶養者情報、26.氏名、27.住所、28.電話番号、29.性別、30.生年月日、31.続柄、32.住民日、33.保険証種別、34.保険証作成日、35.保険証有効期限、36.保険証交付情報、37.保険証回収情報、38.高齢受給者証負担割合、適用認定証・標準負担額減額証情報(39.発行期日、40.適用区分、41.申請年月日、42.長期該当情報)、特定疾病療養受療証情報(43.疾病名、44.自己負担限度額、45.発行期日)、46.更新年月日、47.更新職員ID

<保険料賦課情報>

1.宛名番号、2.被保険者証番号、3.個人番号、4.国保主宛名番号、5.国保主個人番号、賦課情報(6.相当年度、7.賦課年度、8.賦課基準日、9.賦課区、10.所得割額、11.資産割額、12.均等割額、13.平等割額、14.軽減情報、15.減免情報、16.期別情報、17.年間賦課額、18.納入通知書発行日、19.通知書番号、20.納付手段、21.更正年月日、22.更正処理区分)、年金特別徴収情報(23.基礎年金番号、24.年金被保険者情報、25.介護特別徴収情報、26.特別徴収金額情報、27.特別徴収回付記録情報)、所得情報(28.所得金額情報、29.収入金額情報、30.控除金額情報、31.特別控除額情報、32.住民税課税情報)、33.介護適用除外情報、34.更新年月日、35.更新職員ID

<給付情報>

1.宛名番号、2.被保険者証番号、3.個人番号、4.国保主宛名番号、5.国保主個人番号、6.70歳未満所得区分、7.前期高齢者所得区分、レセプト情報(8.レセプト番号、9.処理年月、10.療養区分、11.種別、12.給付コード、13.診療年月、14.診療実日数、15.点数、16.医療機関情報、17.費用額情報、18.公費情報、19.一部負担金減免・猶予情報、20.過誤・再審査情報)、療養費情報(21.療養費申請情報、22.処理年月、23.療養区分、24.種別、25.給付コード、26.診療年月、27.診療実日数、28.医療機関情報、29.支給情報、30.支払先情報、31.費用額情報、32.公費情報)、高額療養費(33.高額療養費申請情報、34.計算元70未満歳所得区分、35.計算元前期高齢者所得区分、36.高額療養費計算内訳情報、37.該当レセプト情報、38.支給情報、39.支払先情報、40.申請勧奨情報)、出産育児一時金情報(41.出産育児一時金申請情報、42.出産区分、43.支給情報、44.支払先情報)、葬祭費情報(45.葬祭費申請情報、46.死亡年月日、47.葬祭日、48.支給情報、49.支払先情報)、高額医療介護合算療養費情報(50.介護保険資格情報、51.申請者情報、52.医療保険分自己負担額情報、53.介護保険分自己負担額情報、54.自保険者分支給情報、55.他保険者分支給情報、56.支給情報、57.支払先情報)、不当利得情報(58.返納金情報、59.対象レセプト情報)、60.更新年月日、61.更新職員ID

<保険料収納情報>

1.賦課相当年度、2.賦課年度、3.期別、4.宛名番号、5.被保険者証番号、6.個人番号、調定情報(7.調定額、8.納期限、9.延滞金額)、納付情報(10.本料納付額、11.延滞金納付額、12.納付年月日、13.口座振替情報)、還付・充当情報(14.調定年度、15.賦課年度、16.期別、17.過誤納情報、18.還付金額、19.還付加算金額、20.還付年月日、21.還付口座情報、22.充当金額、23.充当年月日)、24.更新年月日、25.更新職員ID

【統合宛名管理テーブル】

1.個人番号、2.団体内統合宛名番号、3.業務宛名番号、4.住所、5.氏名、6.生年月日、7.性別、8.カナ氏名

【申請管理テーブル】

1.受付番号、2.氏名、3.生年月日、4.性別、5.住所、6.電話番号、7.メールアドレス、8.手続名称、9.手続コード、10.申請日時、11.ステータスコード、12.ステータス名称、13.業務宛名番号、14.団体内統合宛名番号、15.利用者証明書シリアル番号、16.カナ氏名、17.FAX番号

○「オンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者異動情報の提供」業務を実施するために、以下の項目を市区町村国保の特定個人情報ファイルの記録項目へ追加しています。

- ・被保険者証記号および被保険者証番号ごとに付番した枝番(個人を識別する2桁の番号)
- ・券面記載の被保険者証記号
- ・券面記載の被保険者証番号
- ・券面記載の氏名(漢字)
- ・券面記載の氏名(漢字)の読み仮名
- ・券面記載氏名が通称名の場合の本名等(漢字)
- ・券面記載氏名が通称名の場合の本名等(漢字)の読み仮名
- ・被保険者証裏面への性別記載の有無

・D/被害者等に関する自己情報開示の申出の有無

・自己負担限度額が変更となった場合、または治癒により証を回収した場合の回収の理由が発生した日

【2. 滞納情報ファイル】

1.所属コード 2.所属課名 3.グループ名称 4.担当者名 5.業務グループ名称 6.個人番号 7.滞納者名 8.住所 9.科目コード 10.区 11.調定年度 12.通知書番号 13.対象年度 14.事業開始年度 15.事業終了年度 16.申告区分 17.調区 18.期別 19.収納額 20.収納延滞金 21.領収年月日 22.収納年月日 23.データ区分 24.納付種類コード 25.収入区分1 26.収入区分2 27.変更日 28.宛名氏名カナ 29.宛名氏名 30.宛名郵便番号 31.宛名住所 32.宛名自宅電話番号 33.関係者区分 34.関係者個人番号 35.氏名カナ 36.氏名 37.郵便番号 38.備考 39.主従区分 40.主個人番号 41.関係 42.滞納者名カナ 43.執行停止ID 44.執行停止金額 45.執行停止要件 46.執行停止確定日 47.再調査回数 48.申請区分 49.申請事由 50.決裁日 51.決裁状態 52.解除_取消日 53.当初納期限 54.納期限 55.法定納期限 56.当初法定納期限等 57.法定納期限等 58.時効完成日 59.当初調定額 60.調定額 61.調定延滞金 62.未納額 63.滞納額 64.滞納延滞金 65.過誤納付額 66.最終領収年月日 67.最終収納年月日 68.完納フラグ 69.督促状発送日 70.処分票フラグ 71.一次催告書発送フラグ 72.分納区分 73.不納欠損確定日 74.徴収猶予開始日 75.徴収猶予終了日 76.換価猶予開始日 77.換価猶予終了日 78.繰上徴収日 79.不納欠損要件 80.催告停止フラグ 81.催告停止開始日 82.催告停止終了日 83.共有個人番号 84.補記情報 85.端末ID 86.新規登録日 87.新規登録時刻 88.更新日 89.更新時刻 90.氏名(名称) 91.共有区分 92.所有者 93.所有者郵便番号 94.所有者住所 95.持ち分子数 96.持ち分母数 97.入力日時 98.電話先 99.相手先 100.相手先名称 101.交渉内容 102.交渉詳細 103.交渉区分 104.削除フラグ 105.交渉担当者名 106.交渉担当者GP名 107.交渉担当者所属課名 108.個人担当者名 109.個人担当者GP名 110.個人担当者所属課名 111.徴収ID 112.猶予内容 113.猶予条件 114.猶予期間開始日 115.猶予期間終了日 116.解除日 117.減免区分 118.期限後1カ月減免率 119.期限後1カ月超減免率 120.特例基準割合適用 121.登記日 122.担保必要額 123.担保提供有無 124.担保無事由 125.担保解除日 126.担保解除事由 127.免除ID 128.免除内容 129.減免条件 130.特例基準割合適用有無 131.免除開始日 132.免除終了日 133.換価ID 134.個人担当者所属名 135.分納ID 136.対象区分 137.対象者通番 138.対象者名 139.分納保証人有無 140.分納保証人名称 141.分納日 142.滞納合計 143.分納理由 144.初回支払日 145.初回支払額 146.二回目以降年月 147.残余金 148.毎月支払日 149.回数指定有無 150.支払回数 151.毎月支払額 152.支払サイクル 153.休日の取り扱い 154.延滞金計算方法 155.端数調整区分 156.端数調整月支払額 157.ボーナス併用有無 158.加算月 159.加算額1 160.加算月2 161.加算額2 162.誓約書受領有無 163.延滞金取扱区分 164.分納担当者名 165.分納担当者GP名 166.分納担当者所属課名 167.支払回番号 168.支払回番号枝番 169.支払方法 170.回数 171.年月 172.予定額 173.収納日 174.充当項目 175.充当金額 176.利率 177.延滞利率 178.充当金額1 179.充当金額1 充当順位 180.充当金額2 181.充当金額2 充当順位 182.充当金額3 183.充当金額3 充当順位 184.充当金額4 185.充当金額4 充当順位 186.取消 187.支払予定日 188.支払予定額 189.残金額 190.充当済額 191.延滞金 192.督促手数料 193.支払済フラグ 194.充当入金日先頭 195.充当入金番号先頭 196.充当入金日最後 197.充当入金番号最後 198.充当金額残額 199.充当利息 200.ソート順 201.グループ名 202.差押ID 203.申請者所属名 204.申請担当者グループコード 205.申請者係 206.申請者名 207.差押区分 208.管理番号 209.権利者氏名 210.交付要求区分 211.交付要求該当条項 212.破産交付要求区分 213.破産交付要求年月日 214.手続きID 215.事件番号 216.受付年月日 217.差押年月日 218.受付番号 219.当時差押年月日 220.延滞金計算日 221.解除受付年月日 222.解除受付番号 223.差押件数 224.財産種別大名称 225.財産種別小名称 226.差押財産評価額合計 227.配当予定日 228.取立金額 229.充当ID 230.充当区分 231.換価代金交付期日 232.充当日 233.充当前本税未納額 234.充当前未納延滞金 235.本税充当金 236.延滞金充当金 237.逆連携不要フラグ 238.繰上ID 239.繰上通番 240.決裁状態区分 241.繰上前納期限 242.繰上後納期限 243.時刻設定区分 244.設定時刻 245.不納欠損ID 246.ステータス変更事由 247.所属課コード 248.財産ID 249.財産種別大 250.財産種別小 251.財産毎通番 252.財産枝番 253.財産内容 254.実残高 255.評価依頼先 256.評価依頼日 257.評価日 258.評価額 259.評価費用 260.特記事項 261.調査結果 262.調査開始日 263.調査完了日 264.預金照会先銀行数 265.作成日時 266.見積評価額 267.個別評価額 268.履行条件 269.履行期限日 270.財産目録 271.賦課区 272.業務グループ名 273.設定時間 274.待機フラグ 275.コメント 276.対象グループ名 277.対象担当者名 278.対象担当者GP名 279.対象担当者所属コード 280.対象担当者所属課名 281.地区担当者コード 282.地区グループ 283.個別設定フラグ 284.特別滞納設定フラグ 285.交渉状況区分 286.最新交渉入力年月日 287.最新交渉入力担当者 288.納付約束区分 289.最新納付約束年月日 290.最新納付約束金額 291.訪問約束区分 292.最新訪問約束年月日 293.最新訪問約束担当者 294.来庁約束区分 295.最新来庁約束年月日 296.最新来庁約束担当者 297.待電約束区分 298.最新待電約束年月日 299.最新待電約束担当者 300.最終接触年月日 301.滞納者種別 302.現在滞納者種別 303.最新収納年月日 304.最新収納金額 305.ワークフロー状態1 306.ワークフロー状態2 307.滞納年度 308.総滞納残合計_原 309.総滞納残延滞金_原 310.総滞納残合計原納 311.総滞納残延滞金原納 312.過誤納付額_納 313.未納額合計 314.指示区分 315.承認区分 316.分納履行区分 317.執行停止区分 318.最新執行停止日 319.最新不納欠損日 320.滞納処分要解除 321.期限経過 322.未決裁有 323.期別催告停止フラグ 324.特徴過誤納付有無 325.国保資格証対象フラグ 326.同一人番号 327.世帯番号 328.住民区分 329.地区コード 330.自治省コード 331.行政区コード 332.方書 333.性別 334.生年月日 335.続柄 336.自宅電話 337.携帯電話 338.勤務先 339.勤務先住所 340.勤務先電話番号 341.送付先 342.住定日 343.住定事由 344.住失日 345.住失事由 346.最新異動年月日 347.最新異動事由 348.死亡年月日 349.約束区分 350.約束区分名称 351.約束取付年月日 352.約束年月日 353.約束金額 354.約束場所 355.納付年月日 356.納付金額 357.訪問場所 358.約束履行状況 359.登録担当者名 360.登録担当者GP名 361.登録担当者所属課名 362.約束担当者名 363.約束担当者GP名 364.役職担当者所属課名 365.実行担当者名 366.実行担当者GP名 367.実行担当者所属課名 368.個人所属課名 369.発行連番 370.請求未納額 371.請求延滞金 372.納付指定日 373.まとめ回数 374.確認番号 375.帳票ID 376.コンビ二連携番号 377.出力日時

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
1. 国民健康保険情報ファイル	
2. 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。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	<p>・届出書又は申請書の受理の際、個人番号カード又は通知カード及び顔写真付きの身分証明書の提示等による本人確認を行い、対象者であることを確認する。</p> <p>・届出書等の内容を国民健康保険システムに入力後、入力者以外の者がその入力された内容と届出書等を照合し、正しく反映されているか確認を行う。</p> <p>＜共通基盤における措置＞</p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、当該事務の対象者以外の情報を入手することはできない。</p> <p>＜国保連合会からの入手における措置＞</p> <p>・国保総合PCにおける措置</p> <p>・入手元は、国保連合会の国保総合(国保集約)システムに限定されており、配信されるデータは国保連合会において、関連性や妥当性および整合性のチェック(*)が行われていることが前提となるため対象者以外の情報を入手することはない。</p> <p>・国保総合PCにおいて対象者の検索や検索結果を表示する画面には、個人番号を表示しないことよって、誤った対象者に関する特定個人情報の入手を防止している。</p> <p>* :ここでいう関連性・整合性チェックとは、すでに個人番号が紐付いている(宛名番号が同じ)人に、以前と異なる個人番号を紐付けようとした場合、あるいは個人番号が空白の場合に、確認リストを出力する等の機能のことを指す。</p>
必要な情報以外を入手することを防止するための措置の内容	<p>・届出書等は、必要とする情報以外が記載できない様式としている。</p> <p>・国民健康保険システムは、必要とする情報以外を登録、管理できない仕様としている。</p> <p>＜共通基盤における措置＞</p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、当該事務に必要な情報以外の情報を入手することはできない。</p> <p>＜国保連合会からの入手における措置＞</p> <p>・国保総合PCにおける措置</p> <p>・入手元は、国保連合会の国保総合(国保集約)システムに限定されており、配信されるデータは国保連合会においてあらかじめ指定されたインターフェース(*)によって配信されることが前提となるため、必要な情報以外を入手することはない。</p> <p>* :ここでいう指定されたインターフェースとは、国保総合(国保集約)システムの外部インターフェース仕様書に記載されている国保連合会の国保総合(国保集約)システムと市区町村に設置する国保総合PCとの間でやりとりされるデータ定義のことをいい、その定義に従った項目(法令等で定められた範囲)でないと、国保連合会の国保総合(国保集約)システムからデータ配信ができない仕組みになっている。</p> <p>＜サービス検索・電子申請機能における措置＞</p> <p>・住民がサービス検索・電子申請機能から電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。</p> <p>・住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。</p>
その他の措置の内容	—
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
リスク2： 不適切な方法で入手が行われるリスク	
	<p>・届出書等の受理は、あらかじめ決められた窓口限定し、奪取が行えないようにしている。</p> <p>・国民健康保険システムの利用は、限られた専用の端末のみで利用でき、あらかじめ承認した利用者・権限の範囲に限っている。</p> <p>＜共通基盤における措置＞</p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を</p>

<p>リスクに対する措置の内容</p>	<p>保有している事務と情報を必要としている事務との間で合意が行われていることを必須条件としている。 ・情報を保有している事務と情報を必要としている事務双方から共通基盤の利用に係る申請書を提出させ、内容に相違がないか確認した上で設定を行っている。</p> <p><国保連合会からの入手における措置> ・国保総合PCにおける措置 ・特定個人情報の入手元は、国保連合会の国保総合(国保集約)システムに限定されており、専用線を用いるとともに、指定されたインタフェース(法令で定められる範囲)でしか入手できないようシステムで制御しており、国保総合(国保集約)システムの外部インタフェース仕様書に記載されている対象、周期およびデータ定義等によって、本市と国保連合会の双方に共通の認識があり、その定義に従った内容でないデータの送受信ができないことで、不適切な方法で入手が行われるリスクを軽減している。</p> <p><サービス検索・電子申請機能における措置> サービス検索・電子申請機能の画面の誘導において住民に何の手続きを探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものが明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。</p>
<p>リスクへの対策は十分か</p>	<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>
<p>リスク3: 入手した特定個人情報 that 不正確であるリスク</p>	
<p>入手の際の本人確認の措置の内容</p>	<p>・届出書等の受理の際、個人番号カード又は通知カード及び顔写真付きの身分証明書の提示を受けて、本人確認を行う。 ・代理人から届出書等を受理する際は、本人からの委任状の確認及び代理人の本人確認を行う。</p> <p><共通基盤における措置> ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の情報と紐付けられたり、全く別の情報に書き換えられたりすることはない。</p> <p><国保連合会からの入手における措置> ・国保総合PCにおける措置 ・特定個人情報の入手元は、国保連合会の国保総合(国保集約)システムに限定されているとともに、国保総合PCにおいて国保連合会から入手する情報は、本市において本人確認を行った上で国保連合会に送信した被保険者情報に、国保連合会が事務処理等を行った結果を付加して配信された情報であるため、本人確認は本市において国保連合会に送付する前に実施済みである。 ・さらに、国保連合会においても本市の国民健康保険システムと同様の宛名番号をキーとして個人識別事項を管理しており、宛名番号をキーとして必要なデータが配信されることをシステム上で担保することで正確性を確保している。 ・国民健康保険システムにおける措置 ・入手した特定個人情報は、本市の国民健康保険システムの被保険者データと突合し正確性を確認してから、当該システムのデータベースへ更新することとしており、不整合があった場合は、国保連合会に電話等で連絡し是正を求めることを行うこととしている。</p> <p><サービス検索・電子申請機能における措置> 住民がサービス検索・電子申請機能から電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。</p>
<p>個人番号の真正性確認の措置の内容</p>	<p>・届出書等の受理の際、個人番号カード又は通知カード等の提示を受けて、国民健康保険システムで照合することにより個人番号の真正性確認を行う。</p> <p><共通基盤における措置> ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の個人番号と紐付けられたり、全く別の番号に書き換えられたりすることはない。</p> <p><国保連合会からの入手における措置> ・国保総合PCにおける措置 ・国保連合会から入手する特定個人情報ファイルには、個人番号は記録されていない。</p>

<p>特定個人情報の正確性確保の措置の内容</p>	<ul style="list-style-type: none"> ・入手した情報について、窓口での聞き取りや添付書類との照合等により確認することで正確性を確保している。 ・本市職員が収集した情報に基づいて、適宜、職権で修正することで正確性を確保している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、システム間連携の過程で情報の正確性が失われることはない。 <p><国保連合会からの入手における措置></p> <ul style="list-style-type: none"> ・国保総合PCにおける措置 <ul style="list-style-type: none"> ・国保連合会から配信される被保険者情報については、本市および他市から送信された被保険者異動情報等をもとに、国保総合(国保集約)システムにおいて処理を行い、その処理結果は本市および他市の双方に配信され、本市および他市の職員が確認している。 ・国保連合会から配信される継続世帯確定結果については、本市から送信した被保険者異動情報等をもとに、国保総合(国保集約)システムにおいて処理を行い、その処理結果を本市の職員が確認している。 ・国民健康保険システムにおける措置 <ul style="list-style-type: none"> ・入手した特定個人情報は、本市の国民健康保険システムの被保険者データと突合し正確性を確認してから、当該システムのデータベースへ更新することとしており、不整合があった場合は、国保連合会に電話等で連絡し是正を求めることを行うこととしている。
<p>その他の措置の内容</p>	<p>—</p>
<p>リスクへの対策は十分か</p>	<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>
<p>リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク</p>	
<p>リスクに対する措置の内容</p>	<ul style="list-style-type: none"> ・特定個人情報が記載された届出書等は、鍵付保管庫等で保管している。 ・事務処理で使用した届出書等は、処理完了後は速やかに保管庫に移している。 ・国民健康保険システムのネットワークは、外部からアクセスできない専用回線を用い、専用の端末のみと接続している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行った上で、あらかじめ認められた通信以外の通信を許可しない仕組みとすることで、特定個人情報の漏えいを防止している。 <p><国保連合会からの入手における措置></p> <ul style="list-style-type: none"> ・国保総合PCにおける措置 <ul style="list-style-type: none"> ・本市の国保総合PCは、国保連合会のみと接続され、接続には専用線を用いる。 ・本市の国保総合PCと国保連合会の国保総合(国保集約)システムとの通信には、認証・通信内容の暗号化を実施している。 ・本市の国保総合PCと国保連合会の国保総合(国保集約)システムとの専用ネットワークは、ウイルス対策ソフトウェア、ファイアウォール等によってセキュアなシステム稼働環境を確保することにより、不適切な方法によってデータが漏えい・紛失することのリスクを軽減している。 ・ウイルス対策ソフトウェアは自動でアップデートを行うこととしており、接続拠点の追加、削除等を含め、ファイアウォール等の設定変更が必要となった際は、国保連合会により迅速に実施される。 ・国保総合PCにおいて対象者の検索や検索結果を表示する画面には、個人番号を表示しないことにより、不適切な操作等によってデータが漏えい・紛失することのリスクを軽減している。 ・国保総合PCへのログイン時の職員認証の他に、ログインを実施した職員・時刻・操作内容の記録が実施されるため、その抑止効果として、不適切な操作等によってデータが漏えい・紛失することのリスクを軽減している。 ・国保総合PCと本市の国民健康保険システムとの間の情報の授受において使用する電子記録媒体については、次の措置を講じる。 <ul style="list-style-type: none"> ・電子記録媒体は記録された情報を暗号化する機能を有しているものに限定する。 ・電子記録媒体は、権限を付与された最小限の職員だけが取り扱うように限定する。 ・電子記録媒体は媒体管理簿で管理し、保管庫に施錠保管する。 ・電子記録媒体に保存する情報については、作業が終わる都度、速やかに情報を消去する。 ・保管する必要がない使用済の電子記録媒体は、物理的破壊等の復元防止措置を行い破棄する。 ・情報システム管理者は月次レベルで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。 <p><サービス検索・電子申請機能における措置></p> <ul style="list-style-type: none"> ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。
<p>リスクへの対策は十分か</p>	<p>[十分である] <選択肢> 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>

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

—

3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク	
宛名システム等における措置の内容	<p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤では、それぞれの番号利用事務の対象となる者の個人番号又は団体内統合宛名番号にのみアクセスできるようにアクセス制御を行っており、目的を超えた紐付けは行われない仕組みとなっている。 ・共通基盤の団体内統合宛名機能は、個人番号と団体内統合宛名番号の紐付を管理する機能であり、事務に必要な情報との紐付けは行われない仕組みとなっている。
事務で使用するその他のシステムにおける措置の内容	<ul style="list-style-type: none"> ・国民健康保険システムには、業務に関係のない情報は保持しない。 ・他業務システムから直接アクセスできない仕組みとしている。
その他の措置の内容	<p><国保総合PCにおける措置></p> <ul style="list-style-type: none"> ・市区町村の職員等が不正にデータ抽出等できないように、GUIによるデータ抽出機能(*)は国保総合PCに搭載しないことにより、個人番号利用事務以外でデータが抽出等されることはなく、事務に必要な情報との紐付けが行われるリスクを軽減している。 *:ここでいうGUIによるデータ抽出機能とは、国民健康保険関係情報ファイルのデータベースからデータを抽出するにあたって、抽出条件等を端末の画面上から簡単なマウス操作等で指定でき、CSV等のデータ形式で国保総合PC上のハードディスク等にファイルを出力する機能のことを指す。
リスクへの対策は十分か	<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>
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	<p>[行っている]</p> <p><選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<ul style="list-style-type: none"> ・国民健康保険システムへのアクセスは、共通基盤の認証が必要である。 ・国民健康保険システムには、申請に基づき登録したユーザIDのみがアクセスでき、ユーザIDごとに業務に必要な機能のみに権限を付与している。 ・退職、人事異動等によりシステムを利用しなくなる場合、人事情報に基づき、ユーザIDを削除している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・システムを利用する必要がある職員に対し、個人ごとにユーザIDを割り当て、ICカード及びパスワードによる認証を行っている。 <p><国保総合PCにおける措置></p> <ul style="list-style-type: none"> ・国保総合PCを利用する必要がある事務取扱担当者特定し、個人ごとにユーザIDを割り当てるとともに、パスワードによるユーザ認証を実施している。 ・なりすましによる不正を防止する観点から、共用IDの発行は禁止している。 ・国保総合PCにおいて対象者の検索や検索結果を表示する画面には、個人番号を表示しないことにより、特定個人情報不正に使用されることリスクを軽減している。 ・情報セキュリティ研修等による周知・啓発、情報セキュリティの自己点検を定期的に行うことにより、ログインしたまま端末を放置せず、離席時にはログアウトすることやログインID、パスワードの使いまわしをしないことを徹底している。 ・パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する。
アクセス権限の発効・失効の管理	<p>[行っている]</p> <p><選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<ol style="list-style-type: none"> 1. 発効の管理 <ul style="list-style-type: none"> ・正規職員、非正規職員ともに、システム利用者申請書に基づき、アクセス権限を設定している。 2. 失効の管理 <ul style="list-style-type: none"> ・正規職員については、退職・人事異動等の人事情報に基づき、アクセス権限を失効させている。 ・非正規職員については、システム利用者申請書に記載された雇用期間に基づき、アクセス権限を失効させている。 <p><共通基盤における措置></p> <ol style="list-style-type: none"> 1. 発効管理

	具体的な管理方法	<ul style="list-style-type: none"> ・人事異動等により、ユーザIDの登録が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書を共通基盤管理者に提出し、承認を得る。 ・共通基盤管理者はユーザID申請書に基づき、ユーザIDの割り当て及びICカードの発行を行う。 <p>2. 失効管理</p> <ul style="list-style-type: none"> ・人事異動等により、ユーザIDの削除が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書及びICカードを共通基盤管理者に提出し、承認を得る。 ・共通基盤管理者はユーザID申請書に基づき、ユーザIDの削除を行う。 <p><国保総合PCにおける措置></p> <p>1. 発効管理</p> <ul style="list-style-type: none"> ・国保総合PCを利用する必要がある事務取扱担当者を特定し、個人ごとにユーザIDを発行し、その職員の業務の範囲に応じたアクセス権限を付与する。 <p>2. 失効管理</p> <ul style="list-style-type: none"> ・人事異動等権限が不要となった場合は、速やかに不要となったIDや権限を失効させる。
アクセス権限の管理	[行っている]	<p style="text-align: right;"><選択肢></p> <p style="text-align: center;">1) 行っている 2) 行っていない</p> <ul style="list-style-type: none"> ・課又は係ごとに業務で使用する機能をあらかじめ設定し、その機能に限るよう権限設定を行っている。 ・アクセス権限を有する全職員について、権限設定に誤りがないか年1回確認を行う。 <p><共通基盤における措置></p> <p>1. ICカード管理台帳を作成し、ユーザIDごとのシステム利用権限を管理している。</p> <p>2. ユーザIDの登録、変更、削除に関する記録を10年間保管することとしている。</p> <p><国保総合PCにおける措置></p> <p>ユーザIDやアクセス権限を人事異動時などに確認し、不要なIDやアクセス権限は削除する。また、アクセス権限を有する全職員について、権限設定に誤りがないか年1回確認を行う。</p>
	具体的な管理方法	<ul style="list-style-type: none"> ・課又は係ごとに業務で使用する機能をあらかじめ設定し、その機能に限るよう権限設定を行っている。 ・アクセス権限を有する全職員について、権限設定に誤りがないか年1回確認を行う。 <p><共通基盤における措置></p> <p>1. ICカード管理台帳を作成し、ユーザIDごとのシステム利用権限を管理している。</p> <p>2. ユーザIDの登録、変更、削除に関する記録を10年間保管することとしている。</p> <p><国保総合PCにおける措置></p> <p>ユーザIDやアクセス権限を人事異動時などに確認し、不要なIDやアクセス権限は削除する。また、アクセス権限を有する全職員について、権限設定に誤りがないか年1回確認を行う。</p>
特定個人情報の使用の記録	[記録を残している]	<p style="text-align: right;"><選択肢></p> <p style="text-align: center;">1) 記録を残している 2) 記録を残していない</p> <p>システムのアクセスログ管理機能により、利用者、日時、利用端末、利用情報等の情報を記録している。</p> <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤の利用に係る操作記録(ログ)では、利用者、日時、利用端末等を記録している。 ・操作記録(ログ)は、10年間保存することとしている。 <p><国保総合PCにおける措置></p> <ul style="list-style-type: none"> ・国保総合PCへのログイン時の認証の他に、ログインを実施した職員等・時刻・操作内容を記録している。 ・情報システム管理者は年1回又はセキュリティ上の問題が発生した際に、記録の内容と関連する書面の記録を照合して確認し、不正な運用が行われていないかを監査する。 ・当該記録については、一定期間保存することとしている。
その他の措置の内容	-	
リスクへの対策は十分か	[十分である]	<p style="text-align: right;"><選択肢></p> <p style="text-align: center;">1) 特に力を入れている 2) 十分である</p> <p style="text-align: center;">3) 課題が残されている</p>
リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容		<ul style="list-style-type: none"> ・外部機関とデータ連携を行う部署以外の業務端末について、電子記録媒体にデータを記録することができない設定としている。 ・EUC機能について、操作ログを取得することにより、不正なデータの抽出・複製を抑制している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・データのバックアップは自動的に実行され、バックアップファイルの取得は入退室管理が行われるデータセンターにおいてのみ可能となっている。 <p><国保総合PCにおける措置></p> <ul style="list-style-type: none"> ・市区町村の職員等が不正にデータ抽出等できないように、GUIによるデータ抽出機能(*)は国保総合PCに搭載しないことにより、個人番号利用事務以外でデータが抽出等されることはない。 ・国保総合PCへのログイン時の認証の他に、ログインを実施した職員等・時刻・操作内容が記録され、国保連合会においても定期的又はセキュリティ上の問題が発生した際に、記録の内容を確認し、不正な運用が行われていないかを監査される。 <p>* :ここでいうGUIによるデータ抽出機能とは、国民健康保険関係情報ファイルのデータベースからデータを抽出するにあたって、抽出条件等を端末の画面上から簡単なマウス操作等で指定でき、CSV等のデータ形式で国保総合PC上のハードディスク等にファイルを出力する機能のことを指す。</p> <ul style="list-style-type: none"> ・国保総合PCと本市の国民健康保険システムとの間の情報の授受において使用する電子記録媒体に

	<p>ついては、次の措置を講じる。</p> <ul style="list-style-type: none"> ・電子記録媒体は記録された情報を暗号化する機能を有しているものに限定する。 ・電子記録媒体は、権限を付与された最小限の職員だけが取り扱うように限定する。 ・電子記録媒体は媒体管理簿で管理し、保管庫に施錠保管する。 ・電子記録媒体に保存する情報については、作業が終わる都度、速やかに情報を消去する。 ・保管する必要がない使用済の電子記録媒体は、物理的破壊等の復元防止措置を行い破棄する。 ・情報システム管理者は月次レベルで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。
リスクへの対策は十分か	<p>[十分である]</p> <p><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4: 特定個人情報ファイルが不正に複製されるリスク	
リスクに対する措置の内容	<ul style="list-style-type: none"> ・外部機関とデータ連携を行う部署以外の業務端末について、電子記録媒体にデータを記録することができない設定としている。 ・EUC機能について、操作ログを取得することにより、不正なデータの抽出・複製を抑制している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・データのバックアップは自動的に実行され、バックアップファイルの取得は入退室管理が行われるデータセンターにおいてのみ可能となっている。 <p><国保総合PCにおける措置></p> <ul style="list-style-type: none"> ・市区町村の職員等が不正にデータ抽出等できないように、GUIによるデータ抽出機能(*)は国保総合PCに搭載しないことにより、個人番号利用事務以外でデータが抽出等されることはない。 ・国保総合PCへのログイン時の認証の他に、ログインを実施した職員等・時刻・操作内容が記録され、国保連合会においても定期的又はセキュリティ上の問題が発生した際に、記録の内容を確認し、不正な運用が行われていないかが監査される。 <p>* :ここでいうGUIによるデータ抽出機能とは、国民健康保険関係情報ファイルのデータベースからデータを抽出するにあたって、抽出条件等を端末の画面上から簡単なマウス操作等で指定でき、CSV等のデータ形式で国保総合PC上のハードディスク等にファイルを出力する機能のことを指す。</p> <ul style="list-style-type: none"> ・国保総合PCと本市の国民健康保険システムとの間の情報の授受において使用する電子記録媒体については、次の措置を講じる。 ・電子記録媒体は記録された情報を暗号化する機能を有しているものに限定する。 ・電子記録媒体は、権限を付与された最小限の職員だけが取り扱うように限定する。 ・電子記録媒体は媒体管理簿で管理し、保管庫に施錠保管する。 ・電子記録媒体に保存する情報については、作業が終わる都度、速やかに情報を消去する。 ・保管する必要がない使用済の電子記録媒体は、物理的破壊等の復元防止措置を行い破棄する。 ・情報システム管理者は月次レベルで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。
リスクへの対策は十分か	<p>[十分である]</p> <p><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>
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>特定個人情報を含む届出書等の紙媒体が不正に使用されるリスクに対しては、執務室を関係者以外立入禁止としており、また特定個人情報を含む紙媒体は鍵付保管庫等で保管している。</p>	

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
<p>委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク</p>		
<p>情報保護管理体制の確認</p>	<ul style="list-style-type: none"> ・契約時に受託者が情報セキュリティ関連資格(プライバシーマーク認定、ISO27001認証、ISO9001認証)を取得しているか確認している。 ・契約書に基づき、業務の推進体制及び情報セキュリティ対策等を記載した実施計画書を提出させ、確認している。 ・情報資産の取扱いを徹底させるため、代表者及び従業員から誓約書を提出させている。 <p><市区町村保険者事務共同処理業務>及び<医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務> 本市の情報セキュリティ対策基準に基づき、委託先において個人情報が適正に管理されているかどうかを以下の観点で確認する。</p> <ul style="list-style-type: none"> ・個人情報の管理的な保護措置(個人情報取扱規定、体制の整備等) ・個人情報の物理的保護措置(人的安全管理、施設および設備の整備、データ管理、バックアップ等) ・個人情報の技術的保護措置(アクセス制御、アクセス監視やアクセス記録等) ・委託内容に応じた情報セキュリティ対策が確保されること ・プライバシーマーク、ISO27001、情報セキュリティマネジメントシステムの国際規格の認証取得情報 	
<p>特定個人情報ファイルの閲覧者・更新者の制限</p>	<p>[制限している] <選択肢> 1) 制限している 2) 制限していない</p>	
<p>具体的な制限方法</p>	<ul style="list-style-type: none"> ・委託契約書により守秘義務を課しているほか、別記「個人情報取扱特記事項」に個人情報の適切な取扱いについて明記している。 ・あらかじめ、実施計画書により本業務の現場責任者及び受持者を報告させている。 ・特定個人情報ファイルへアクセスを行う場合は、許可した者のみがアクセスできるよう権限設定を行っている。 <p><市区町村保険者事務共同処理業務> ・本市の情報セキュリティ対策基準に基づき、委託契約書には「委託先の責任者、委託内容、作業者、作業場所の特定」を明記することとしている。</p> <ul style="list-style-type: none"> ・また、アクセス権限を付与する従業員数を必要最小限に制限し、付与するアクセス権限も必要最小限とすることを委託事業者に遵守させることとしている。 ・さらに、委託事務の定期報告および緊急時報告義務を委託契約書に明記し、アクセス権限の管理状況を年1回報告させることとしている。 <p><医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務> ・取りまとめ機関の職員に許可された業務メニューのみ表示するよう医療保険者等向け中間サーバー等で制御している。</p> <ul style="list-style-type: none"> ・運用管理要領等にアクセス権限と事務の対応表を規定し、職員と臨時職員、取りまとめ機関と委託事業者の所属の別等により、実施できる事務の範囲を限定している。 ・アクセス権限と事務の対応表は随時見直しを行う。 ・パスワードは、規則性のある文字列や単語は使わず、推測されにくいものを使用する。 <p><国保総合(国保集約)システムのクラウド移行作業時に関する措置> ・データ抽出・テストデータ生成及びデータ投入に関する作業者には、委託先の責任者が特定個人情報ファイルの取扱権限を持つIDを発効するが、当該IDの権限及び数は必要最小限とし、作業者は範囲を超えた操作が行えないよう系統的に制御することを委託先に遵守させることとしている。</p> <ul style="list-style-type: none"> ・移行作業終了の際には、委託先の責任者が迅速にアクセス権限を更新し、当該IDを失効させることを委託先に遵守させることとしている。 	
<p>特定個人情報ファイルの取扱いの記録</p>	<p>[記録を残している] <選択肢> 1) 記録を残している 2) 記録を残していない</p>	
<p>具体的な記録方法</p>	<ul style="list-style-type: none"> ・特定個人情報ファイルのアクセスについて、委託先及び再委託先の従業員のアクセスログを記録している。 ・システム以外で特定個人情報ファイルを取り扱う場合、委託先から委託先及び再委託先の作業者、作業内容等を記載した作業記録を提出させる。 <p><共通基盤における措置> ・委託先及び再委託先の従業員の共通基盤に係る操作記録(ログ)を取得し、保存している。</p> <ul style="list-style-type: none"> ・操作記録(ログ)には、操作日時、操作端末のIPアドレス、ユーザID、画面ID、個人番号等を記録している。 ・操作記録(ログ)はそれぞれ、10年間保存することとしている。 <p><市区町村保険者事務共同処理業務></p>	

	<p>具体的な方法</p>	<ul style="list-style-type: none"> ・委託先の従業員等が本市の国民健康保険に関する被保険者等の個人番号を閲覧等した場合には、国保連合会の国保総合(国保集約)システムにおいて、特定個人情報にアクセスした従業員等・時刻・操作内容を記録し、当該記録は一定期間保存することとしている。 ・国保連合会では、年1回またはセキュリティ上の問題が発生した際に当該記録を確認し、不正な運用が行われていないかを点検する。 ・本市の情報セキュリティ管理者は、委託契約に基づき、委託先に当該記録の開示を請求し、調査することで操作個人を特定する。 <p><医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務></p> <ul style="list-style-type: none"> ・操作ログを中間サーバーで記録している。 ・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。 <p><国保総合(国保集約)システムのクラウド移行作業時に関する措置></p> <ul style="list-style-type: none"> ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録することを委託先に遵守させることとしている。 ・移行作業にあたって、作業員以外を対象ファイルにアクセスできないようにし、リスク範囲を限定することを委託先に遵守させることとしている。 ・移行以外の目的・用途でファイルを作成しないよう、委託先に対して周知徹底を行うとともに、作業時にチェックリストなどを用いて不必要な複製がされていないか記録を残すことを委託先に遵守させることとしている。 ・特定個人情報ファイルにアクセスする移行作業は二人で行う相互牽制の体制で実施することを委託先に遵守させることとしている。 ・移行作業に関しては定期的にログをチェックし、データ抽出等の不正な持ち出しが
<p>特定個人情報の提供ルール</p>	<p>委託先から他者への提供に関するルールの内容及びルール遵守の確認方法</p>	<p>[定めている] <選択肢> 1) 定めている 2) 定めていない</p> <ul style="list-style-type: none"> ・契約書において、個人情報の取扱いを第三者に行わせる場合は、本市の承諾を必要としており、委託先の申請に基づき、再委託の必要性、再委託先の情報管理体制を確認した上で、再委託を承諾している。 ・個人情報を取扱う作業場所は、市が指定する場所のみとしている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、事前に作業申請書による報告を求め、必要に応じて立入検査の実施をする。 <p><市区町村保険者事務共同処理業務></p> <ul style="list-style-type: none"> ・本市の情報セキュリティ対策基準に基づき、委託先は、特定個人情報の目的外利用および第三者に提供してはならないこと、特定個人情報の複写、複製、またはこれらに類する行為をすることはできないことなどについて委託契約書に明記することとしている。 ・さらに、本市の情報セキュリティ管理者が委託契約の監査・調査事項に基づき、必要があるときは委託先に対して調査を行い、または報告を求める。 <p><医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務></p> <ul style="list-style-type: none"> ・契約書において本市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ち出しが行われていないか監査する。 <p><市区町村保険者事務共同処理業務></p> <ul style="list-style-type: none"> ・本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項における個人情報の適正な取扱いを義務づけるとともに、従業員から誓約書を提出させている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査の実施をする。 <p><市区町村保険者事務共同処理業務></p> <ul style="list-style-type: none"> ・本市の情報セキュリティ対策基準に基づき、委託契約書において、委託業務の定期報告および緊急時報告を義務付けし、特定個人情報の取扱いに関して定期的に委託先から書面にて報告を受けることとしている。 ・本市から国保連合会への特定個人情報の送付に関しては、国保総合PCで送付を行った際に送付記録を帳簿に記入している。 ・記録は、一定期間保存する。 ・特定個人情報等の貸与に関しては、外部提供する場合に必要なに応じてパスワードの設定を行うこと、および管理者の許可を得ることを遵守するとともに、委託終了時の返還・廃棄について委託契約書に明記することとしている。 ・さらに、本市の情報セキュリティ管理者が委託契約の調査事項に基づき、必要があるときは調査を行い、または報告を求める。 <p><医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務></p> <ul style="list-style-type: none"> ・提供情報は、業務委託完了時にすべて返却又は消去する。 ・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ち出しが行われていないか監査する。
<p>特定個人情報の消去ルール</p>		<p>[定めている] <選択肢> 1) 定めている 2) 定めていない</p>

	<p>ルール内容及び ルール遵守の確認方法</p>	<p>・契約書において、委託先は、個人情報記録された資料等を契約の終了後又は解除後、直ちに本市に返還しなければならないこととされている。</p> <p>・ハードディスク等の記録装置に保存された特定個人情報については、委託業者が記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。</p> <p>・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査を実施する。</p> <p>・記録装置に保存された特定個人情報の消去については、本市に対し、作業完了報告を実施させることとしている。</p> <p><市区町村保険者事務共同処理業務>及び<医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務></p> <p>・特定個人情報等は、業務完了後は速やかに返還し、または漏えいを起こさない方法によって確実に消去、または処分することを、本市の情報セキュリティ対策基準に基づき、委託契約書に明記することとしている。</p> <p>・委託契約終了後は、委託先から特定個人情報等の消去・廃棄等に関する報告書を提出させ、本市の情報システム管理者が消去および廃棄状況の確認を行う。</p> <p><クラウド移行作業時に関する措置></p> <p>・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録することを委託先に遵守させることとしている。</p>
<p>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</p>	<p>規定の内容</p>	<p>[定めている] <選択肢> 1) 定めている 2) 定めていない</p> <p>秘密保持、収集の制限、目的外の利用及び提供の制限、適正管理、作業場所の指定、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。</p> <p><市区町村保険者事務共同処理業務>及び<医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務></p> <p>・秘密保持義務</p> <p>・事業所内からの特定個人情報の持出しの禁止</p> <p>・特定個人情報の目的外利用の禁止</p> <p>・漏えい事案等が発生した場合の再委託先の責任の明確化</p> <p>・委託契約終了後の特定個人情報の返却または廃棄</p> <p>・従業者に対する監督・教育</p> <p>・契約内容の遵守状況について報告を求める規定</p> <p>等を定めるとともに、委託先が本市と同等の安全管理措置を講じていることを確認する。</p>
<p>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確保</p>		<p>[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</p> <p>契約書において、再委託を行う場合にはあらかじめ本市の承諾を得ることとしており、本市が承諾するに当たっては、再委託の必要性、再委託先の情報管理体制などを確認の上、承諾することとしている。</p> <p><市区町村保険者事務共同処理業務></p> <p>再委託を行う場合は、再委託契約に次の事項を盛り込むこととする。</p> <p>・秘密保持義務</p> <p>・事業所内からの特定個人情報の持出しの禁止</p> <p>・特定個人情報の目的外利用の禁止</p> <p>・漏えい事案等が発生した場合の再委託先の責任の明確化</p> <p>・再委託契約終了後の特定個人情報の返却または廃棄</p> <p>・従業者に対する監督・教育</p> <p>・契約内容の遵守状況について報告を求める規定 等</p> <p>また、再委託先が本市と同等の安全管理措置を講じていることを確認する。</p> <p>・国保総合(国保集約)システムを、クラウド事業者が保有・管理する環境に設置する場合、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ことになるため、クラウド事業者は、次を満たすものとする。</p> <p>・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること</p> <p>・セキュリティ管理策が適切に実施されていることが確認できること</p> <p>・日本国内でのデータ保管を条件としていること</p> <p>・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等</p>

	<p>具体的な方法</p>	<ul style="list-style-type: none"> ・上記のほか、「政府情報システムにおけるソフトウェアへの利用に係る基本方針」等による各種条件を満たしていること。 ・クラウド事業者が提供するクラウドサービスは、政府情報システムのためのセキュリティ評価制度 (ISMAP) に基づくクラウドサービスリストに掲載されているものとする。 <p>・国保総合(国保集約)システムを、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上および運用上のセキュリティ(OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化etc)をどのように確保したかを書面にて示した上で、許諾を得ること。</p> <p><医療保険者等向け中間サーバー等における資格履歴管理事務及び機関別符号取得等事務> 医療保険者等向け中間サーバー等の運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、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ことになるため、クラウド事業者は、次を満たすものとする。</p> <ul style="list-style-type: none"> ・ISO/IEC27017又はCSマーク・ゴールドの認証及びISO/IEC27018の認証を取得していること ・セキュリティ管理策が適切に実施されていることが確認できること ・日本国内でのデータ保管を条件としていること ・上記のほか、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たしていること。 <p>運用支援環境を、クラウド事業者が保有・管理する環境に設置する場合、開発者および運用者は、クラウド事業者が提示する責任共有モデルを理解し、OSから上のレイヤーに対して、システム構築上および運用上のセキュリティ(OSやミドルウェアの脆弱性対応、適切なネットワーク設定、アプリケーション対応、データ暗号化etc)をどのように確保したかを書面にて示した上で、許諾を得ること。</p> <p><国保総合(国保集約)システムのクラウド移行作業時に関する措置></p> <ul style="list-style-type: none"> ・データ抽出・テストデータ生成及びデータ投入に関する作業には、委託先の責任者が特定個人情報ファイルの取扱権限を持つIDを発効するが、当該IDの権限及び数は必要最小限とし、作業者は範囲を超えた操作が行えないよう系統的に制御することを委託先に遵守させることとしている。 ・移行作業終了の際には、委託先の責任者が迅速にアクセス権限を更新し、当該IDを失効させることを委託先に遵守させることとしている。 ・移行作業に用いる電子記録媒体に格納したファイルは暗号化し、追記できない状態とし、作業終了後は、不正使用がないことを確認した上で破棄し、破棄日時・破棄方法を記録することを委託先に遵守させることとしている。 ・移行以外の目的・用途でファイルを作成しないよう、委託先に対して周知徹底を行うとともに、作業時にチェックリストなどを用いて不必要な複製がされていないか記録を残すことを委託先に遵守させることとしている。 ・特定個人情報ファイルにアクセスする移行作業は二人で行う相互牽制の体制で実施することを委託先に遵守させることとしている。 ・移行作業に関しては定期的にログをチェックし、データ抽出等の不正な持ち出しが行われていないか監視することを委託先に遵守させることとしている。
<p>その他の措置の内容</p>	<p>—</p>	
<p>リスクへの対策は十分か</p>	<p>[十分である]</p>	<p><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>
<p>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</p>		
<p><国保連合会における措置></p> <ul style="list-style-type: none"> ・国保総合(国保集約)システム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、国保総合(国保集約)システム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。 ・国保総合(国保集約)システムではUTM(コンピュータウイルスやハッキング等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、侵入検知および侵入防止を行うとともに、ログの解析を行う。 ・国保総合(国保集約)システムでは、ウイルス対策ソフトウェアを導入し、パターンファイルの更新を行う。 ・導入しているOSおよ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。 ・国保総合(国保集約)システムサーバー等をデータセンターに設置し、入退室記録管理、監視カメラによる監視および施錠管理を行う。 ・特定個人情報等を取扱う機器、電子媒体および書類等の盗難または紛失等を防止するために、物理的な安全管理措置を講ずる。 ・国保総合(国保集約)システムを使用して特定個人情報ファイルの複製等の操作が可能な職員を最小限に限定する。 ・特定個人情報ファイルを電子記録媒体に複製する際には、不必要な複製を制限するため、事前に管理者の承認を得る。 ・許可された電子記録媒体または機器等以外のものについて使用の制限等の必要な措置を講ずる。また、記録機能を有する機器の情報システム端末等への接続の制限等の必要な措置を講ずる。 ・電子記録媒体は、媒体管理簿で管理し、保管庫に施錠保管する。電子記録媒体に保存する情報については、作業が終わる都度、速やかに情報を消去する。保管する必要がない使用済の電子記録媒体は、物理的破壊等の復元防止措置を行い破棄する。 <p><取りまとめ機関における措置></p> <ul style="list-style-type: none"> ・支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した 		

資格情報等を基に、資格履歴ファイルに格納する業務」及び「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」のうち「機関別符号取得業務」、「情報提供業務(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)」の特定個人情報保護評価を実施している。

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1: 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	<p>・特定個人情報の提供・移転を行う場合は、実施日時、提供・移転の内容等を記録している。</p> <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤に係る操作記録(ログ)については、日時、連携ID、移転・提供元システム名、移転・提供先システム名等を記録している。 ・操作記録(ログ)はそれぞれ、10年間保存することとしている。 	
特定個人情報の提供・移転に関するルール	[定めている]	<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	<p>・特定個人情報の提供・移転の際は、提供・移転先から申請書を提出させ、根拠法令や特定個人情報の内容等の申請内容を精査し、必要な情報のみを提供・移転している。</p> <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・ルールの内容 <ul style="list-style-type: none"> ・共通基盤を利用して別の事務で使用しているシステムに特定個人情報を提供・移転する場合には、情報を保有している事務と情報を必要としている事務との間で事前に協議を行った上で、共通基盤担当に申請書を提出する手順となっている。申請書が提出されない場合、共通基盤を利用した提供・移転はできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤の運用管理機能で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了時の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。 ・ルール遵守の確認方法 <ul style="list-style-type: none"> ・共通基盤担当者が、申請書及び共通基盤の設定の突き合わせを行い、申請書に記載された連携仕様とおりの社内連携が行われているかどうか、申請書に記載されたとおりの電子記録媒体使用許可の制御が行われているかどうか確認する。また、当該申請をした業務システムの担当者においても、システムの端末を操作して、申請内容が実行されているか確認する。 ・共通基盤により、業務システム端末の運用状況を監視しており、許可されていない電子記録媒体が接続された場合には、監視画面に警告が表示されるとともに、当該端末、ユーザ等を記録した操作記録(ログ)が取得・保存される。 	
その他の措置の内容	—	
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
リスク2: 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	<p>提供・移転の承認をしたものについては、承認の条件として、あらかじめ定めた方法(共通基盤連携、媒体連携)でのみ提供・移転を行っている。</p> <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤を利用して別の事務で使用しているシステムに特定個人情報を提供・移転する場合には、情報を保有している事務と情報を必要としている事務との間で合意が行われていることを必須条件としている。 ・情報を保有している事務と情報を必要としている事務双方から共通基盤の利用に係る申請書を提出させ、内容に相違がないか確認した上で設定を行っている。 	
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
リスク3: 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク		

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

<p>リスクに対する措置の内容</p>	<p>・国民健康保険システムにおける権限設定により、情報提供ネットワークへ情報照会の権限が与えられた者のみが情報照会を行う。 ・情報照会のログを取得し、不適切な情報照会を抑止する。</p> <p><共通基盤における措置> ・共通基盤を利用して、中間サーバーを経由し、情報提供ネットワークシステムに情報照会を行う場合には、中間サーバー及び情報提供ネットワークシステムとの連携仕様に基づき、自動的に情報照会が行われる仕組みとなっており、目的外の情報を入手することはできない。</p> <p><中間サーバー・ソフトウェアにおける措置> ①情報照会機能(※1)により、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(※2)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、番号利用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。 ②中間サーバーの職員認証・権限管理機能(※3)では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、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>(※1)情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 (※2)番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 (※3)中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。</p>
---------------------	---

<p>リスクへの対策は十分か</p>	<p>[十分である]</p> <p style="text-align: right;"> <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: 安全が保たれない方法によって入手が行われるリスク

<p>リスクに対する措置の内容</p>	<p>国民健康保険システムと共通基盤は、閉鎖した基幹業務系ネットワークで接続されており、端末機の接続についてもMACアドレスによる認証等により、不適切な接続を防止している。</p> <p><共通基盤における措置> ・共通基盤を利用して、中間サーバーを経由し、情報提供ネットワークシステムに情報照会を行う場合には、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行っており、特定個人情報の漏えいを防止している。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了時の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。</p> <p><中間サーバー・ソフトウェアにおける措置> ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。</p> <p><中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、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行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。</p>
---------------------	--

	<p>(2) 中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。</p>
リスクへの対策は十分か	<p>[十分である]</p> <p><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3: 入手した特定個人情報 that 不正確であるリスク	
リスクに対する措置の内容	<p>・国民健康保険システムにおける情報照会は、個人番号により共通基盤に対して行う。共通基盤で管理する個人番号に1対1で対応する団体内統合宛名番号により、中間サーバーに照会し、情報を取得することにより、照会対象者に係る正確な特定個人情報を入手する。</p> <p><共通基盤における措置> ・共通基盤を利用して、中間サーバーに保存された情報照会の結果の入手を行う場合には、中間サーバーとの連携仕様にに基づき、自動的に結果の入手が行われる仕組みとなっており、入手の過程で情報の正確性が失われることはない。</p> <p><中間サーバー・ソフトウェアにおける措置> ① 中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。</p>
リスクへの対策は十分か	<p>[十分である]</p> <p><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4: 入手の際に特定個人情報 that 漏えい・紛失するリスク	
リスクに対する措置の内容	<p>国民健康保険システム端末は閉鎖した基幹業務系のネットワークで共通基盤と接続するとともに、MACアドレスによる認証等により、不適切な端末接続による特定個人情報の漏えい・紛失を防止している。</p> <p><共通基盤における措置> ・共通基盤を利用して、中間サーバーを経由し、情報提供ネットワークシステムに情報照会を行う場合には、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行っており、特定個人情報の漏えいを防止している。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了時の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。</p> <p><中間サーバー・ソフトウェアにおける措置> ① 中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している(※)。 ② 既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③ 情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報 that 漏えい・紛失するリスクを軽減している。 ④ 中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、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。 (※) 中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。</p>

	<p><中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、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行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。</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5: 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><共通基盤における措置> ・共通基盤を利用し、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、不正に特定個人情報を登録することはできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了時の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。</p> <p><中間サーバー・ソフトウェアにおける措置> ①情報提供機能(※)により、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、中間サーバーにも格納して、情報提供機能により、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。 ②情報提供機能により、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た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、特定個人情報不正に提供されるリスクに対応している。 ③機微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。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、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。 (※)情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。</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6: 不適切な方法で提供されるリスク	
リスクに対する措置の内容	<p><共通基盤における措置> ・共通基盤を利用し、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、不適切な方法で特定個人情報を登録することはできない。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤の運用管理機能で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了時の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。</p> <p><中間サーバー・ソフトウェアにおける措置> ①セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオ</p>

	<p>ンライン連携を抑止する仕組みになっている。 (※)暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能。</p> <p><中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、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行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスできないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。</p>
<p>リスクへの対策は十分か</p>	<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>
<p>リスク7: 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク</p>	
<p>リスクに対する措置の内容</p>	<p>情報提供は、共通基盤で個人番号に1対1で対応する団体内統合宛名及び符号により行うため、提供対象者に係る正確な特定個人情報を提供することができる。</p> <p><共通基盤における措置> ・共通基盤を利用し、中間サーバーに特定個人情報の副本を登録する場合には、中間サーバーとの連携仕様に基づき、自動的に特定個人情報の副本の登録が行われる仕組みとなっており、誤った情報を中間サーバーに登録することはない。</p> <p><中間サーバー・ソフトウェアにおける措置> ①情報提供機能により、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、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 (※)特定個人情報を副本として保存・管理する機能。</p>
<p>リスクへの対策は十分か</p>	<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>
<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><中間サーバー・ソフトウェアにおける措置> ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、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システム上担保されており、不正な名寄せが行われるリスクに対応している。</p> <p><中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、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行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。</p>	

7. 特定個人情報の保管・消去

リスク1: 特定個人情報の漏えい・滅失・毀損リスク

①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[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

具体的な対策の内容

<広島市における措置>
 ・特定個人情報は本市データセンター内に設置したサーバーのデータベース内に保管する。
 ・データセンターでは、以下の3か所の入口において入退管理を行う。
 1.データセンター入口のセキュリティゲート
 2.サーバー室入口の電子錠
 3.サーバー室内サーバー設置場所入口の電子錠
 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証(指紋)の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて、入室を許可した者に対して個人ごとに貸与している。
 また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること(共連れ)を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。
 ・サーバーは事務で使用するシステムごとのサーバーラック内に設置され、施錠される。サーバーラックは事前にサーバーの使用許可を得た者以外の者が開錠することはできない。
 ・データセンター内(サーバー室内を含む)には監視カメラを設置するほか、24時間365日警備員が常駐し、定期的に巡回を行う。
 ・データセンターから情報記録媒体の持ち出しを行う場合、事前に本市担当職員が押印した情報記録媒体等持出承認書をデータセンターに持参し、退館する際に警備員に提出することとしている。
 ・データセンターから退館する際、警備員による手荷物検査を行い、情報記録媒体等持出承認書に記載のない情報記録媒体を保持していた場合、データセンターからの持ち出しはできない。
 ・特定個人情報を含むサーバー内のデータのバックアップテープはデータセンター内の耐火金庫に保管されるほか、大規模災害時の復旧に備えてデータセンターから300km以上離れた場所に分散保管される。
 ・特定個人情報の消去にあたっては、委託業者がハードディスク等の記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。また、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。
 ・特定個人情報が記録された電子記録媒体及び紙媒体は、鍵付保管庫等で保管している。
 ・特定個人情報を取り扱う事務室等については、部外者の進入を禁止している。
 ・窓口付近に設置する端末機は、通行人等から画面が見えない向きに設置している。

<中間サーバー・プラットフォームにおける措置>
 ①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAL)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。
 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。
 ・日本国内でデータを保管している。

⑥技術的対策	[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
--------	--------------	--

<広島市における措置>
 1. 不正アクセス防止
 ・共通基盤の各種機能の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が特定個人情報にアクセスすることはできない。また、各種機能に係る操作記録(ログ)の取得・保存を行っており、不正使用が認められる場合には、職員の特定が可能であることを周知することで、特定個人情報への不正アクセスの抑止を図っている。
 ・本市の庁内ネットワークは、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行った上で、あらかじめ設定された通信仕様に基づく通信のみ許可する仕組みとすることで、特定個人情報の漏えいを防止している。また、本市の庁内ネットワークは、常時監視を行っており、

て、特定個人情報の漏えいを防止している。また、本市の市内ネットワークは、常時監視を行っており、不正アクセス等の脅威が検知された場合には、監視画面に警告が表示されると共に、脅威の種類、対象端末(又はサーバー、ネットワーク機器)、時間等を記録する操作記録(ログ)が取得・保存される。

2. ウイルス対策

- ・ウイルス対策ソフトを導入し、パターンファイルを常に最新になるよう、日次レベルで更新し、各業務システム及び端末に配信している。
- ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了時の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。
- ・共通基盤により、業務システム端末の運用状況を監視しており、許可されていない電子記録媒体が接続された場合には、監視画面に警告が表示されるとともに、当該端末、ユーザ等を記録した操作記録(ログ)が取得・保存される。

具体的な対策の内容

<中間サーバー・プラットフォームにおける措置>

- ①中間サーバー・プラットフォームでは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。
- ②中間サーバー・プラットフォームでは、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。
- ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。
- ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。
- ⑤中間サーバーのデータベースに保存される特定個人情報、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。
- ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
- ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。

<国保総合(国保集約)システムの保管・消去>

- ・国保総合PCにおける措置
 - ・市区町村と国保総合(国保集約)システムとで情報を連携する場合、国保総合PC上に一時ファイルが作成されるが、ファイル転送の終了後には自動で削除される。
 - ・国保総合PCで使用できる外部媒体は、情報システム管理者が使用許可したもののみを使用可能とする。
 - ・国保総合PCには、ウイルス対策ソフトウェアを導入し、ウイルスパターンファイルは適時更新する。
 - ・不正アクセス防止策として、ファイアウォールを導入している。
 - ・オペレーティングシステム等にはパッチの適用を随時に、できるだけ速やかに実施している。

⑦バックアップ	[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
⑧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
⑨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		
⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	生存者の個人番号と同様の保管、管理を実施している。	
その他の措置の内容		
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

リスク2: 特定個人情報が古い情報のまま保管され続けるリスク	
リスクに対する措置の内容	<p>保有する個人情報については、異動が確認できた場合、随時、最新情報に更新している。</p> <p><国保総合(国保集約)システムの保管・消去></p> <ul style="list-style-type: none"> ・国保総合PCにおける措置 <ul style="list-style-type: none"> ・登録された情報は国保総合PCに保管されるデータはなく、国保総合PCからは、国保総合(国保集約)システムの個人番号(特定個人情報ファイル)を操作することはできないため、特定個人情報が古い情報のまま 保存され続けるリスクはない。
リスクへの対策は十分か	<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3: 特定個人情報が消去されずいつまでも存在するリスク	
消去手順	<p>[定めている] <選択肢></p> <p>1) 定めている 2) 定めていない</p>
手順の内容	<p>保管期間経過後、次の方法により適切に消去する。</p> <ul style="list-style-type: none"> ・特定個人情報が保存された記録媒体に対して委託業者が一定回数以上の無作為な書き込みを行った上で、媒体そのものを物理的に破壊することで当該媒体に記録された特定個人情報を消去し、消去した情報、媒体、日付等を記録する。また、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。 ・届出書等の紙媒体は、広島市文書取扱規程に基づき、溶解処理を行っている。 <p><国保総合(国保集約)システムの保管・消去></p> <ul style="list-style-type: none"> ・国保総合PCにおける措置 <ul style="list-style-type: none"> ・登録された情報は国保総合PCに保管されるデータはなく、国保総合PCからは、国保総合(国保集約)システムの個人番号(特定個人情報ファイル)を操作することはできないため、特定個人情報が消去されずいつまでも存在するリスクはない。
その他の措置の内容	—
リスクへの対策は十分か	<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	
<ul style="list-style-type: none"> ・USBメモリ等の電子記録媒体について、情報セキュリティ実施手順により、責任者、保管方法、利用や情報消去の手続き等の取扱いを定めている。 ・USBメモリ等の電子記録媒体について、未使用時は鍵付保管庫等で保管している。 ・USBメモリ等の電子記録媒体について、廃棄する場合、破砕処理、データ消去ソフトウェアによるデータ消去を行っている。 <p><取りまとめ機関における措置></p> <ul style="list-style-type: none"> ・支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「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」のうち「機関別符号取得業務」、「情報提供業務(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)」の特定個人情報保護評価を実施している。 	

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
2. 滞納情報ファイル	
2. 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。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	<p>・特定個人情報、共通基盤を介して入手しており、届出書等の紙媒体やUSBメモリ等の電子記録媒体では入手していない。</p> <p><共通基盤における措置></p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、当該事務の対象者以外の情報を入手することはできない。</p>
必要な情報以外を入手することを防止するための措置の内容	<p><共通基盤における措置></p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、当該事務に必要な情報以外の情報を入手することはできない。</p>
その他の措置の内容	—
リスクへの対策は十分か	<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>
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	<p>・滞納管理システムの利用は、限られた専用の端末のみで利用でき、あらかじめ承認した利用者・権限の範囲に限っている。</p> <p><共通基盤における措置></p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意が行われていることを必須条件としている。</p> <p>・情報を保有している事務と情報を必要としている事務双方から共通基盤の利用に係る申請書を提出させ、内容に相違がないか確認した上で設定を行っている。</p>
リスクへの対策は十分か	<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>
リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	<p><共通基盤における措置></p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の情報と紐付けられたり、全く別の情報に書き換えられたりすることはない。</p>
個人番号の真正性確認の措置の内容	<p><共通基盤における措置></p> <p>・共通基盤を利用して別の事務で使用しているシステムから特定個人情報を入手する場合には、情報を保有している事務と情報を必要としている事務との間で合意された仕様に基づき、自動的に情報の入手が行われる仕組みとなっており、入手した情報が他人の個人番号と紐付けられたり、全く別の番号に書き換えられたりすることはない。</p>

3. 特定個人情報の使用	
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク	
宛名システム等における措置の内容	<p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤では、それぞれの番号利用事務の対象となる者の個人番号又は団体内統合宛名番号にのみアクセスできるようにアクセス制御を行っており、目的を超えた紐付けは行われない仕組みとなっている。 ・共通基盤の団体内統合宛名機能は、個人番号と団体内統合宛名番号の紐付けを管理する機能であり、事務に必要な情報との紐付けは行われない仕組みとなっている。
事務で使用するその他のシステムにおける措置の内容	<ul style="list-style-type: none"> ・滞納管理システムには、業務に関係のない情報は保持しない。 ・他業務システムから直接アクセスできない仕組みとしている。
その他の措置の内容	—
リスクへの対策は十分か	<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>
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	<p>[行っている]</p> <p><選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<ul style="list-style-type: none"> ・滞納管理システムへのアクセスは、共通基盤の認証が必要である。 ・滞納管理システムには、申請に基づき登録したユーザIDのみがアクセスでき、ユーザIDごとに業務に必要な機能のみに権限を付与している。 ・退職、人事異動等によりシステムを利用しなくなる場合、人事情報に基づき、ユーザIDを削除している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・システムを利用する必要がある職員に対し、個人ごとにユーザIDを割り当て、ICカード及びパスワードによる認証を行っている。
アクセス権限の発効・失効の管理	<p>[行っている]</p> <p><選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<p>1 発効の管理</p> <ul style="list-style-type: none"> ・正規職員、非正規職員ともに、システム利用者申請書に基づき、アクセス権限を設定している。 <p>2 失効の管理</p> <ul style="list-style-type: none"> ・正規職員については、退職・人事異動等の人事情報に基づき、アクセス権限を失効させている。 ・非正規職員については、システム利用者申請書に記載された雇用期間に基づき、アクセス権限を失効させている。 <p><共通基盤における措置></p> <p>1. 発効管理</p> <ul style="list-style-type: none"> ・人事異動等により、ユーザIDの登録が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書を共通基盤管理者に提出し、承認を得る。 ・共通基盤管理者はユーザID申請書に基づき、ユーザIDの割り当て及びICカードの発行を行う。 <p>2. 失効管理</p> <ul style="list-style-type: none"> ・人事異動等により、ユーザIDの削除が必要な場合、業務システムの管理者は、速やかに当該職員について、ユーザID申請書及びICカードを共通基盤管理者に提出し、承認を得る。 ・共通基盤管理者はユーザID申請書に基づき、ユーザIDの削除を行う。
アクセス権限の管理	<p>[行っている]</p> <p><選択肢></p> <p>1) 行っている 2) 行っていない</p>
具体的な管理方法	<ul style="list-style-type: none"> ・課又は係ごとに業務で使用する機能をあらかじめ設定し、その機能に限るよう権限設定を行っている。 ・アクセス権限を有する全職員について、権限設定に誤りがないか年1回確認を行う。 <p><共通基盤における措置></p> <p>1. ICカード管理台帳を作成し、ユーザIDごとのシステム利用権限を管理している。</p> <p>2. ユーザIDの登録、変更、削除に関する記録を10年間保管することとしている。</p>

特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	<p>システムのアクセスログ管理機能により、利用者、日時、利用端末、利用情報等の情報を記録している。</p> <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤の利用に係る操作記録(ログ)では、利用者、日時、利用端末等を記録している。 ・操作記録(ログ)は、10年間保存することとしている。 	
その他の措置の内容	—	
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
リスク3: 従業者が事務外で使用するリスク		
リスクに対する措置の内容	<ul style="list-style-type: none"> ・システム利用者アクセス権限は、業務に必要な機能に限っている。 ・システムのアクセスログ管理機能により、利用者のアクセス情報を管理し、業務外のアクセスを調査できるようにしている。 ・システム利用者への情報セキュリティ研修などを行い、事務外での使用禁止を徹底している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・共通基盤の利用に係る操作記録(ログ)を取得・保存しており、事務外で利用した場合には、その職員を特定可能であることを職員に周知し、事務外での使用の抑止を図っている。 	
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
リスク4: 特定個人情報ファイルが不正に複製されるリスク		
リスクに対する措置の内容	<ul style="list-style-type: none"> ・外部機関とデータ連携を行う部署以外の業務端末について、電子記録媒体にデータを記録することができない設定としている。 ・EUC機能について、操作ログを取得することにより、不正なデータの抽出・複製を抑制している。 <p><共通基盤における措置></p> <ul style="list-style-type: none"> ・データのバックアップは自動的に実行され、バックアップファイルの取得は入退室管理が行われるデータセンターにおいてのみ可能となっている。 	
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		
—		

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない				
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク						
情報保護管理体制の確認	<ul style="list-style-type: none"> ・契約時に受託者が情報セキュリティ関連資格(プライバシーマーク認定、ISO27001認証、ISO9001認証)を取得しているか確認している。 ・契約書に基づき、業務の推進体制及び情報セキュリティ対策等を記載した実施計画書を提出させ、確認している。 ・情報資産の取扱いを徹底させるため、代表者及び従業員から誓約書を提出させている。 					
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	<選択肢> 1) 制限している 2) 制限していない				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; background-color: #ffff00;">具体的な制限方法</td> <td style="background-color: #ffff00;"> <ul style="list-style-type: none"> ・特定個人情報ファイルの取扱者の名簿を提出させている。 ・特定個人情報ファイルへアクセスを行う場合は、許可した者のみがアクセスできるよう権限設定を行っている。 </td> </tr> </table>	具体的な制限方法	<ul style="list-style-type: none"> ・特定個人情報ファイルの取扱者の名簿を提出させている。 ・特定個人情報ファイルへアクセスを行う場合は、許可した者のみがアクセスできるよう権限設定を行っている。 				
具体的な制限方法	<ul style="list-style-type: none"> ・特定個人情報ファイルの取扱者の名簿を提出させている。 ・特定個人情報ファイルへアクセスを行う場合は、許可した者のみがアクセスできるよう権限設定を行っている。 					
特定個人情報ファイルの取扱いの記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; background-color: #ffff00;">具体的な方法</td> <td style="background-color: #ffff00;"> <ul style="list-style-type: none"> ・特定個人情報ファイルのアクセスについて、委託先及び再委託先の従業員のアクセスログを記録している。 ・システム以外で特定個人情報ファイルを取り扱う場合、委託先から委託先及び再委託先の作業員、作業内容等を記載した作業記録を提出させる。 <p style="margin-top: 5px;"><共通基盤における措置></p> <ul style="list-style-type: none"> ・委託先及び再委託先の従業員の共通基盤に係る操作記録(ログ)を取得し、保存している。 ・操作記録(ログ)には、操作日時、操作端末のIPアドレス、ユーザID、画面ID、個人番号等を記録している。 ・操作記録(ログ)はそれぞれ、10年間保存することとしている。 </td> </tr> </table>	具体的な方法	<ul style="list-style-type: none"> ・特定個人情報ファイルのアクセスについて、委託先及び再委託先の従業員のアクセスログを記録している。 ・システム以外で特定個人情報ファイルを取り扱う場合、委託先から委託先及び再委託先の作業員、作業内容等を記載した作業記録を提出させる。 <p style="margin-top: 5px;"><共通基盤における措置></p> <ul style="list-style-type: none"> ・委託先及び再委託先の従業員の共通基盤に係る操作記録(ログ)を取得し、保存している。 ・操作記録(ログ)には、操作日時、操作端末のIPアドレス、ユーザID、画面ID、個人番号等を記録している。 ・操作記録(ログ)はそれぞれ、10年間保存することとしている。 				
具体的な方法	<ul style="list-style-type: none"> ・特定個人情報ファイルのアクセスについて、委託先及び再委託先の従業員のアクセスログを記録している。 ・システム以外で特定個人情報ファイルを取り扱う場合、委託先から委託先及び再委託先の作業員、作業内容等を記載した作業記録を提出させる。 <p style="margin-top: 5px;"><共通基盤における措置></p> <ul style="list-style-type: none"> ・委託先及び再委託先の従業員の共通基盤に係る操作記録(ログ)を取得し、保存している。 ・操作記録(ログ)には、操作日時、操作端末のIPアドレス、ユーザID、画面ID、個人番号等を記録している。 ・操作記録(ログ)はそれぞれ、10年間保存することとしている。 					
特定個人情報の提供ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; background-color: #ffff00;">委託先から他者への提供に関するルールの内容及びルール遵守の確認方法</td> <td style="background-color: #ffff00;"> <ul style="list-style-type: none"> ・契約書において、個人情報の取扱いを第三者に行わせる場合は、本市の承諾を必要としており、委託先の申請に基づき、再委託の必要性、再委託先の情報管理体制を確認した上で、再委託を承諾している。 ・個人情報を取扱う作業場所は、市が指定する場所のみとしている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、事前に作業申請書による報告を求め、必要に応じて立入検査の実施をする。 </td> </tr> <tr> <td style="background-color: #ffff00;">委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法</td> <td style="background-color: #ffff00;"> <ul style="list-style-type: none"> ・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項における個人情報の適正な取扱いを義務づけるとともに、従業員から誓約書を提出させている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査の実施をする。 </td> </tr> </table>	委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・契約書において、個人情報の取扱いを第三者に行わせる場合は、本市の承諾を必要としており、委託先の申請に基づき、再委託の必要性、再委託先の情報管理体制を確認した上で、再委託を承諾している。 ・個人情報を取扱う作業場所は、市が指定する場所のみとしている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、事前に作業申請書による報告を求め、必要に応じて立入検査の実施をする。 	委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項における個人情報の適正な取扱いを義務づけるとともに、従業員から誓約書を提出させている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査の実施をする。 		
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・契約書において、個人情報の取扱いを第三者に行わせる場合は、本市の承諾を必要としており、委託先の申請に基づき、再委託の必要性、再委託先の情報管理体制を確認した上で、再委託を承諾している。 ・個人情報を取扱う作業場所は、市が指定する場所のみとしている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、事前に作業申請書による報告を求め、必要に応じて立入検査の実施をする。 					
委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・契約書において、本市の情報セキュリティポリシーの遵守と個人情報取扱特記事項における個人情報の適正な取扱いを義務づけるとともに、従業員から誓約書を提出させている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査の実施をする。 					
特定個人情報の消去ルール	[定めている]	<選択肢> 1) 定めている 2) 定めていない				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; background-color: #ffff00;">ルールの内容及びルール遵守の確認方法</td> <td style="background-color: #ffff00;"> <ul style="list-style-type: none"> ・契約書において、委託先は、個人情報が記録された資料等を契約の終了後又は解除後、直ちに本市に返還しなければならないこととされている。 ・ハードディスク等の記録装置に保存された特定個人情報については、委託業者が記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査を実施する。 ・記録装置に保存された特定個人情報の消去については、本市に対し、作業完了報告を実施させることとしている。 </td> </tr> </table>	ルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・契約書において、委託先は、個人情報が記録された資料等を契約の終了後又は解除後、直ちに本市に返還しなければならないこととされている。 ・ハードディスク等の記録装置に保存された特定個人情報については、委託業者が記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査を実施する。 ・記録装置に保存された特定個人情報の消去については、本市に対し、作業完了報告を実施させることとしている。 				
ルールの内容及びルール遵守の確認方法	<ul style="list-style-type: none"> ・契約書において、委託先は、個人情報が記録された資料等を契約の終了後又は解除後、直ちに本市に返還しなければならないこととされている。 ・ハードディスク等の記録装置に保存された特定個人情報については、委託業者が記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。 ・契約書に基づき、履行状況を確認するため、委託先に対し、報告を求め、必要に応じて立入検査を実施する。 ・記録装置に保存された特定個人情報の消去については、本市に対し、作業完了報告を実施させることとしている。 					
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				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; background-color: #ffff00;">規定の内容</td> <td style="background-color: #ffff00;"> 秘密保持、収集の制限、目的外の利用及び提供の制限、適正管理、作業場所の指定、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。 </td> </tr> </table>	規定の内容	秘密保持、収集の制限、目的外の利用及び提供の制限、適正管理、作業場所の指定、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。				
規定の内容	秘密保持、収集の制限、目的外の利用及び提供の制限、適正管理、作業場所の指定、複写及び複製の禁止、資料の返還、事故発生時の報告等について規定している。					

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確保	[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	契約書において、再委託を行う場合にはあらかじめ本市の承諾を得ることとしており、本市が承諾するに当たっては、再委託の必要性、再委託先の情報管理体制などを確認の上、承諾することとしている。	
その他の措置の内容	-	
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		
-		

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1: 不正な提供・移転が行われるリスク			
特定個人情報の提供・移転の記録	[]	<選択肢> 1) 記録を残している	2) 記録を残していない
具体的な方法			
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
リスク2: 不適切な方法で提供・移転が行われるリスク			
リスクに対する措置の内容			
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
リスク3: 誤った情報を提供・移転してしまうリスク、誤った相手に提供・移転してしまうリスク			
リスクに対する措置の内容			
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			

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	
7. 特定個人情報の保管・消去	
リスク1: 特定個人情報の漏えい・滅失・毀損リスク	
①NISC政府機関統一基準群	[政府機関ではない] <選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している] <選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している] <選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している] <選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[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
具体的な対策の内容	<p><広島市における措置></p> <ul style="list-style-type: none"> ・特定個人情報は本市データセンター内に設置したサーバーのデータベース内に保管する。 ・データセンターでは、以下の3か所の入口において入退管理を行う。 <ol style="list-style-type: none"> 1.データセンター入口のセキュリティゲート 2.サーバー室入口の電子錠 3.サーバー室内サーバー設置場所入口の電子錠 上記1及び2においては、ICカードでの認証を行い、3においてはICカード、パスワード及び生体認証(指紋)の三要素での認証を行っている。なお、ICカードは、事前に申請を受けて入室を許可した者に対して個人ごとに貸与している。 また、入室を許可されない者が入室を許可された者に追従して不正に侵入すること(共連れ)を防止するため、データセンター入口のセキュリティゲートでは有人監視を実施するほか、重要な区画の入口には監視カメラを設置している。 ・サーバーは事務で使用するシステムごとのサーバーラック内に設置され、施錠される。サーバーラックは事前にサーバーの使用許可を得た者以外の者が開錠することはできない。 ・データセンター内(サーバー室内を含む)には監視カメラを設置するほか、24時間365日警備員が常駐し、定期的に巡回を行う。 ・データセンターから情報記録媒体の持ち出しを行う場合、事前に本市担当職員が押印した情報記録媒体等持出承認書をデータセンターに持参し、退館する際に警備員に提出することとしている。 ・データセンターから退館する際、警備員による手荷物検査を行い、情報記録媒体等持出承認書に記載のない情報記録媒体を保持していた場合、データセンターからの持ち出しはできない。 ・特定個人情報を含むサーバー内のデータのバックアップテープはデータセンター内の耐火金庫に保管されるほか、大規模災害時の復旧に備えてデータセンターから300km以上離れた場所に分散保管される。 ・特定個人情報の消去にあたっては、委託業者がハードディスク等の記録装置に対する一定回数以上の上書き又は物理的な破壊等のデータ消去作業を行った上で廃棄することとしている。また、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。 ・特定個人情報が記録された電子記録媒体及び紙媒体は、鍵付保管庫等で保管する。 ・特定個人情報を取り扱う事務室等については、部外者の進入を禁止している。 ・窓口付近に設置する端末機は、通行人等から画面が見えない向きに設置している。 <p><中間サーバー・プラットフォームにおける措置></p> <p>①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。</p> <ul style="list-style-type: none"> ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。

<p>⑥技術的対策</p> <p>具体的な対策の内容</p>	<p>[十分に行っている]</p> <p><広島市における措置></p> <p>1. 不正アクセス防止</p> <ul style="list-style-type: none"> ・共通基盤の各種機能の利用にあたっては、ICカードによる利用者認証及び権限管理を行っており、あらかじめ登録された職員以外が特定個人情報にアクセスすることはできない。また、各種機能に係る操作記録(ログ)の取得・保存を行っており、不正使用が認められる場合には、職員の特定が可能であることを周知することで、特定個人情報への不正アクセスの抑止を図っている。 ・本市の庁内ネットワークは、本市外部のネットワークからアクセスができない専用回線を用い、通信の暗号化を行った上で、あらかじめ設定された通信仕様に基づく通信のみ許可する仕組みとすることで、特定個人情報の漏えいを防止している。また、本市の庁内ネットワークは、常時監視を行っており、不正アクセス等の脅威が検知された場合には、監視画面に警告が表示されると共に、脅威の種類、対象端末(又はサーバー、ネットワーク機器)、時間等を記録する操作記録(ログ)が取得・保存される。 <p>2. ウイルス対策</p> <ul style="list-style-type: none"> ・ウイルス対策ソフトを導入し、パターンファイルを常に最新になるよう、日次レベルで更新し、各業務システム及び端末に配信している。 ・磁気ディスク、USBメモリ等の電子記録媒体の利用は原則禁止とし、業務システム端末で利用できないよう、共通基盤で制御されている。電子記録媒体の利用は、あらかじめ、利用目的、利用頻度、利用端末等を明らかにした上で、業務主管課長から共通基盤管理責任者である情報システム課長に使用制限の解除を申請し、情報システム課長から共通基盤のシステムエンジニアに制限解除を指示する。共通基盤のシステムエンジニアが制限解除を行った後、業務主管課において、動作確認を行うという手順としている。電子記録媒体利用終了時の利用制限再設定についても、同様の手順としている。また、利用できる電子記録媒体は記録された情報を暗号化する機能を有するものに限定している。 ・共通基盤により、業務システム端末の運用状況を監視しており、許可されていない電子記録媒体が接続された場合には、監視画面に警告が表示されるとともに、当該端末、ユーザ等を記録した操作記録(ログ)が取得・保存される。 <p><中間サーバー・プラットフォームにおける措置></p> <p>①中間サーバー・プラットフォームでは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。</p> <p>②中間サーバー・プラットフォームでは、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。</p> <p>③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。</p> <p>④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。</p> <p>⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。</p> <p>⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。</p> <p>⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。</p> <p><国保総合(国保集約)システムの保管・消去></p> <ul style="list-style-type: none"> ・国保総合PCにおける措置 ・市区町村と国保総合(国保集約)システムとで情報を連携する場合、国保総合PC上に一時ファイルが作成されるが、ファイル転送の終了後には自動で削除される。 ・国保総合PCで使用できる外部媒体は、情報システム管理者が使用許可したもののみを使用可能とする。 ・国保総合PCには、ウイルス対策ソフトウェアを導入し、ウイルスパターンファイルは適時更新する。 ・不正アクセス防止策として、ファイアウォールを導入している。 ・オペレーティングシステム等にはパッチの適用を随時に、できるだけ速やかに実施している。 	<p><選択肢></p> <p>1) 特に力を入れて行っている 2) 十分に行っている</p> <p>3) 十分に行っていない</p>
<p>⑦バックアップ</p>	<p>[十分に行っている]</p>	<p><選択肢></p> <p>1) 特に力を入れて行っている 2) 十分に行っている</p> <p>3) 十分に行っていない</p>
<p>⑧事故発生時手順の策定・周知</p>	<p>[十分に行っている]</p>	<p><選択肢></p> <p>1) 特に力を入れて行っている 2) 十分に行っている</p> <p>3) 十分に行っていない</p>
<p>⑨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</p>	<p>[発生なし]</p>	<p><選択肢></p> <p>1) 発生あり 2) 発生なし</p>
<p>その内容</p>		
<p>再発防止策の内容</p>		

⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	生存者の個人番号と同様の保管、管理を実施している。	
その他の措置の内容		
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
リスク2: 特定個人情報が古い情報のまま保管され続けるリスク		
リスクに対する措置の内容	保有する個人情報については、異動が確認できた場合、随時、最新情報に更新している。	
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
リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	<p>保管期間経過後、次の方法により適切に消去する。</p> <ul style="list-style-type: none"> ・特定個人情報が保存された記録媒体に対して委託業者が一定回数以上の無作為な書き込みを行った上で、媒体そのものを物理的に破壊することで当該媒体に記録された特定個人情報を消去し、消去した情報、媒体、日付等を記録する。また、データ消去証明書の提出を求め、必要に応じて立入検査を実施している。 ・特定個人情報等の重要情報が印刷された紙媒体は、広島市文書取扱規程に基づき、溶解処理を行っている。 	
その他の措置の内容	—	
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		
<ul style="list-style-type: none"> ・USBメモリ等の電子記録媒体について、情報セキュリティ実施手順により、責任者、保管方法、利用や情報消去の手続き等の取扱いを定めている。 ・USBメモリ等の電子記録媒体について、未使用時は鍵付保管庫等で保管している。 ・USBメモリ等の電子記録媒体について、廃棄する場合、破砕処理、データ消去ソフトウェアによるデータ消去を行っている。 		

IV その他のリスク対策 ※

1. 監査	
①自己点検	<p>[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</p> <p>「広島市情報セキュリティポリシー」に、「定期的に又は必要に応じて自己点検を行い、改善の必要があるものについては、速やかに改善措置を行うこと」を定め、毎年1回、情報セキュリティの自己点検を実施することとしている。</p> <p><中間サーバー・プラットフォームにおける措置> 運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、毎年1回、自己点検を実施することとしている。</p>
②監査	<p>[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</p> <p>「広島市情報セキュリティポリシー」に、「定期的に又は必要に応じて情報セキュリティ監査を行い、改善の必要があるものについては、速やかに改善措置を行うこと」を定め、4年に1回、外部監査を実施することとしている。</p> <p><中間サーバー・プラットフォームにおける措置> ①運用規則等に基づき、中間サーバー・プラットフォームについて、毎年1回、監査を行うこととしている。 ②政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。</p> <p><国保総合(国保集約)システムにおける措置> ・番号利用法第29条の3第2項による個人情報保護委員会への特定個人情報ファイルの取扱いの状況に関する報告(それに伴い、国保連合会にも同様の報告を求めることにする)。</p>
2. 従業者に対する教育・啓発	
従業者に対する教育・啓発	<p>[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</p> <p>次に掲げる情報セキュリティ研修・公務員倫理研修を毎年実施し、具体的な情報セキュリティ事故の事例紹介等により、職員の情報セキュリティ意識・法令遵守意識の向上を図っている。 なお、情報セキュリティ研修については、eラーニングを導入し、未受講者に対して催促メールを送信することで受講率の向上を図っている。また、公務員倫理研修(情報セキュリティに関する部分)については、庁内LANの全庁資料室に研修資料を掲載しているため、未受講者がいつでも研修資料を参照できる。</p> <ul style="list-style-type: none"> ・情報セキュリティ研修 <ul style="list-style-type: none"> 新規採用職員研修、一般職員研修、新任課長級職員研修、新任課長補佐級職員研修 ・公務員倫理研修(情報セキュリティに関する部分) <ul style="list-style-type: none"> 全職員研修、所属長研修、所属長による所属内研修 <p><中間サーバー・プラットフォームにおける措置> ・IPA(情報処理推進機構)が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則(接続運用規程等)や情報セキュリティに関する教育を年次(年2回)及び随時(新規要員着任時)実施することとしている。</p> <p><国保総合(国保集約)システムにおける措置> <国保総合(国保集約)システムに関する教育・啓発> ・教育事項: 国保総合(国保集約)システムの操作・運用ならびに個人情報保護に関する教育および研修 ・教育頻度: 年間1回程度 ・教育方法: 集合教育 ・教育対象: 職員および嘱託員 ・違反行為に対する措置: 違反行為を行ったものに対しては、都度指導の上、違反行為の程度によっては懲戒の対象となりうる。 ・委託先である国保連合会に対しては、契約内容において、個人情報保護に関する秘密保持契約を締結している。 ・教育の未受講者に対しては、再受講の機会を付与している。</p>
3. その他のリスク対策	
<p><中間サーバー・プラットフォームにおける措置> 中間サーバー・プラットフォームを活用することにより、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者による高レベルのセキュリティ管理(入退室管理等)、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。</p> <p><取りまとめ機関における措置> 支払基金が「医療保険者等向け中間サーバー等における資格履歴管理事務」のうち「運用支援環境において、委託区画から取得した資格情報等を基に、資格履歴ファイルに格納する業務」及び「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」のうち「機関別符号取得業務」、「情報提供業務(オンライン資格確認等システムで管理している情報と紐付けるために使用する情報の提供)」の特定個人情報保護評価を実施している。</p>	

V 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	広島市公文書館 〒730-0051 広島市中区大手町四丁目1番1号 大手町平和ビル8階 電話番号:082-243-2583(直通)
②請求方法	所定の請求書に必要事項を記載し、前記「①請求先」に提出する。その際、運転免許証など本人であることを確認できる身分証明書等を提示する必要がある。
特記事項	広島市ホームページに請求方法や手数料等について掲載している。
③手数料等	[無料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: 請求そのものや開示の際の閲覧、視聴は無料。写しの交付等は一定の手数料が必要。写しの交付を受ける際に、公文書館に納付する。)
④個人情報ファイル簿の公表	[行っている] <選択肢> 1) 行っている 2) 行っていない
個人情報ファイル名	国民健康保険システム(国民健康保険情報ファイル)
公表場所	広島市公文書館
⑤法令による特別の手続	—
⑥個人情報ファイル簿への不記載等	—
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	広島市健康福祉局保健部保険年金課 〒730-8586 広島市中区国泰寺町一丁目6番34号 電話番号:082-504-2157(直通)
②対応方法	問合せの受付時に受付票を起票し、対応について記録を残す。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和5年8月31日
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 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(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	市ホームページに意見公募する旨を掲載し、評価書(再評価案)の所管課における閲覧及び配布、ホームページへの掲載を行う。意見の提出は、持参、郵送、FAX又は電子メールにより受け付ける。
②実施日・期間	令和5年10月2日から令和5年10月31日
③期間を短縮する特段の理由	—
④主な意見の内容	医療情報の漏えいについて、病状等の医療情報が他人に漏れると、中傷や嫌がらせにつながる可能性があることから、取り扱いには注意が必要である。
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和5年11月7日から令和5年12月8日
②方法	専門性を有する第三者(個人情報の保護及び情報システムに知見を有している者)の意見を聴く。
③結果	
4. 個人情報保護委員会の承認【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

(別添3)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
令和8年3月24日	1 基本情報 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3	①システムの名称 共通基盤(庁内連携システム及び宛名システムに相当)	①システムの名称 共通基盤(庁内連携システム、宛名システム及び申請管理システムに相当)	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	1 基本情報 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3	②システムの機能 1. ポータル機能 ICカードによる利用者認証、権限管理及び業務システムの起動を行う機能。 2. システム間連携制御機能 共通基盤と業務システム間及び異なる業務システム間のデータ連携を行う機能。 3. 運用管理機能 システム監視、稼働記録(ログ)管理、ウイルス対策及びデータのバックアップを行う機能。 4. 団体内統合宛名機能 個人番号と団体内統合宛名番号とを紐付けて管理する機能。団体内統合宛名番号が未登録の個人番号については、新規に団体内統合宛名番号を割り当てる。 5. 中間サーバー連携機能 中間サーバーと共通基盤間のデータ連携を行い、中間サーバーへの情報照会要求の送信及び照会結果の受信並びに特定個人情報の副本の登録を行う機能。	②システムの機能 (※1～5修正なし) 6. ぴったりサービス対応機能 サービス検索・電子申請機能と共通基盤間のデータ連携を行い、サービス検索・電子申請機能への申請データ取得要求及び返信のあった申請データの取得並びに申請データ処理状況の登録を行う。取得した申請データは、「2. システム間連携制御機能」により住民記録システムからマイナンバーカードに搭載されている利用者証明用電子証明書のシリアル番号と住記宛名番号が紐づいた情報を取得し、申請データに含まれるシリアル番号を住記宛名番号へ変換し、住記宛名番号及び団体内統合宛名番号を申請データに紐づけてデータベースに保管するとともに、申請データを業務システムに連携する機能。	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	1 基本情報 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3	[○]その他(中間サーバー、国民健康保険システム、介護保険システム、福祉情報システム、財務会計システム、人事・給与システム)	[○]その他(中間サーバー、国民健康保険システム、介護保険システム、福祉情報システム、財務会計システム、人事・給与システム、サービス検索・電子申請機能)	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	1 基本情報 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8	—	①システムの名称 サービス検索・電子申請機能	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	1 基本情報 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8	—	・【住民向け機能】自らが受けることができるサービスをオンラインで検索及び申請ができる機能 ・【地方公共団体向け機能】住民が電子申請を行った際の申請データ取得画面又は機能を、地方公共団体に公開する機能	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	1 基本情報 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8	—	[○]庁内連携システム [○]宛名システム等	事後	サービス検索・電子申請機能の利用に伴う修正。

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
令和8年3月24日	I 基本情報 5. 個人番号の利用 法律上の根拠	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(以下「番号利用法」という。)第9条第1項、番号利用法別表第一の30の項、番号利用法別表第一の主務省令で定める事務を定める命令第24条、番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条 <オンライン資格確認の準備業務> ・番号利用法 第9条第1項(利用範囲)別表第1 項番30 ・番号利用法別表第1の主務省令で定める事務を定める命令 第24条 ・国民健康保険法 第113条の3 第1項及び第2項	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(以下「番号利用法」という。)第9条第1項、番号利用法別表の44の項、番号利用法別表の主務省令で定める事務を定める命令第24条、番号利用法第9条第2項及び広島市個人番号の利用に関する条例第3条 <オンライン資格確認の準備業務> ・番号利用法 第9条第1項(利用範囲)別表 項番44 ・番号利用法別表の主務省令で定める事務を定める命令 第24条 ・国民健康保険法 第113条の3 第1項及び第2項	事後	改正番号法の施行に伴う修正、重要な変更該当しないため修正により対応。
令和8年3月24日	I 基本情報 6. 情報提供ネットワークシステムによる情報連携 ②法律上の根拠	【情報照会の根拠】 番号利用法第19条第8号 番号利用法別表第二 42の項、43の項、44の項、45の項 番号利用法別表第二の主務省令で定める事務及び情報を定める命令 第25条、第25条の2、第26条 ※番号利用法別表第二 45の項に係る主務省令は未制定。 【情報提供の根拠】 番号利用法第19条第8号 番号利用法別表第二 1の項、2の項、3の項、4の項、5の項、9の項、12の項、15の項、17の項、22の項、26の項、27の項、30の項、33の項、39の項、42の項、46の項、58の項、62の項、78の項、80の項、87の項、88の項、93の項、97の項、106の項、109の項、120の項	【情報照会の根拠】 番号利用法第19条第8号に基づく主務省令第2条の表 69の項、70の項、71の項 番号利用法別表の主務省令で定める事務を定める命令 第24条 【情報提供の根拠】 番号利用法第19条第8号に基づく主務省令第2条の表 2の項、3の項、6の項、13の項、16の項、19の項、27の項、38の項、42の項、48の項、56の項、65の項、69の項、83の項、87の項、111の項、115の項、125の項、131の項、137の項、141の項、145の項、158の項、161の項、164の項、165の項、166の項、173の項	事後	改正番号法の施行に伴う修正、重要な変更該当しないため修正により対応。
令和8年3月24日	I 基本情報 6. 情報提供ネットワークシステムによる情報連携 ②法律上の根拠(続き)	番号利用法別表第二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号、第4号、第5号、第7号、第8号、第10号、第11号、第17号、第3条第4号、第5号、第6号、第8号、第9号、第10号、第11号、第12号、第4条、第5条第3号、第4号、第5号、第6号、第7号、第8号、第9号、第10号、第8条第1号、第2号、第3号、第10条の2第2号、第11条の2第2号、第12条の3第1号、第15条第1号、第19条、第20条第10号、第11号、第22条の2第2号、第3号、第4号、第5号、第6号、第7号、第8号、第24条の2第3号、第4号、第5号、第6号、第9号、第10号、第25条第2号、第3号、第7号、第8号、第31条の2第4号、第5号、第6号、第7号、第10号、第11号、第33条第1号、第41条の2第3号、第43条第2号、第3号、第5号、第7号、第44条、第46条第1項第1号、第3号、第4号、第5号、第6号、第7号、第49条第2号、第53条第1号、第2号、第5号、第55条の2、第59条の3第3号 ※番号利用法別表第二 30の項、46の項、88の項に係る主務省令は未制定。	(上記のとおり)	事後	改正番号法の施行に伴う修正、重要な変更該当しないため修正により対応。
令和8年3月24日	I 基本情報 6. 情報提供ネットワークシステムによる情報連携 ②法律上の根拠(続き)	<オンライン資格確認の準備業務> ・番号利用法 附則第6条第4項 (利用目的:情報連携のためではなくオンライン資格確認の準備として機関別符号を取得する等) ・国民健康保険法 第113条の3 第1項及び第2項	<オンライン資格確認の準備業務> ・番号利用法 附則第6条第4項 (利用目的:情報連携のためではなくオンライン資格確認の準備として機関別符号を取得する等) ・国民健康保険法 第113条の3 第1項及び第2項	事後	改正番号法の施行に伴う修正、重要な変更該当しないため修正により対応。
令和8年3月24日	(別添1)事務の内容	図(省略)	図(省略) ※サービス検索・電子申請の利用に伴う修正。	事後	サービス検索・電子申請機能の利用に伴う修正。

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
令和8年3月24日	(別添1)事務の内容	備考 【被保険者資格管理に関する事務】 ①住民異動による資格取得・喪失、氏名変更、世帯変更等の届出の受理、確認を行う。 ②届出書等に記載された個人番号について、必要に応じて個人番号の真正性の確認を行う。 ③被用者保険等の喪失による資格取得、被用者保険等への加入に伴う資格喪失届の受理、確認を行う。 ④被保険者証、高齢受給者証等の交付申請受理、確認及び交付を行う。 ⑤都道府県単位で資格管理を行うため、被保険者情報の連携を行う。(別紙「1. 資格継続業務」参照)また、オンライン資格確認等システムで被保険者の資格情報を利用するため、国保総合(国保集約)システム経由で、医療保険者等向け中間サーバー等システムの委託区画へ、被保険者異動情報の登録を行う。(別紙「3. オンライン資格確認の準備のための医療保険者等向け中間サーバー等への被保険者異動情報の提供」参照)	備考 【被保険者資格管理に関する事務】 修正なし	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	(別添1)事務の内容(続き)	【保険料賦課管理に関する事務】 ⑥保険料の算定等のための所得(年金情報を含む。)を把握する。 ⑦保険料の賦課を行う。 ⑧保険料の減免の申請受理、決定を行う。 ⑨年金の特別徴収情報を提供する。 【給付管理に関する事務】 ⑩各保険給付の申請受理、確認を行う。 ⑪保険給付申請の内容を審査し、世帯の所得状況に応じた支給を行う。 ⑫高額療養費の高額該当回数の引き継ぎ確認を行う。(別紙「2. 高額該当の引き継ぎ業務」参照) ⑬国保連合会からレセプト情報を受領し、再審査・過誤の確認を行う。	【保険料賦課管理に関する事務】 ⑥保険料の算定等のための所得(年金情報を含む。)を把握する。無所得の申立ては、窓口や郵送での書類の受入のほか、サービス検索・電子申請機能での受領により行う。 ⑦サービス検索・電子申請機能により申請された電子申請データを申請管理システムにより受領 ⑧保険料の賦課を行う。 ⑨保険料の減免の申請受理、決定を行う。 ⑩年金の特別徴収情報を提供する。 【給付管理に関する事務】 ⑪各保険給付の申請受理、確認を行う。 ⑫保険給付申請の内容を審査し、世帯の所得状況に応じた支給を行う。 ⑬高額療養費の高額該当回数の引き継ぎ確認を行う。(別紙「2. 高額該当の引き継ぎ業務」参照) ⑭国保連合会からレセプト情報を受領し、再審査・過誤の確認を行う。	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	(別添1)事務の内容(続き)	【保険料収納管理に関する事務】 ⑭保険料の納付状況について、金融機関等からの領収済通知書等により確認する。 ⑮保険料の過納付や誤納付について、超過額を還付又は充当し、世帯主に通知する。 ⑯保険料を納期限までに完納しない場合は、世帯主に督促状を送付する。 【保険料滞納管理に関する事務】 ⑰督促状を送付後も保険料を完納しない場合は、広島市市税等お知らせセンターから世帯主に電話による納付勧奨等を行う。また、職員による滞納整理を開始する。	【保険料収納管理に関する事務】 ⑮保険料の納付状況について、金融機関等からの領収済通知書等により確認する。 ⑯保険料の過納付や誤納付について、超過額を還付又は充当し、世帯主に通知する。 ⑰保険料を納期限までに完納しない場合は、世帯主に督促状を送付する。 【保険料滞納管理に関する事務】 ⑰督促状を送付後も保険料を完納しない場合は、広島市市税等お知らせセンターから世帯主に電話による納付勧奨等を行う。 また、職員による滞納整理を開始する。	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 2. 基本情報 ④記録される項目 主な記録項目	・連絡先等情報 [○]4情報(氏名、性別、生年月日、住所)	・連絡先等情報 [○]5情報(氏名、氏名の振り仮名、性別、生年月日、住所)	事前	評価書様式の改正に伴う修正

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
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 2. 基本情報 ④記録される項目 その妥当性	1. 識別情報 ・個人番号:対象者を正確に特定するために保有(参照)する。 ・その他識別情報(内部番号):本市において、個人を一意に識別するために独自の識別番号を保有する。 2. 連絡先等情報 ・5情報:被保険者証、保険料の納入通知書等の印字等、事務で必要とする氏名、住所等を管理するために保有する。 ・連絡先:本人への連絡等のため保有する。 ・その他住民票関係情報:世帯主と被保険者の関係を示す続柄等を保有する。	1. 識別情報 ※ 修正なし 2. 連絡先等情報 ・5情報:被保険者証、保険料の納入通知書等の印字等、事務で必要とする氏名、住所等を管理するために保有する。 ・連絡先:本人への連絡等のため保有する。 ・その他住民票関係情報:世帯主と被保険者の関係を示す続柄等を保有する。	事前	評価書様式の改正に伴う修正
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 2. 基本情報 ④記録される項目 その妥当性 (続き)	3. 業務関係情報 ・地方税関係情報:保険料の算定、高額療養費の支給等を行うための所得情報を保有する。 ・医療保険関係情報:本事務を運用するための国民健康保険情報を保有する。 ・生活保護・社会福祉関係情報:市外の施設に入所したが引き続き本市の国民健康保険に加入する住所地特例に係る入所施設等の情報を保有する。 ・介護・高齢者福祉関係情報:高額介護合算療養費の支給を行うための介護保険情報を保有する。 ・雇用・労働関係情報:非自発的失業者に係る雇用保険情報を保有する。 ・年金関係情報:年金から特別徴収により保険料を徴収するための年金関係情報を保有する。	3. 業務関係情報 ※ 修正なし	事前	評価書様式の改正に伴う修正
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 3. 特定個人情報の入手・私用 ②入手方法	[O]その他(市税システム端末の直接操作)	[O]その他(市税システム端末の直接操作。サービス検索・電子申請機能、申請管理システム)	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 3. 特定個人情報の入手・私用 ⑤本人への明示	・本人から入手する情報については、届出書、申請書等の書面で入手しており、使用目的は明確である。 ・関係先から入手する情報については、国民健康保険法第113条の2、番号利用法第9条第1項、第19条第8号、別表第一の30の項、別表第二の42の項、43の項、44の項、45の項及び番号利用法第9条第2項により定める条例に基づいて入手しており、使用目的は明確である。	・本人から入手する情報については、届出、申請等により入手しており、使用目的は明確である。 ・関係先から入手する情報については、国民健康保険法第113条の2、番号利用法第9条第1項、第19条第8号、別表の44の項、番号利用法第19条第8号に基づく主務省令第2条の表の69、70、71の項及び番号利用法第9条第2項により定める条例に基づいて入手しており、使用目的は明確である。	事後	改正番号法の施行に伴う修正、重要な変更に関与しないため修正により対応。
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 3. 特定個人情報の入手・私用 ⑧使用方法	1. 被保険者資格管理事務 ・国民健康保険異動届等により、資格の取得又は喪失に係る情報の管理を行う。 ・資格の取得又は被保険者証等再交付申請書の受理等により、被保険者証の発行等に係る情報の管理を行う。 2. 保険料賦課管理事務 ・所得情報等により保険料の算定を行う。 ・保険料の納入通知書の発行等の情報の管理を行う。 ・保険料減免申請書の受理により、保険料の減免に係る情報の管理を行う。 3. 給付管理事務 ・保険給付に必要な所得区分の判定に係る情報の管理を行う。 ・保険給付に必要なレセプト情報の管理を行う。 ・高額療養費支給申請書等の受理により、保険給付に係る情報の管理を行う。	1. 被保険者資格管理事務 ※ 修正なし 2. 保険料賦課管理事務 ・サービス検索・電子申請機能を通じて申請された電子申請データの受理、審査等を行う。 ・所得情報等により保険料の算定を行う。 ・保険料の納入通知書の発行等の情報の管理を行う。 ・保険料減免申請書の受理により、保険料の減免に係る情報の管理を行う。 3. 給付管理事務 ※ 修正なし	事後	サービス検索・電子申請機能の利用に伴う修正。

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
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 3. 特定個人情報の入手・私用 ⑧使用方法(続き)	4. 保険料収納管理事務 ・領収済通知書の受理により、保険料の収納に係る情報の管理を行う。 ・保険料の過納により、還付又は充当に係る情報の管理を行う。 ・口座振替依頼書の受理により、口座振替に係る情報の管理を行う。 ・保険料の滞納により、督促状の発行に係る情報の管理を行う。	4. 保険料収納管理事務 ※ 修正なし	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 5. 特定個人情報の提供・移転(委託に伴うものを除く。)提供先1	別紙1に掲げる情報照会者(番号利用法第19条第8号別表第二に定める情報照会者)	別紙1に掲げる情報照会者(番号利用法第19条第8号に基づく主務省令第2条の表に定める情報照会者)	事後	改正番号法の施行に伴う修正、重要な変更該当しないため修正により対応。
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 6. 特定個人情報の保管・消去 ①保管場所	<広島市における措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間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。	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間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	中間サーバーの更改に伴い修正
令和8年3月24日	II 特定個人情報ファイルの概要(国民健康保険情報ファイル) 6. 特定個人情報の保管・消去 ③消去方法	<広島市における措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度(ISMAP)に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。	事前	中間サーバーの更改に伴い修正
令和8年3月24日	II 特定個人情報ファイルの概要(滞納情報ファイル) 2. 基本情報 ④記録される項目 主な記録項目	・連絡先等情報 [○]4情報(氏名、性別、生年月日、住所)	・連絡先等情報 [○]5情報(氏名、氏名の振り仮名、性別、生年月日、住所)	事前	評価書様式の改正に伴う修正

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
令和8年3月24日	II 特定個人情報ファイルの概要(滞納情報ファイル) 2. 基本情報 ④記録される項目 その妥当性	1. 識別情報 ・個人番号:対象者を正確に特定するために保有(参照)する。 ・その他識別情報(内部番号):本市において、個人を一意に識別するために独自の識別番号を保有する。 2. 連絡先等情報 ・4情報:保険料の納付催告書の印字等、事務で必要とする氏名、住所等を管理するために保有する。 ・連絡先:本人への連絡等のため保有する。 ・その他住民票関係情報:世帯主と被保険者の関係を示す続柄等を保有する。 3. 業務関係情報 ・医療保険関係情報:本事務を運用するための国民健康保険情報を保有する。	1. 識別情報 ※ 修正なし 2. 連絡先等情報 ・5情報:被保険者証、保険料の納入通知書等の印字等、事務で必要とする氏名、住所等を管理するために保有する。 ・連絡先:本人への連絡等のため保有する。 ・その他住民票関係情報:世帯主と被保険者の関係を示す続柄等を保有する。 3. 業務関係情報 ※ 修正なし	事前	評価書様式の改正に伴う修正
令和8年3月24日	II 特定個人情報ファイルの概要(滞納情報ファイル) 6. 特定個人情報の保管・消去 ①保管場所	<広島市における措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は、サーバー室に設置された中間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。	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間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	中間サーバーの更改に伴い修正
令和8年3月24日	II 特定個人情報ファイルの概要(滞納情報ファイル) 6. 特定個人情報の保管・消去 ③消去方法	<広島市における措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者が特定個人情報を消去することはない。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去する。	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度(ISMAP)に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。	事前	中間サーバーの更改に伴い修正

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
令和8年3月24日	(別添2)ファイル記録項目	<p>【1. 国民健康保険情報ファイル】 ※ 略</p> <p>【統合宛名管理テーブル】 1.個人番号、2.団体内統合宛名番号、3.業務宛名番号、4.住所、5.氏名、6.生年月日、7.性別</p> <p>【2. 滞納情報ファイル】 ※ 略</p>	<p>【1. 国民健康保険情報ファイル】 ※ 修正なし</p> <p>【統合宛名管理テーブル】 1.個人番号、2.団体内統合宛名番号、3.業務宛名番号、4.住所、5.氏名、6.生年月日、7.性別、8.カナ氏名</p> <p>【申請管理テーブル】 1.受付番号、2.氏名、3.生年月日、4.性別、5.住所、6.電話番号、7.メールアドレス、8.手続名称、9.手続コード、10.申請日時、11.ステータスコード、12.ステータス名称、13.業務宛名番号、14.団体内統合宛名番号、15.利用者証明書シリアル番号、16.カナ氏名、17.FAX番号</p> <p>【2. 滞納情報ファイル】 ※ 修正なし</p>	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	<p>Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル)</p> <p>2. 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。)</p> <p>リスク1: 目的外の入手が行われるリスク</p> <p>必要な情報以外を入手することを防止するための措置の内容</p>	<p>・届出書等は、必要とする情報以外が記載できない様式としている。</p> <p>・国民健康保険システムは、必要とする情報以外を登録、管理できない仕様としている。</p> <p><共通基盤における措置> ※ 略</p> <p><国保連合会からの入手における措置> ※ 略</p>	<p>・届出書等は、必要とする情報以外が記載できない様式としている。</p> <p>・国民健康保険システムは、必要とする情報以外を登録、管理できない仕様としている。</p> <p><共通基盤における措置> ※ 修正なし</p> <p><国保連合会からの入手における措置> ※ 修正なし</p> <p><サービス検索・電子申請機能における措置> ・住民がサービス検索・電子申請機能から電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。</p> <p>・住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。</p>	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	<p>Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル)</p> <p>2. 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。)</p> <p>リスク2: 不適切な方法で入手が行われるリスク</p> <p>リスクに対する措置の内容</p>	<p>・届出書等の受理は、あらかじめ決められた窓口限定し、奪取が行えないようにしている。</p> <p>・国民健康保険システムの利用は、限られた専用の端末のみで利用でき、あらかじめ承認した利用者・権限の範囲に限っている。</p> <p><共通基盤における措置> ※ 略</p> <p><国保連合会からの入手における措置> ※ 略</p>	<p>・届出書等の受理は、あらかじめ決められた窓口限定し、奪取が行えないようにしている。</p> <p>・国民健康保険システムの利用は、限られた専用の端末のみで利用でき、あらかじめ承認した利用者・権限の範囲に限っている。</p> <p><共通基盤における措置> ※ 修正なし</p> <p><国保連合会からの入手における措置> ※ 修正なし</p> <p><サービス検索・電子申請機能における措置> サービス検索・電子申請機能の画面の誘導において住民に何の手続を探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものか明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。</p>	事後	サービス検索・電子申請機能の利用に伴う修正。

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
令和8年3月24日	<p>Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル)</p> <p>2. 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。)</p> <p>リスク3: 入手した特定個人情報が入力された本人確認の措置の内容</p>	<p>・届出書等の受理の際、個人番号カード又は通知カード及び顔写真付きの身分証明書の提示を受けて、本人確認を行う。</p> <p>・代理人から届出書等を受理する際は、本人からの委任状の確認及び代理人の本人確認を行う。</p> <p><共通基盤における措置> ※ 略</p> <p><国保連合会からの入手における措置> ※ 略</p>	<p>・届出書等の受理の際、個人番号カード又は通知カード及び顔写真付きの身分証明書の提示を受けて、本人確認を行う。</p> <p>・代理人から届出書等を受理する際は、本人からの委任状の確認及び代理人の本人確認を行う。</p> <p><共通基盤における措置> ※ 修正なし</p> <p><国保連合会からの入手における措置> ※ 修正なし</p> <p><サービス検索・電子申請機能における措置> ・住民がサービス検索・電子申請機能から電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。</p>	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	<p>Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル)</p> <p>2. 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。)</p> <p>リスク4: 入手した特定個人情報が入力された本人確認の措置の内容</p>	<p>・特定個人情報が記載された届出書等は、鍵付保管庫等で保管している。</p> <p>・事務処理で使用した届出書等は、処理完了後は速やかに保管庫に移している。</p> <p>・国民健康保険システムのネットワークは、外部からアクセスできない専用回線を用い、専用の端末のみと接続している。</p> <p><共通基盤における措置> ※ 略</p> <p><国保連合会からの入手における措置> ※ 略</p>	<p>・特定個人情報が記載された届出書等は、鍵付保管庫等で保管している。</p> <p>・事務処理で使用した届出書等は、処理完了後は速やかに保管庫に移している。</p> <p>・国民健康保険システムのネットワークは、外部からアクセスできない専用回線を用い、専用の端末のみと接続している。</p> <p><共通基盤における措置> ※ 修正なし</p> <p><国保連合会からの入手における措置> ※ 修正なし</p> <p><サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。</p>	事後	サービス検索・電子申請機能の利用に伴う修正。
令和8年3月24日	<p>Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル)</p> <p>6. 情報提供ネットワークシステムとの接続</p> <p>リスク4: 入手の際に特定個人情報が入力された本人確認の措置の内容</p>	<p>国民健康保険システム端末は閉鎖した基幹業務系のネットワークで共通基盤と接続するとともに、MACアドレスによる認証等により、不適切な端末接続による特定個人情報の漏えい・紛失を防止している。</p> <p><共通基盤における措置> ※ 略</p> <p><中間サーバー・ソフトウェアにおける措置> ※ 略</p> <p><中間サーバー・プラットフォームにおける措置> ①～② ※ 略 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。</p>	<p>国民健康保険システム端末は閉鎖した基幹業務系のネットワークで共通基盤と接続するとともに、MACアドレスによる認証等により、不適切な端末接続による特定個人情報の漏えい・紛失を防止している。</p> <p><共通基盤における措置> ※ 修正なし</p> <p><中間サーバー・ソフトウェアにおける措置> ※ 修正なし</p> <p><中間サーバー・プラットフォームにおける措置> ①～② ※ 修正なし ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。</p>	事前	中間サーバーの更改に伴い修正

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
令和8年3月24日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル) 6. 情報提供ネットワークシステムとの接続 リスク6: 不適切な方法で提供されるリスク リスクに対する措置の内容	<共通基盤における措置> ※ 略 <中間サーバー・ソフトウェアにおける措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①~② ※ 略 ③中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	<共通基盤における措置> ※ 修正なし <中間サーバー・ソフトウェアにおける措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①~② ※修正なし ③中間サーバー・プラットフォームの事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	事前	中間サーバーの更改に伴い修正
令和8年3月24日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル) 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	<中間サーバー・ソフトウェアにおける措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①~③ ※ 略 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの事業者における情報漏えい等のリスクを極小化する。	<中間サーバー・ソフトウェアにおける措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①~③ ※ 修正なし ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事前	中間サーバーの更改に伴い修正
令和8年3月24日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル) 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	<広島市における措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームを中間サーバー用データセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないように、警備員などにより確認している。	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。	事前	中間サーバーの更改に伴い修正
令和8年3月24日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル) 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①~③ ※ 略	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①~③ ※ 修正なし ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。	事前	中間サーバーの更改に伴い修正

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
令和8年3月24日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(国民健康保険情報ファイル) 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容(続き)	<国保総合(国保集約)システムの保管・消去> ※ 略	<国保総合(国保集約)システムの保管・消去> ※ 修正なし	事前	中間サーバーの更改に伴い修正
令和8年3月24日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(滞納情報ファイル) 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑤物理的対策 具体的な対策の内容	<広島市における措置> ※ 略 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームを中間サーバー用データセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ②事前に申請し承認されてない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないように、警備員などにより確認している。	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・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サービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。	事前	中間サーバーの更改に伴い修正
令和8年3月24日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策(滞納情報ファイル) 7. 特定個人情報の保管・消去 リスク1: 特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①～③ ※ 略	<広島市における措置> ※ 修正なし <中間サーバー・プラットフォームにおける措置> ①～③ ※ 修正なし ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。	事前	中間サーバーの更改に伴い修正

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
令和8年3月24日	IV その他のリスク対策 1. 監査 ②監査 具体的な内容	<p>「広島市情報セキュリティポリシー」に、「定期的 に又は必要に応じて情報セキュリティ監査を行 い、改善の必要があるものについては、速やか に改善措置を行うこと」を定め、4年に1回、外 部監査を実施することとしている。</p> <p><中間サーバー・プラットフォームにおける措置 > ①運用規則等に基づき、中間サーバー・プラッ トフォームについて、毎年1回、監査を行うこと としている。 ②政府情報システムのためのセキュリティ評価 制度 (ISMAP) に登録されたクラウドサービス事 業者は、定期的 ISMAP 監査機関リストに登録 された監査機関による監査を行うこととしてい る。</p> <p><国保総合(国保集約)システムにおける措置 > ・番号利用法第29条の3第2項による個人情報 保護委員会への特定個人情報ファイルの取扱 いの状況に関する報告(それに伴い、国保連合 会にも同様の報告を求めるとする)。</p>	<p>「広島市情報セキュリティポリシー」に、「定期的 に又は必要に応じて情報セキュリティ監査を行 い、改善の必要があるものについては、速やか に改善措置を行うこと」を定め、4年に1回、外 部監査を実施することとしている。</p> <p><中間サーバー・プラットフォームにおける措置 > ①運用規則等に基づき、中間サーバー・プラッ トフォームについて、毎年1回、監査を行うこと としている。 ②政府情報システムのためのセキュリティ評価 制度 (ISMAP) に登録されたクラウドサービス事 業者は、定期的 ISMAP 監査機関リストに登録 された監査機関による監査を行うこととしてい る。</p> <p><国保総合(国保集約)システムにおける措置 > ・番号利用法第29条の3第2項による個人情報 保護委員会への特定個人情報ファイルの取扱 いの状況に関する報告(それに伴い、国保連合 会にも同様の報告を求めるとする)。</p>	事前	中間サーバーの更改に伴い 修正
	IV その他のリスク対策 3. その他のリスク対策	<p><中間サーバー・プラットフォームにおける措置 > 中間サーバー・プラットフォームを活用するこ とにより、統一した設備環境による高レベルのセ キュリティ管理(入退室管理等)、ITリテラシの高 い運用担当者によるセキュリティリスクの低減、 及び技術力の高い運用担当者による均一的で 安定したシステム運用・監視を実現する。</p> <p><取りまとめ機関における措置> 支払基金が「医療保険者等向け中間サーバー 等における資格履歴管理事務」のうち「運用支 援環境において、委託区画から取得した資格情 報等を基に、資格履歴ファイルに格納する業 務」及び「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」のうち「機関別符号取 得業務」、「情報提供業務(オンライン資格確認 等システムで管理している情報と紐付けるため に使用する情報の提供)」の特定個人情報保護 評価を実施している。</p>	<p><中間サーバー・プラットフォームにおける措置 > 中間サーバー・プラットフォームを活用するこ とにより、政府情報システムのためのセキュリ ティ評価制度 (ISMAP) に登録されたクラウドサー ビス事業者による高レベルのセキュリティ管理(入 退室管理等)、ITリテラシの高い運用担当者に よるセキュリティリスクの低減、及び技術力の高 い運用担当者による均一的で安定したシステム 運用・監視を実現する。</p> <p><取りまとめ機関における措置> 支払基金が「医療保険者等向け中間サーバー 等における資格履歴管理事務」のうち「運用支 援環境において、委託区画から取得した資格情 報等を基に、資格履歴ファイルに格納する業 務」及び「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」のうち「機関別符号取 得業務」、「情報提供業務(オンライン資格確認 等システムで管理している情報と紐付けるため に使用する情報の提供)」の特定個人情報保護 評価を実施している。</p>	事後	中間サーバーの更改に伴い 修正