

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
	介護保険事業に関する事務

個人のプライバシー等の権利利益の保護の宣言	
山形市は、介護保険事業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
山形市長

個人情報保護委員会 承認日【行政機関等のみ】
公表日

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	介護保険事業に関する事務
②事務の内容 ※	介護保険法に基づき下記の事務を行っている。 特定個人情報保護ファイルは、介護保険法及び行政手続における特定の個人を識別するための番号の利用等に関する法律(以下「番号法」という。)の規定に基づき、以下の事務で取り扱う。 ・被保険者の介護保険資格管理に関する事務 ・保険料の賦課・徴収管理に関する事務 ・受給者管理に関する事務 ・給付管理に関する事務 ・地域支援事業に関する事務(被保険者の保健医療の向上及び福祉の増進を図るため、被保険者、介護サービス事業者その他の関係者が被保険者に係る情報を共有し、及び活用することを促進する事業として、介護情報基盤を活用した情報連携を実施する。) 申請管理システムについては以下のとおり取り扱う。 ・窓口や郵送での書類の受付により基幹システムへ入力 ・「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」により基幹システムに転記入力 地域支援事業に関する事務として実施する介護情報基盤を活用した情報連携に係る介護保険事務は、以下のとおり取り扱う。 ・市区町村は、介護情報基盤へ本事務に係る対象者の個人番号を含む対象者情報、介護保険関係情報、介護保険認定情報、介護保険住宅改修費利用情報、介護保険福祉用具購入費利用情報等の紐付け及び登録を行う。 ・介護サービス事業所は、介護保険資格確認等WEBサービス経由で、事業所の利用者に関して市区町村が登録した情報の確認等を行う。 ・住民は、マイナポータル経由で、本事務に係る自身の介護保険資格情報、介護保険認定審査進捗情報、介護保険住宅改修費利用情報、介護保険福祉用具購入費利用情報等の情報の確認等を行う。
③対象人数	[10万人以上30万人未満] <選択肢> 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	介護保険システム
②システムの機能	[資格管理]・被保険者資格の取得、喪失管理・被保険者証および資格者証の交付と回収・適用除外者の管理・住所地特例適用者の管理・他法受給情報の管理(生活保護／老齢福祉年金) [賦課管理]・賦課算定・所得の把握・特別徴収・保険料の減免・減額 [受給管理]・要介護認定の申請管理・訪問調査・医師の意見書の依頼・認定(決定)・利用者負担の軽減の管理 [給付管理]・ケアプランの管理・受給者台帳の管理・給付実績の管理・福祉用具購入費・住宅改修費の管理・高額介護サービス費の管理・高額医療合算介護サービス費の管理 [その他]・報告資料等の作成機能 ・情報提供ネットワークシステムを通じて口座登録・連携ファイル関係情報を取得
③他のシステムとの接続	[☐] 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 (収納管理システム、滞納管理システム、介護情報基盤)

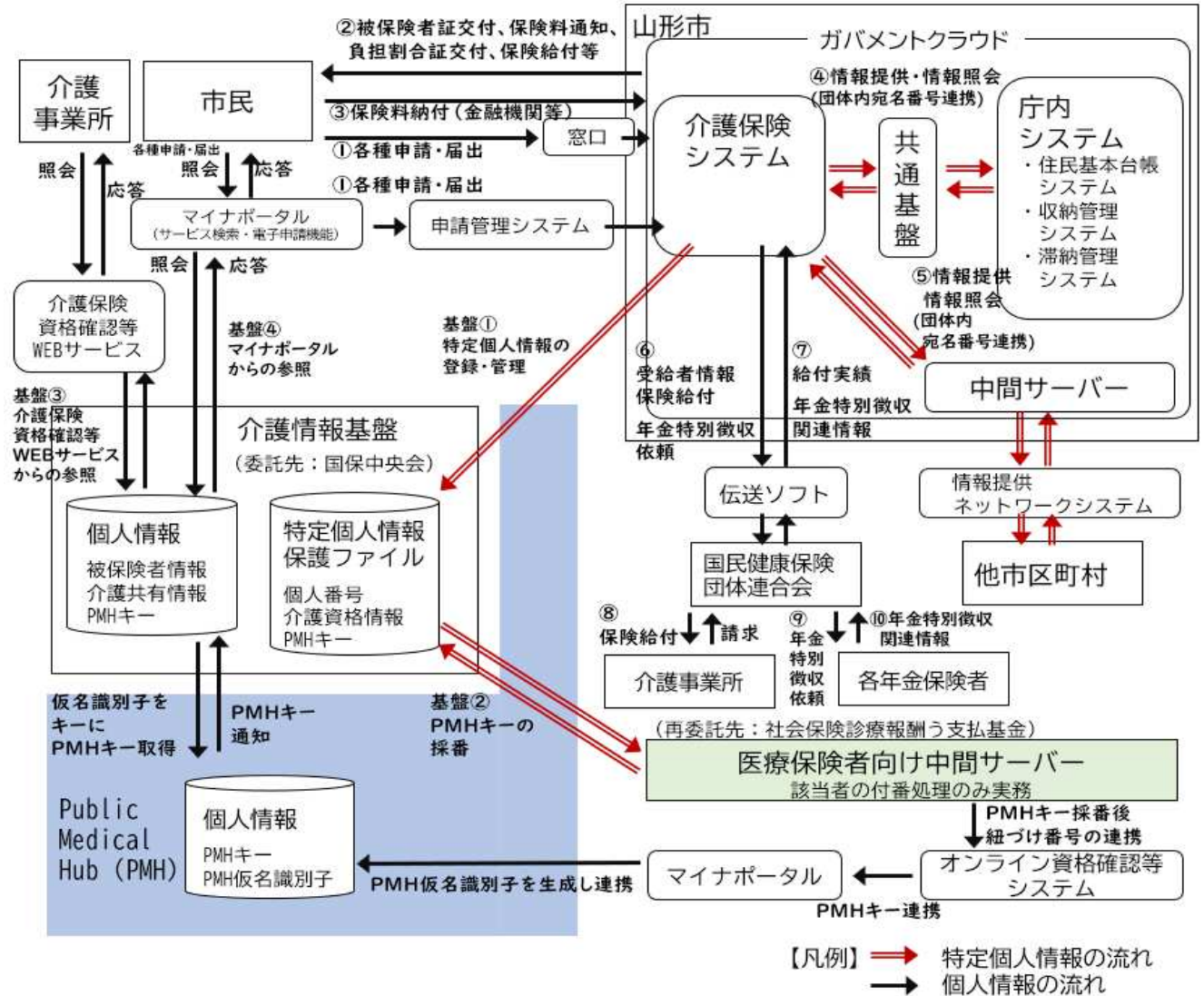
システム2	
①システムの名称	収納管理システム
②システムの機能	賦課情報取込 ・賦課情報登録機能 介護保険保険業務より、賦課情報を受け取り、収納情報に登録する。 更正が行われた場合は、更正処理後の賦課情報も受け取る。 収納 ・消込機能 被保険者または各機関より各種納付情報を受け取り、収納情報の消込処理を行う。 ・還付、充当機能 還付、充当の対象者を抽出し、充当先がある場合は、充当処理を行い、被保険者へ充当通知書を通知する。 充当先がない場合、該当被保険者に関する還付を行い、収納情報を更新する。 ・督促、催告機能 納期限を過ぎても納付が行われていない被保険者を抽出し、督促状を出力する。 督促を実施しても納付が行われない被保険者を抽出し、段階的に催告書を出力する。 口座振替管理機能 被保険者より口座振替に関する申込、変更、取消等を受け付け、金融機関へ照会等を行い、納付方法を登録、変更、取消を行う。 滞納繰越： ・滞納繰越機能 前年度の滞納分について、滞納繰越処理を行う。 発行： ・各種証明書発行機能 納付額確認書等を作成、交付する。 照会： ・収納情報照会機能 該当の者に対する、賦課・収納情報等を照会する。 会計資料作成： 月報、収納集計表等の各種会計資料が作成できる。
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 住民基本台帳ネットワークシステム [○] 宛名システム等 [○] その他 （ 介護保険システム、滞納管理システム [] 庁内連携システム [] 既存住民基本台帳システム [] 税務システム)

システム3	
①システムの名称	滞納管理システム
②システムの機能	滞納整理 ・滞納者登録機能 収納情報より、滞納者を抽出し、滞納情報に登録する。 ・催告機能 督促を促しても納付しない被保険者に対して、催告書を出力する。 ・相談対応機能 被保険者より徴収猶予の申請を受け付け、審査結果を登録する。 納付計画に対する納付誓約書を受け取り、情報を管理する。 被保険者より、延滞金減免の申請を受け付け、審査結果を登録する。 ・処分機能 財産調査、交付要求、差し押さえ、公売(換価)、執行停止 決算: ・不納欠損 執行停止及び時効により納付義務が消滅した時、滞納情報から該当データを抹消する。 ・滞納繰越 前年度の滞納分について、滞納繰越処理を行う。 発行: ・各種証明書発行機能 各種証明書等を作成、交付する。 ・納付書再発行機能 照会: ・滞納情報照会機能 該当の者に対する、滞納情報等を照会する。 統計資料作成: - 必要な統計資料を作成し、該当期間に報告する。
③他のシステムとの接続	☐ 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 （ 介護保険システム、収納管理システム ）
システム4	
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	【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。 具体的には以下の電子申請を受け付ける。 (1)要介護・要支援認定の申請 (2)要介護・要支援更新認定の申請 (3)要介護・要支援状態区分変更認定の申請 (4)居宅(介護予防)サービス計画作成(変更)依頼の届出 (5)介護保険負担割合証の再交付申請 (6)被保険者証の再交付申請 (7)高額介護(予防)サービス費の支給申請 (8)介護保険負担限度額認定申請 (9)居宅介護(介護予防)福祉用具購入費の支給申請 (10)居宅介護(介護予防)住宅改修費の支給申請(住宅改修前) (11)居宅介護(介護予防)住宅改修費の支給申請(住宅改修後) (12)住所移転後の要介護・要支援認定申請 【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	☐ 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 （ サービス検索・電子申請機能 ）

システム5	
①システムの名称	申請管理システム
②システムの機能	連携サーバ サービス検索・電子申請機能で受け付けた電子申請データを申請管理システムに連携する(受け渡す)機能 申請管理システム 連携サーバから連携された電子申請データを参照する機能
③他のシステムとの接続	☐ 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6～10	
システム6	
①システムの名称	介護情報基盤
②システムの機能	<介護情報基盤を活用した情報連携に係る介護保険事務> 介護情報基盤が介護保険に係る各種データを扱う際には、個人を特定するキーとして、介護保険被保険者番号又はPublic Medical Hub(以下「PMH」という。)固有の識別子(PMHキー)にて制御する仕様としている(PMHキーは、特定個人情報と紐づけることで個人を特定するキーである)。詳細な機能は以下のとおり。 ①特定個人情報の登録・管理 ・情報連携のため、当市は、介護情報基盤(PMH介護領域)へ本事務に係る対象者の個人番号等の紐付け及び登録を行う。(LGWAN回線等経由) ・介護情報基盤に登録された特定個人情報は、自治体からのアクセスのみに制御される。また特定個人情報を出力する機能はない。 ②PMHキー採番 ・介護情報基盤は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼する。 ・医療保険者等向け中間サーバーは、PMHキーを採番して介護情報基盤に回答する。 ・医療保険者等向け中間サーバーはPMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムはPMHキーと紐付番号を紐付けて、マイナポータルに連携する。 ・マイナポータルは新たにPMH用の仮名識別子(PMH仮名識別子)を生成し、シリアル番号、PMH仮名識別子、PMHキーと紐付けて、PMHに連携する。 (連携後、マイナポータル上からPMHキーは削除される。)以降、マイナポータルからの介護情報参照等が可能となる。 ③介護保険資格確認等WEBサービスからの参照 ・介護事業所が介護保険資格確認等WEBサービス経由で、事業所にて管理している被保険者の介護情報を確認する。 ・介護保険資格確認等WEBサービスは、被保険者番号をキーに介護情報基盤に対して介護情報(証等の情報、認定情報等)を照会する。 ・介護情報基盤は被保険者番号をキーに介護情報基盤の介護情報を取得し返却する。 ④マイナポータルからの参照 ・住民がマイナポータル経由で、自身の介護保険情報を確認する。 ・マイナポータルは、PMH仮名識別子をキーに介護情報基盤に被保険者情報を照会する。 ・介護情報基盤はPMH共通にPMH仮名識別子を連携しPMHキーを取得し、PMHキーをキーに介護情報基盤の介護情報を取得し返却する。
③他のシステムとの接続	☐ 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 (介護保険システム、認定審査会システム、マイナポータル、PMH、介護保険資格確認等WEBサービス、医療保険者等向け中間サーバー、オンライン資格確認等システム、履歴照会回答システム、介護保険審査支払等システム、LIFEシステム、HPKI認証局、資格確認端末)
システム11～15	
システム16～20	

3. 特定個人情報ファイル名	
介護保険関係情報ファイル	
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	・保険料の賦課及び保険給付において、保険料や負担割合等を適切に算定するため、特定個人情報ファイルを利用し、被保険者等の地方税関係情報を正確かつより効率的に把握する必要がある。 ・保険者や被保険者が各種証明書類を取得する手続きを省略し、住民の負担軽減及び事務の効率化を図るため、特定個人情報ファイルを利用し、国や他の自治体と連携する必要がある。
②実現が期待されるメリット	・被保険者等の情報を正確に把握できることから、公平公正な保険料の賦課及び保険給付が期待できる。 ・他市町村からの転入者や被保険者の所得等の確認等について、保険者が書面で行う照会・公用請求や、被保険者が添付する各種証明書類の省略が図られ、行政事務の効率化や被保険者の負担軽減が期待できる。
5. 個人番号の利用 ※	
法令上の根拠	番号法 ・第9条第1項 別表第100の項 番号法の別表の主務省令で定める事務を定める命令 ・第50条
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	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表 [情報照会] 第131、132の項 [情報提供] 第3欄(情報提供者)が市町村長であり、同第4欄に「介護保険給付等関係情報」を含む項 (2、3、7、11、15、42、56、65、69、80、83、86、87、108、115、125、128、132、144、161)
7. 評価実施機関における担当部署	
①部署	山形市福祉推進部介護保険課
②所属長の役職名	介護保険課長
8. 他の評価実施機関	

(別添1) 事務の内容



<介護情報基盤を活用した情報連携に係る介護保険事務>

PMHにおいて介護情報基盤が介護保険に係る各種データを扱う際には、個人を特定するキーとして、被保険者番号又は独自の項目であるPMHキーにて制御する仕様としている。PMHキーは①～②の流れで、医療保険者等向け中間サーバーにて採番される。採番後に医療保険者等向け中間サーバーより連携を受けたマイナポータルではPMH仮名識別子の生成が行われ、PMHにてPMHキーとPMH仮名識別子の紐づけが行われる。採番の過程で制御情報として特定個人情報は介護情報基盤に登録されるものの、PMHキーが採番されて以降は、介護保険資格確認等WEBサービスから介護保険に関連する情報にアクセスする際には被保険者番号をキーとして、マイナポータルから介護保険に関連する情報にアクセスする際にはPMH仮名識別子をキーとして、PMHキーをPMH(共通)から取得し制御する仕組みとなっている。このため、特定個人情報ファイルへのアクセスは、個人番号等の紐づけ及び登録のみに限定する仕組みとしている。

(備考)

1 被保険者の資格管理

①④ 被保険者等からの届出、住民基本台帳システムとの庁内連携による転入、65歳年齢到達、死亡等の情報に基づき、資格の取得及び死亡、転出等による資格の喪失管理を行う。

② 被保険者に被保険者証等の送付・窓口交付を行う。

2 保険料の賦課・徴収

②④⑤⑥ 市税システムとの庁内連携等による被保険者の所得等の情報に基づき、保険料を賦課し、通知する。

① 被保険者等から保険料の減免申請書を収受する。

② 決定した内容について、被保険者に保険料納入通知書等を送付する。

⑥⑨⑩ 国民健康保険団体連合会(国保連)を通じて、年金保険者と特別徴収情報の交換を行う。

③ 被保険者は、年金からの特別徴収、金融機関での納付書又は口座振替等の方法により保険料を納付する。

④ 被保険者の納付(納入)状況について、収納管理システムとの庁内連携により確認する。

②④ 過納付や誤納付については、超過額を還付又は充当し、被保険者に通知する。

②④ 納期限までに完納しない場合は、被保険者に督促状を送付する。

3 受給者管理(要支援・要介護認定)

① サービス利用を希望する被保険者等からの要支援・要介護認定申請に基づき、要介護認定を行う。

② 被保険者に対して、要介護認定結果通知書等を送付する。

② 身体障害者手帳等をお持ちでない要介護1～5の方に、障害者控除対象者認定書の交付する。

4 保険給付

⑥ 国保連に受給者情報を提供する。

⑥⑦⑧ 国保連を通じて介護サービスの費用の支払い(保険給付)を行い、その実績情報等を受理する。

① 被保険者等からの介護サービスの費用の償還払い等の支給申請を収受する。

② 被保険者等に介護サービスの費用の償還払いを行う。

⑥⑦ 国保連に必要な情報を照会し、情報提供を受ける。

<介護情報基盤を活用した情報連携に係る介護保険事務>

基盤①特定個人情報の登録・管理

・情報連携のため、本市区町村は、介護情報基盤へ本事務に係る対象者の個人番号等の紐付け及び登録を行う。(LGWAN回線等経由)

・介護情報基盤に登録された特定個人情報は、自治体からのアクセスのみに制御される。また特定個人情報を出力する機能はない。

基盤②PMHキー採番

・介護情報基盤は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼する。医療保険者等向け中間サーバーは、PMHキーを採番して介護情報基盤に回答する。

・医療保険者等向け中間サーバーはPMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。

・オンライン資格確認等システムはPMHキーと紐付番号を紐付けて、マイナポータルに連携する。

・マイナポータルは新たにPMH用の仮名識別子(PMH仮名識別子)を生成し、シリアル番号、PMH仮名識別子、PMHキーと紐付けて、PMHに連携する。(連携後、マイナポータル上からPMHキーは削除される。)以降、マイナポータルからの介護情報参照等が可能となる。

基盤③介護保険資格確認等WEBサービスからの参照

・介護事業所が介護保険資格確認等WEBサービス経由で、事業所にて管理している被保険者の介護情報を確認する。

・介護保険資格確認等WEBサービスは、被保険者番号をキーに介護情報基盤に対して介護情報(証等の情報、認定情報等)を照会する。

・介護情報基盤は被保険者番号をキーに介護情報基盤の介護情報を取得し返却する。

基盤④マイナポータルからの参照

・住民がマイナポータル経由で、自身の介護保険情報を確認する。

・マイナポータルは、PMH仮名識別子をキーに介護情報基盤に被保険者情報を照会する。

・介護情報基盤はPMH共通にPMH仮名識別子を連携しPMHキーを取得し、PMHキーをキーに介護情報基盤の介護情報を取得し返却する。

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

介護保険関係情報ファイル

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 ※	・被保険者:65歳以上の者(年齢到達予定者を含む)、または40歳以上65歳未満の医療保険加入者で、本人申請に基づき被保険者証が交付されている者。資格取得後、転出等により資格喪失した者を含む。 ・世帯員:被保険者と同一の世帯に属する者	
その必要性	・被保険者は、介護保険関係情報の管理を行うために必要。 ・世帯員は、被保険者の保険料の算定及び給付費の支給判定を行うために必要。	
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 ※	・識別情報 [☐] 個人番号 [☐] 個人番号対応符号 [☐] その他識別情報(内部番号) ・連絡先等情報 [☐] 5情報(氏名、氏名の振仮名、性別、生年月日、住所) [☐] 連絡先(電話番号等) [☐] その他住民票関係情報 ・業務関係情報 [☐] 国税関係情報 [☐] 地方税関係情報 [☐] 健康・医療関係情報 [☐] 医療保険関係情報 [☐] 児童福祉・子育て関係情報 [☐] 障害者福祉関係情報 [☐] 生活保護・社会福祉関係情報 [☐] 介護・高齢者福祉関係情報 [☐] 雇用・労働関係情報 [☐] 年金関係情報 [☐] 学校・教育関係情報 [☐] 災害関係情報 [☐] その他 (口座登録・連携ファイル関係情報)	
その妥当性	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):当市において、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(以降、宛名番号と表記) 基本5情報:被保険者証の印刷等、介護保険関係情報の管理のために保有する。 地方税関係情報:利用者負担、保険料賦課額を判定するために保有する。 医療保険関係情報:給付費適正化のために保有する 生活保護・社会福祉関係情報:被保険者資格、利用者負担段階、保険料段階を判定するために保有する。 介護・高齢者福祉関係情報:当事務を運用するための介護保険情報等を保有する。 年金関係情報:利用者負担、保険料賦課額を判定するために保有する。 <介護情報基盤を活用した情報連携に係る介護保険事務> ・識別情報 介護被保険者番号、個人番号(マイナンバー)、PMHキー…介護情報基盤が外部と情報連携するために必要となる。 ・業務関係情報 介護・高齢者福祉関係情報…(介護保険事務の適切な実施にあたり必要となる情報を管理し、)介護情報基盤が、外部と情報連携するために必要となる。	
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	山形市福祉推進部介護保険課	

3. 特定個人情報の入手・使用			
①入手元 ※		☐ 本人又は本人の代理人 ☐ 評価実施機関内の他部署 （ 住民基本台帳担当課、個人住民税担当課、国保年金課、福祉課 ） ☐ 行政機関・独立行政法人等 （ デジタル庁 ） ☐ 地方公共団体・地方独立行政法人 （ 他市町村等 ） ☐ 民間事業者 （ ） ☐ その他 （ 社会保険診療報酬支払基金 ）	
②入手方法		☐ 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 ☐ 電子メール ☐ 専用線 ☒ 庁内連携システム ☐ 情報提供ネットワークシステム ☐ その他 （ 住基ネット、サービス検索・電子申請機能、申請管理システム、LGWAN回線を用いた介護保険システムからのデータ連携、医療保険者等向け中間サーバー ）	
③入手の時期・頻度		個人番号、その他識別情報(内部番号)、基本5情報:随時 地方税関係情報:随時または月次、年次 医療保険関係情報:随時 生活保護・社会福祉関係情報:随時 介護・高齢者福祉関係情報:随時 年金関係情報:月次、年次 <介護情報基盤を活用した情報連携に係る介護保険事務> ・PMHキーの採番処理依頼時に都度、介護保険システムから特定個人情報を入手する。	
④入手に係る妥当性		介護保険事業に関する事務を適正に行うため、法令の範囲内で適宜、申請等の情報、税情報等の収集を行う必要がある。 <介護情報基盤を活用した情報連携に係る介護保険事務> ・PMHキーの採番処理依頼時に都度、市区町村介護保険システムから自動的に連携する。	
⑤本人への明示		・本人及び代理人から入手する情報(介護保険法等に規定がある場合を除く)は、利用目的を明示する。 ・庁内連携システム等による入手については、番号法第9条第2項に基づく市条例において明示されている。 ・情報提供ネットワークによる入手については、番号法第19条第8号に基づく主務省令第2条の表第131、132の項において明示されている。 ・住民基本台帳ネットワークシステムによる入手については、番号法第14条第2項において、地方公共団体情報システム機構に対し機構保存本人確認情報の提供を求めることができる旨が明示されている。	
⑥使用目的 ※		・被保険者および世帯構成員に関する特定個人情報を効率よく検索および管理するために使用する(番号法第9条第1項)	
変更の妥当性		—	
⑦使用の主体	使用部署 ※	山形市福祉推進部介護保険課	
	使用者数	[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	

⑧使用方法 ※		・届出書等に記載された個人番号の真正性を確認するため、当システム(新規取得の場合は、住基システムや宛名管理システム等)にて、届出書に記載された個人番号で検索して、特定個人情報の確認を行う。 ・税情報等、他の特定個人情報を参照する際に、副次的な突合キーとして個人番号を使用する。 ・「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。 ＜介護情報基盤を活用した情報連携に係る介護保険事務＞ ・情報連携のため、当市は、介護情報基盤(PMH介護領域)へ本事務に係る対象者の個人番号等の紐付け及び登録を行う。(LGWAN回線等経由) ・介護情報基盤は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼する。 ・医療保険者等向け中間サーバーは、PMHキーを採番して介護情報基盤に回答する。 ・医療保険者等向け中間サーバーはPMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムはPMHキーと紐付番号を紐付けて、マイナポータルに連携する。 ・マイナポータルは新たにPMH用の仮名識別子(PMH仮名識別子)を生成し、シリアル番号、PMH仮名識別子、PMHキーと紐付けて、PMHに連携する。(連携後、マイナポータル上からPMHキーは削除される。)以降、マイナポータルからの介護情報参照等が可能となる。
	情報の突合 ※	＜介護情報基盤を活用した情報連携に係る介護保険事務以外の介護保険事務＞ ・個人を正確に特定するために個人番号を利用して正確性を確保する。 ・申請者を確認するために既存住基システムを通じて取り込んだ番号紐付情報と突合する。
	情報の統計分析 ※	介護保険における被保険者の資格、保険料賦課・徴収、認定、給付状況について、各種統計資料を作成しているが、特定の個人を判別するような情報の分析や統計は行わない。また、個人番号を使用した統計分析は行わない。
	権利利益に影響を与え得る決定 ※	被保険者の資格取得・喪失の決定、保険料の賦課決定、保険料の還付の支払いの決定、要介護(要支援)認定申請結果の決定、自己負担割合の決定、高額介護(介護予防)サービス費及び総合事業高額介護予防サービス費相当事業・高額医療合算介護(介護予防)サービス費及び総合事業高額医療合算介護予防サービス費相当事業、介護保険居宅介護(介護予防)福祉用具購入費、介護保険居宅介護(介護予防)住宅改修費、介護保険居宅介護(介護予防)サービス費等(償還払)、介護予防・日常生活支援総合事業費(償還払)及び介護保険特定入所者介護(介護予防)サービス費等の支給決定、各種負担限度額(利用者負担減免含む)の認定
⑨使用開始日		平成28年1月4日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		☐ 委託する <選択肢> 1) 委託する 2) 委託しない (2) 件
委託事項1		介護情報基盤を活用した情報連携に係る介護保険事務における特定個人情報ファイルの一部の取扱い
①委託内容		介護情報基盤の利用・情報連携業務及び運用保守業務
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一部 <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	☐ 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
	対象となる本人の範囲 ※	被保険者番号を有する被保険者
	その妥当性	PMHキーの採番や、その適切な管理のために特定個人情報ファイルを取り扱う必要がある。
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 ☒ その他 (LGWAN又は閉域網回線を用いた提供)
⑤委託先名の確認方法		山形市情報公開条例に基づく情報公開請求
⑥委託先名		山形県国民健康保険団体連合会 (山形県国民健康保険団体連合会は、公益社団法人 国民健康保険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	書面による承諾
	⑨再委託事項	介護情報基盤におけるPMHキーを用いた情報連携 介護情報基盤の運用保守

[illegible]

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 (21) 件 ☐ 移転を行っている (1) 件 ☐ 行っていない
提供先1	情報提供者(番号法第19条第8号に基づく主務省令第2条の表第3欄)が「市町村」であり、かつ、同表第4欄に「介護保険給付等関係情報」を含むもの。(別添4) 提供先一覧に記載
①法令上の根拠	(別添4) 提供先一覧に記載
②提供先における用途	(別添4) 提供先一覧に記載
③提供する情報	(別添4) 提供先一覧に記載
④提供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提供する情報の対象となる本人の範囲	(別添4) 提供先一覧に記載
⑥提供方法	☐ 情報提供ネットワークシステム ☐ 電子メール ☐ フラッシュメモリ ☐ その他 () ☐ 専用線 ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ 紙
⑦時期・頻度	照会を受けた都度
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	

移転先1	住民基本台帳担当課
①法令上の根拠	住民基本台帳法第7条第10号の3
②移転先における用途	介護保険の被保険者の資格に関する住民票の記載事項を管理する。
③移転する情報	介護保険の被保険者である者の介護保険資格情報
④移転する情報の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 [10万人以上100万人未満]
⑤移転する情報の対象となる本人の範囲	当市に住民票がある者のうち、介護保険の被保険者情報が管理されている被保険者本人(世帯構成員は含まない)。
⑥移転方法	[☒] 庁内連携システム [] 電子メール [] フラッシュメモリ [] その他 ([] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙)
⑦時期・頻度	介護保険の被保険者において、資格の得喪にかかる異動が発生した都度
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去													
①保管場所 ※		＜山形市における措置＞ ・セキュリティゲートにて入退室管理を行っている部屋に設置したサーバ内に保管する。 ・サーバへのアクセスは、ID/パスワードによる認証が必要である。 ＜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に登録された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/IEC7017、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。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における措置＞ ・特定個人情報の格納領域を分けて、ユーザアカウント権限の制御を行い、さらにアクセス者の識別を行う。 ・外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離する。 ・不正侵入を検知・防御するシステムを導入することで、ネットワーク、Webアプリケーションへの不正アクセスを防止する。 ・ログ監査により、不正アクセスを検知する。 ・データ暗号化、通信暗号化を行う。											
	②保管期間	＜選択肢＞ <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>	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													
	その妥当性	介護保険法等の法令では、保管期間の定めはない。											

③消去方法	＜山形市における措置＞ ・事務処理上、消去して問題ない情報かどうかを一定期間ごとに確認する（介護保険法等には保管期間の定めがない）。 ・外部記憶媒体に一時的に記録した個人番号付電子申請データは、使用の都度速やかに完全消去する。 ・内部で定められた保存期間を経過した申請書等紙媒体は、内部の定めに従い廃棄処分する。 ＜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に準拠したデータ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。 ＜ガバメントクラウドにおける措置＞ 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。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠してデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における措置＞ ・特定個人情報は10年で削除する。 ・データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 ・クラウドサービスが提供するユーザーが独自に作成、管理、制御する暗号化キーを削除することで、暗号化されたデータが復元できないようにする。
7. 備考 —	

(別添2) 特定個人情報ファイル記録項目

<介護情報基盤を活用した情報連携に係る介護保険事務以外>

(別添2)ファイル記録項目のとおり(記録項目の中に要配慮個人情報を含む。)

<介護情報基盤を活用した情報連携に係る介護保険事務>

■PMHキー発行状況情報

・マイナンバー

・PMHキー

・処理通番

・ステータス

・エラーコード

■マイナンバー情報

・マイナンバー

・介護保険者番号

・介護保険被保険者番号

・PMHキー

■削除要求情報

・マイナンバー

・処理通番

・介護保険者番号

・介護保険被保険者番号

・資格取得日(証記載保険者)

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	
介護保険関係情報ファイル	
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	・窓口で申請書・届出書等を受領する場合は、番号法及び関係法令に定める本人確認書類により番号確認を行う。また、誤って対象者以外の情報を入手することがないように、申請書・届出書等の内容と本人確認書類（個人番号カード等）により身元確認を行う。 ・他市町村等から情報を入手する際は、対象者以外の情報を誤って入手することがないように、所定の様式を使用し、処理を統一化する。 ・その他、個人情報の取扱いに関しては、当市セキュリティポリシーに準ずる。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 既存事務において本人確認を行った個人番号を既存システム（各業務システム）からPublic MedicalHub（PMH）に連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。
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	・必要な情報以外を誤って記載することがないように、所定の様式を使用する。 ・庁内の連携により情報を入手する場合は、システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセスを制限により不正なアクセスを防止する。 ・他市町村等から情報を入手する際は、必要以外の情報を入手しないよう、事務マニュアル等を整備し、処理を統一化する。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 定められたインターフェース仕様に沿って決められたデータ項目のみが返却されるようシステムの制御している。自治体ごとのアクセス制御も実施する。
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： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・窓口で届出書等を受領する場合は、本人または代理人の本人確認及び委任状の確認を行う。 ・情報提出を依頼する際は、その使用目的・用途について説明する。 ・庁内のシステム連携により情報を入手する場合は、システムのアクセス制限により操作対象者及び権限を制限し、不必要な情報へのアクセスを制限により不正なアクセスを防止する。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 定められたインターフェース仕様に沿って決められたデータ項目のみが返却されるようシステムの制御している。自治体ごとのアクセス制御も実施する。
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： 入手した特定個人情報ที่ไม่正確であるリスク	
入手の際の本人確認の措置の内容	・本人確認書類（個人番号カード等）の提示を受け、本人確認を行う。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 市区町村介護保険システムより連携される特定個人情報を加工することなくPMHキーの発行要求等で使用するため、不正確な特定個人情報が入手されることはない。

個人番号の真正性確認の措置の内容	・個人番号カード等の提示を受け、真正性確認を行う。 ・転入等により、個人番号カード又は通知カード等の提示による確認が困難な場合は、住基システム又は住民基本台帳ネットワークシステムを利用し、真正性確認を行う。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 市区町村介護保険システムより連携される特定個人情報を加工することなくPMHキーの発行要求等で使用するため、不正確な特定個人情報が入手されることはない。
特定個人情報の正確性確保の措置の内容	・対象者を検索し、入力画面に対象者の特定個人情報が表示されたら、届出書等と読み合わせを行って、対象者であることの確認を行う。 ・届出書等の内容を入力画面へ入力することが終了し、入力確定を実施後、画面の内容と届出書等の内容を照合した上で、データベースを更新する。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 市区町村介護保険システムより連携される特定個人情報を加工することなくPMHキーの発行要求等で使用するため、不正確な特定個人情報が入手されることはない。
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4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	・特定個人情報を記載した紙媒体は、内部の文書管理のルールで定められた保管場所で施錠管理する。 ・介護保険システムを含む山形市の基幹システムは閉じられたネットワークの中にあり、外部との接続が制限された環境で利用している。。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ ・個人情報を格納する領域については、外部連携先システムが直接アクセスが行えないようネットワークを分離するとともに、システム自動処理により、介護情報基盤システム内に格納される運用になっている。 ・外部連携先システムとの通信はVPN等の技術を用いた暗号化を行うことで通信内容秘匿、盗聴対策の対応をしている。
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
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	
・介護保険システムへの情報入力、ユーザーIDとパスワードにより認証を行い、IDに設定された権限のみ有効とすることをシステム上制御し、入力できる項目を限定することで、不適切な方法による情報の入手が行えないことを担保している。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カード等の署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われるため、本人からの情報のみが送信される。 サービス検索・電子申請機能の画面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。 ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カード等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。 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。 ・LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZを設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。境界FWや連携サーバで外部接続先との通信を制限している。申請管理システムから基幹システムまでは、外部との接続が制限された環境で利用している。	

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な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	介護保険事業に関する事務の宛名情報は、事務で使用する部署の職員のみが当該情報にアクセスし、利用できる仕組みとなっている。 介護保険システムの稼働するLANには、外部からの侵入を防止するファイヤーウォールによる適切なアクセス制御を実施している。	
事務で使用するその他のシステムにおける措置の内容	<山形市における措置> ・庁内の他のシステムからアクセスできないよう適切なアクセス制御を講じており、目的を超えた紐付けは行われないようにしている。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ・個人情報を格納する領域については、外部連携先システムが直接アクセスが行えないようネットワークを分離するとともにシステム自動処理により、介護情報基盤システム内に格納される運用になっている。 ・外部連携先システムとの通信はVPN等の技術を用いた暗号化を行うことで通信内容秘匿、盗聴対策の対応をしている。	
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: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
	具体的な管理方法	<山形市における措置> ・介護保険システムへのログインはユーザID、パスワードで行う。 ・システムを利用できる端末を管理することにより、不要な端末からの利用ができない制限を実施している。 <介護情報基盤を活用した情報連携に係る介護保険事務における措置> ・介護情報基盤へのログインはユーザID、パスワードで行う。 ・ログイン用のユーザIDは、管理者がユーザ登録を行った者に限定して発行される。
アクセス権限の発効・失効の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
	具体的な管理方法	<山形市における措置> <発効管理> 職員ごとに業務上必要な権限を特定し、必要最小限の範囲で付与している。 <失効管理> 異動・退職等が発生する都度、権限を見直し、不要となった権限を削除している。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ユーザ区分を整理し、定められたユーザのみがアクセス権限を管理できるようにする。

アクセス権限の管理		[行っている]	<選択肢> 1) 行っている2) 行っていない	
	具体的な管理方法	<山形市における措置> ・ユーザIDやアクセス権限の管理表を作成、定期的を確認し、業務上アクセスが不要となったIDやアクセス権限を変更または削除する。 <介護情報基盤におけるPMHキーを用いた情報連携に係る介護保険事務における追加措置> <アクセス権限の管理> システム基盤への各対象毎のアクセス権限については、以下の管理をしている。 ①クラウドサービス ・運用保守事業者は、ユーザ管理環境でユーザを払い出し、ユーザの役割に応じた最小限の権限を付与した権限グループに所属させることで、各環境へのアクセス権限を管理する。 ・特定個人情報への参照権限を保持するグループについては、運用時のインシデント対応など一時的にアクセス権限を付与することとし、通常運用時は権限を付与しないこととする。 ②OS等 ・運用保守事業者は、ID/パスワードにより端末OSへのユーザのアクセス権限を管理する。 ③アプリケーション ・共用IDは発行せず、必ず個人に対し、ユーザーIDを発行する。 <パスワードポリシー> ・クラウドサービス、OS等に対するパスワードポリシーは、原則クラウドサービス、OS等の機能により設定し、ポリシーに従わないパスワードを自動的に拒否する。 ・システムにより自動作成される初期パスワードは推測容易な場合が多いため、初回利用時にパスワード変更を要求する設計とする。自動で変更要求できない場合は運用ルールによる対応を行う。 ・パスワードの使いまわしや推測されやすいパスワード設定を避けるため、定期的なパスワード変更は行わず、有効期限を無期限とする。		
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	<山形市における措置> ・ログインを実施した職員・時刻・操作内容を記録する。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 特定個人情報の適正な取扱いに関するガイドラインの特定個人情報に関する安全管理措置のうち、システム化に関わる「技術的安全管理措置」に沿って、特定個人情報の保護措置を行っており、特定個人情報の使用の記録については、以下の措置を講じている。 <技術的安全管理措置> ・外部からの不正アクセス等の防止 ーログ監査を行い不正アクセスを検知する。 監査ログについては、クラウドサービスのマネージドサービスにより取得、管理し、クラウドサービスのコンソールにより参照する。		
その他の措置の内容		ー		
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	<山形市における措置> ・特定個人情報ファイルのアクセスに対し、ログを記録している。 ・職員向けに、情報セキュリティ教育を実施し情報セキュリティ対策の重要性及び意識向上を行うとともに、情報システム運用教育を実施し情報システムの適正な運用を行うことの啓発に努めている。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ・特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、事務外の使用を防止している。 ・委託業務については、委託先との契約により、委託業者が従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。 ・操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、業務外での使用を防止する。		
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	＜山形市における措置＞ ・特定個人情報ファイルのアクセスに対し、ログを記録している。 ・外部媒体への出力は、管理者権限を持ったユーザーのみが、特定の操作端末機器を使用し、登録管理された記録媒体のみに限定許可している。 ・システムを利用できる端末を管理することにより、不要な端末からの利用ができない制限を実施している。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 特定個人情報の適正な取扱いに関するガイドラインの特定個人情報に関する安全管理措置のうち、システム化に関わる「技術的安全管理措置」に沿って、特定個人情報の保護措置を行っており、特定個人情報ファイルが不正に複製されるリスクについては、以下の措置を講じている。 ＜技術的安全管理措置＞ ・アクセス制御 - ーユーザアカウント権限の制御を行っている。 - ー外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離している。 - ー情報の種別に応じた格納領域の分割を行っている。 ・外部からの不正アクセス等の防止 - ーウイルス/マルウェア対策・標的型攻撃対策・IDS/IPS・改ざん検知を行い、ネットワークへの不正なアクセスの防止、不正プログラムへの対策を行う。 - ーWebアプリケーションへの不正アクセスを防止する。 - ーセキュリティ設計やセキュアコーディング等のセキュリティ対策を実施した上で、本システムの稼働前にセキュリティの専門家によるセキュリティ診断（ペネトレーションテスト等）を実施し、セキュリティ対策が十分行われていることを確認している。 - ーログ監査を行い不正アクセスを検知する。 ・漏えい等の防止 - ー業務データの暗号化については、キーポリシーによる柔軟なアクセス制御、およびクラウドサービス利用終了時に暗号化消去によるデータの完全廃棄を行うことを目的として、原則ユーザーが独自に作成、管理、制御する暗号化キーを使用し、データの暗号化を行っている。 - ー通信経路の暗号化を行っている。 - ー情報の種別に応じた格納領域の分割を行っている。	
	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
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		
・業務外利用したときは、操作ログを確認することで特定可能であることを職員に周知し、業務外利用の抑止に努めている。 外部媒体への出力は、管理者権限を持ったユーザーのみが、特定の操作端末機器を使用し、登録管理された記録媒体のみに限定許可している。 ・サービス検索・電子申請機能へのアクセスログ、システムへのアクセスログ、操作ログの記録を行い、操作者個人を特定できるようにする。 ・アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。 ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。 ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定されたUSBメモリ等のみを使用する。 ＜申請管理システムの措置＞ ・申請管理システムを利用する必要がある職員を特定し、適切なユーザ割り当て及び認証を行う。 ・申請管理システムへのアクセスログ、操作ログの記録を行い、不正とみられる操作があった場合、操作内容を確認する。		

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

委託先情報管理体制書の提出及び委託先の訪問監査を実施した。

＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞

山形市は、介護情報基盤における情報登録に係る業務及び運用保守業務における特定個人情報の取扱いを公益社団法人国民健康保険中央会に委託することとする。特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）に基づき、委託先となる公益社団法人国民健康保険中央会の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。

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

具体的な制限方法

特定個人情報取り扱いに関する委託契約を取り交わした。

＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞

特定個人情報の適正な取扱いに関するガイドラインの特定個人情報に関する安全管理措置のうち、システム化に関わる「技術的安全管理措置」に沿って、特定個人情報の保護措置を行っており、特定個人情報ファイルの閲覧者・更新者の制限については、以下の措置を講じている。

＜技術的安全管理措置＞

- ・アクセス制御

—ユーザアカウント権限の制御を行っている。

一 外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離している。

一情報の種別に応じた格納領域の分割を行っている。

- ・外部からの不正アクセス等の防止

ウイルス/マルウェア対策・標的型攻撃対策・IDS/IPS・改ざん検知を行い、ネットワークへの不正なアクセスの防止、不正プログラムへの対策を行う。

- Webアプリケーションへの不正アクセスを防止する

一セキュリティ設計やセキュアコーディング等のセキュリティ対策を実施した上で、本システムの稼働前にセキュリティの専門家によるセキュリティ診断(ペネトレーションテスト等)を実施し、セキュリティ対策が十分行われていることを確認している。

一ログ監査を行い不正アクセスを検知する。

・漏えい等の防止

一業稼データの暗

用終了時に暗号化消去によるデータの完全廃棄を行うことを目的として、原則ユーザーが独自に作成、管理、制御する暗号化キーを使用し、データの暗号化を行っている。

一通信経路の暗号化を行っている。

一情報の種別に応じた格納領域の分割を行っている。

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

具体的な方法

＜山形市における措置＞

委託契約にて取扱いについて定めている。

＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞

特定個人情報の適正な取扱いに関するガイドラインの特定個人情報に関する安全管理措置のうち、システム化に関わる「技術的安全管理措置」に沿って、特定個人情報の保護措置を行っており、特定個人情報ファイルの取扱いの記録については、以下の措置を講じている。

＜技術的安全管理措置＞

- ・外部からの不正アクセス等の防止

—ログ監査を行い不正アクセスを検知する。

監査ログについては、クラウドサービスのマネージドサービスにより取得、管理し、クラウドサービスのコンソールにより参照する。

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

委託先から他者への
提供に関するルール
内容及びルール遵守
の確認方法

契約上にて再委託先への提供を禁じている。(市の承諾を得た場合の提供も契約上に明記。)

＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞

・委託先(再委託も含む。)から他者への提供は行わない。

・山形市は委託契約に基づき、委託先(再委託先も含む。)から他者への提供が行われていないことを確認できる。

	委託元と委託先間の提供に関するルール内容及びルール遵守の確認方法	必要があれば実施調査を行うとしている。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ・委託先には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・山形市は委託契約に基づき、委託先(再委託先も含む。)から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。
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
	ルール内容及びルール遵守の確認方法	委託契約終了後、速やかに削除することを定めている。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ・委託契約終了後は保管していた全ての特定個人情報を消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、消去について、山形市は報告を受けることができ、それにより消去状況について確認が可能となる。
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
	規定の内容	(個人情報の保護) 受託者及び従事者は、この契約の履行にあたって法令等を遵守するとともに、個人情報の漏えい、滅失、き損の防止その他個人情報の保護を図るため、個人情報の保護に関する法令等、その他当市の個人情報に関する規程及びこの契約の条項を遵守しなければならない。 (秘密の保持) 受託者は、善良な管理者として注意を払う義務を有し、委託業務の処理上、直接または間接的に知り得た事項については、契約期間中及び契約終了後または解除後において、いかなる理由によっても他に漏らしてはならない。 2 受託者は、目的物を第三者に閲覧させ、または貸出、もしくは提供してはならない。 3 受託者は、当市に対し前二項の義務の履行を担保するため、従事者との連署による誓約書を提出しなければならない。 4 受託者は、従事者に対し、事前及び定期的に秘密の保持についての教育を行わなければならない。 (立ち入り検査等) 当市は、必要と認めるときは、受託者に対して委託業務の処理状況並びに個人情報の保護及び管理状況等について随時に調査し、または報告を求めることができる。 (目的外使用の禁止) 受託者は、個人情報を当市から支持された目的以外に使用し、または第三者へ提供してはならない。 (複写及び複製の禁止) 受託者は、当市から指示された場合以外に、個人情報を記録した書類を複写または複製してはならない。 (物品の持ち込み等の禁止) 受託者は、当市の許可を受けた場合を除き、従事者に作業場所への物品の持ち込みまたは作業場所からの物品の持出しをさせてはならない。 (入出力帳票の適正管理) 受託者は、委託業務の履行に際し、入出力帳票の滅失、き損等を防止し、その適正な管理を図らなければならない。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 特定個人情報の適正な取扱いに関するガイドライン(行政機関等編)を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・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 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項

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	再委託は、原則として禁止しているが、事前に再委託理由、事業者名、取扱情報、安全・信頼性の確保、管理監督の方法等を記載した書面を提出させ、再委託に必要性や業務内容等を確認したうえで承認する。 なお、再委託先にも受託元と同等の守秘義務等が課される。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先である公益社団法人国民健康保険中央会が、再委託先における特定個人情報ファイルの管理状況の定期的な点検(年1回程度又は随時)を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、年1回公益社団法人国民健康保険中央会から報告を受ける。	
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		
・委託先の社会的信用と能力を確認するとともに、その記録を残す。 ・作業者を限定するために委託業者の名簿を提出させる。 ・閲覧、更新権限を持つもののアカウント管理を行い、システム上で操作を制限し、操作履歴(ログ)を取得し、不正な使用がないことを確認する。		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない	
リスク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	・提供の記録を管理保存している。		
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	・番号法及び関係法令で定められた提供先、移転先、事項についてのみ行う。		
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	データの連携については、定例的な処理作業スケジュールで管理している。		
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： 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	データの連携については、あらかじめ定められた仕様に基づくサーバ間通信を基本としており、誤った情報や相手への連携は発生しない。		
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			
・不適切な方法での提供・移転が行われるリスクへの措置 住登外者宛名管理システムと庁内連携システム間のデータの移転は、アクセスを許可された業務システムのみデータを移転することをシステム上制御している。 ・誤った情報を提供・移転してしまうリスクへの措置 システム上、照会元から指定された検索条件に基づき得た結果を適切に提供することを担保している。 ・誤った相手に提供・移転してしまうリスクへの措置 認証できない相手先への提供・移転されないことをシステム上制御している。			

6. 情報提供ネットワークシステムとの接続		[] 接続しない(入手)		[] 接続しない(提供)	
リスク1: 目的外の入手が行われるリスク					
リスクに対する措置の内容	＜山形市における措置＞ 介護保険システムは情報提供ネットワークとは直接接続しない。 ＜中間サーバー・ソフトウェアにおける措置＞ ① 番号法上認められた情報連携以外の照会を拒否する機能を有しており、目的外の入手が行われ ないように備えている。 ② 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、操作内容が記録される 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。				
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: 安全が保たれない方法によって入手が行われるリスク					
リスクに対する措置の内容	＜山形市における措置＞ 介護保険システムは情報提供ネットワークとは直接接続しない。 ＜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 中間サーバーと地方公共団体等との間については、VPN(仮想プライベートネットワーク)等の技術 を 利用し、地方公共団体等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。				
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: 入手した特定個人情報ที่ไม่正確であるリスク					
リスクに対する措置の内容	情報提供ネットワークシステムは、特定個人情報保護委員会との協議を経て総務大臣が設置・管理して いる。中間サーバーは、この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しか入手できない 設計になっている。そのため、照会対象者の正確な特定個人情報を入手することが担保されている。				
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: 入手の際に特定個人情報漏えい・紛失するリスク		
リスクに対する措置の内容	<山形市における措置> 介護保険システムは情報提供ネットワークとは直接接続しない。 <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みを入手するため、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を、一定期間経過後に自動で削除することにより、特定個人情報漏えい・紛失するリスクを軽減している。 ④ 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、操作内容が記録されるため、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。 <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 中間サーバーと地方公共団体等との間については、VPN(仮想プライベートネットワーク)等の技術を利用し、地方公共団体等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。	
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	<山形市における措置> 介護保険システムは情報提供ネットワークとは直接接続しない。 <中間サーバー・ソフトウェアにおける措置> ① 情報提供の要求があった際には、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する機能が備わっている。 ② 情報提供ネットワークシステムに情報提供を行う際には、照会内容に対応した情報のみを自動で生成して送付する機能が備わっている。また、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け取ってから提供する機能が備わっている。これらの機能により、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。 ③ 機微情報(DV支援対象者情報等)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することで、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 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、操作内容が記録されるため、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。	
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	＜山形市における措置＞ 介護保険システムは情報提供ネットワークとは直接接続しない。 ＜中間サーバー・ソフトウェアにおける措置＞ ① 情報提供ネットワークシステムに情報を送信する際は、情報が暗号化される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、操作内容が記録されるため、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・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 中間サーバーと地方公共団体等との間については、VPN(仮想プライベートネットワーク)等の技術を利用し、地方公共団体等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・プラットフォームの事業者及びクラウドサービス事業者が、特定個人情報にはアクセスができないよう管理することで、不適切な方法での情報提供を行えないようにしている。	
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		
リスクに対する措置の内容	＜山形市における措置＞ 誤った相手へ提供・移転しないように、職員は、情報ネットワークと接続する管理されたネットワークを用いる。 ＜中間サーバー・ソフトウェアにおける措置＞ ① 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、照会内容に対応した情報のみを自動で生成して送付する機能が備わっている。また、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け取ってから提供する機能が備わっている。これらの機能により、誤った相手へ特定個人情報を提供するリスクに対応している。 ② 情報提供データベースへ情報が登録される際には、決められた形式のファイルであるかをチェックする機能が備わっている。また情報提供データベースに登録された情報の内容は端末の画面で確認することができる。これらにより、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内の副本データを既存業務システム内の正本データと照合するためのデータを出力する機能を有しており、提供する特定個人情報に誤りがないか確認することができる。 (※)特定個人情報を副本として保存・管理する機能。	
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
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		
＜山形市における措置＞ 情報提供ネットワークシステムとの全ての連携(接続)は、中間サーバが行う構成となっており、情報提供ネットワークシステムは、本市の各業務システムに直接接続はできない。 ＜中間サーバ・ソフトウェアにおける措置＞ ① 中間サーバの職員認証・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。 ＜中間サーバ・プラットフォームにおける措置＞ ① 中間サーバと既存システム、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・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・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・プラットフォームの保守・運用を行う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。		

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		<山形市における措置> ・当市では、高度なセキュリティを用いたサーバー内にデータとして、入退室管理を行っているセキュリティロックの設置した部屋に保管する。サーバーへのアクセスはID/パスワード認証が必要となる。不正アクセスを防止するためにアクセス制御機能として、ユーザーIDによる識別とパスワードによる認証、さらに認証したユーザに対する権限機能により、そのユーザーがシステム上での利用制限することで、ログイン、処理権限の付与、ログ監視を行う。 ・LGWAN接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ・外部記憶媒体については、限定されたUSBメモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 ・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。 ・保有する必要がなくなった届出書等は、確実に、かつ、速やかに廃棄し、又は消去を行う。 <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。 ②ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ③日本国内でデータを保管している。 <申請管理システムにおける措置> ①申請管理システム及び連携サーバについては、電子計算機室等の管理区域に設置しており、入室管理及び監視カメラの設置、などの物理的対策を講じている。 ②申請管理システムに接続可能な端末については、端末本体にデータが残らないよう対策をしている。 ③LGWAN系ネットワークとマイナンバー利用事務系ネットワークの間にDMZを設け、申請管理システムから外部への直接通信を遮断することにより、安全を確保している。また、境界FWや連携サーバで外部接続先との通信を制限している。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ①クラウド事業者が保有・管理する環境(日本国内)に設置し、クラウド事業者による設置場所への入退室記録管理及び施錠管理をすることでリスクを回避する。クラウド事業者は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、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ものを選定し、「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ものとする。 ②クラウド環境にアクセスできる運用・保守拠点では、以下の対策方針に則り運用保守事業者が保守拠点への対策を講じている。 <通信のなりすまし防止> ・介護情報基盤に接続可能なセキュリティ区画の分離、入退室管理を行う。 ・情報システムの機器番号等による接続機器の識別を行う。 <不正プログラムの感染防止> ・OS標準のマルウェア対策機能を利用し、運用保守端末の不正プログラムを検出する。

		<不正プログラム対策の管理> ・OS標準のマルウェア対策機能を利用し、運用保守端末の不正プログラム対応状況を一元管理する。 <構築時の脆弱性対策> ・最新のセキュリティパッチを適用する。 <運用時の脆弱性対策> ・最新のセキュリティパッチを自動適用する。 <ログの蓄積・管理> ・運用保守端末の操作ログを収集する。 <時刻の正確性確保> ・クラウドサービスが提供している時刻同期のサービスを時刻同期元とする。 <情報の物理的保護> ・運用保守端末への対策として下記を実施する。 －端末の離席対策(自動スクリーンロック) －端末のワイヤーロック －記録装置のパスワードロック、暗号化 －データ消去ソフトや物理的破壊による情報の完全廃棄 ・セキュリティ区画への対策として下記を実施する。A268:AH284 －携帯電話、メモリデバイス等の持ち込みの監視及び制限 －物品持ち出し管理 <侵入の物理的対策> ・介護情報基盤に接続可能なセキュリティ区画の分離、入退室管理を行う。 <外部記録媒体を利用する場合の保管・消去に係るリスク対策> ・作業に用いる外部記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる外部記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。
⑥技術的対策		[十分にしている] <選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分に行っていない
		<山形市における措置> LGAWAN接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 <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。 <ガバメントクラウドにおける措置> ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。))に規定する「ASP」をいう。以下同じ。又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。))は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、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。

	具体的な対策の内容	⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、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。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 ＜介護情報基盤を活用した情報連携に係る介護保険事務における追加措置＞ 特定個人情報の適正な取扱いに関するガイドラインの特定個人情報に関する安全管理措置のうち、システム化に関わる「技術的安全管理措置」に沿って、特定個人情報の保護措置を行っている。 ＜技術的安全管理措置＞ ・アクセス制御 —ユーザアカウント権限の制御を行っている。 —外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離している。 —情報の種別に応じた格納領域の分割を行っている。 ・アクセス者の識別と認証 —クラウドサービスのリソースへのアクセス権を一時的に付与するサービスやクラウドサービスのリソースへの操作を許可または拒否する権限を定義するサービスを活用した認可、OS等による認可でアクセス者の識別を行っている。 ・外部からの不正アクセス等の防止 —ウイルス/マルウェア対策・標的型攻撃対策・IDS/IPS・改ざん検知を行い、ネットワークへの不正なアクセスの防止、不正プログラムへの対策を行う。 —Webアプリケーションへの不正アクセスを防止する。 —セキュリティ設計やセキュアコーディング等のセキュリティ対策を実施した上で、本システムの稼働前にセキュリティの専門家によるセキュリティ診断（ペネトレーションテスト等）を実施し、セキュリティ対策が十分行われていることを確認している。 —ログ監査を行い不正アクセスを検知する。 ・漏えい等の防止 —業務データの暗号化については、キーポリシーによる柔軟なアクセス制御、およびクラウドサービス利用終了時に暗号化消去によるデータの完全廃棄を行うことを目的として、原則ユーザーが独自に作成、管理、制御する暗号化キーを使用し、データの暗号化を行っている。 —通信経路の暗号化を行っている。 —情報の種別に応じた格納領域の分割を行っている。 ・データの遠隔地保管 —大阪リージョンにバックアップファイルを保管する。
⑦バックアップ	[十分にしている]	＜選択肢＞ 1) 特に力を入れて行っている 2) 十分にしている 3) 十分に行っていない
⑧事故発生時手順の策定・周知	[十分にしている]	＜選択肢＞ 1) 特に力を入れて行っている 2) 十分にしている 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	[発生あり]	＜選択肢＞ 1) 発生あり 2) 発生なし
	その内容	発生日：令和8年4月2日 内容：市の保有する個人情報を扱う委託業務において、受託事業者が保有するファイルサーバーが不正アクセスを受け、個人情報漏えいのおそれが発生した。 影響を受けた人数：56,966人
	再発防止策の内容	・委託先を含めたデータ管理の徹底、不要データの削除確認、監査体制の強化などを進めていく。 ・事故に関わる受託事業者に対して個人情報の適切な取扱いの徹底を指導するとともに、原因究明と再発防止策の報告を求める。

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	生存者の特定個人情報保護ファイルと同様の方法で保管している。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ・特定個人情報の格納領域を分ける。 ・ユーザアカウント権限の制御を行う。 ・外部接続を行うクラウドサービス、バッチ処理等を行うクラウドサービス、データを格納するクラウドサービスでネットワークを分離する。 ・アクセス者の識別を行えるようにする。 ・不正侵入を検知・防御するシステムを導入することで、ネットワーク、Webアプリケーションへの不正アクセスを防止する。 ・ログ監査により、不正アクセスを検知する。 ・データ暗号化、通信暗号化を行う。	
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	・住民登録内の者については住民基本台帳への記載、変更時にシステム間で自動的に連携する。 ・住民登録外の者については、随時本人確認を行い変更があればその都度データを更新する。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 市区町村介護保険システムより異動情報等が連携され、最新化されるため古い情報のまま保管されるリスクはない。	
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	・事務処理上、消去して問題ない情報がどうかを一定期間ごとに確認する(介護保険法等には保管期間の定めがない)。 ・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。 ・内部で定められた保管期間を経過した申請書等紙媒体は、内部の定めに従い廃棄処分する。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> ・特定個人情報は10年で削除する。 ・データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 ・クラウドサービスが提供するユーザーが独自に作成、管理、制御する暗号化キーを削除することで、暗号化されたデータが復元できないようにする。	
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		
<介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 個人情報等が漏えいした場合の対策として、セキュリティポリシーを遵守し、必要な措置を講ずることとしており、緊急時には、緊急連絡先等により対応する。 ①情報システム担当者にて事案を確認 ②情報セキュリティ管理者(又は情報セキュリティ責任者)に連絡・報告、応急処置等の指示 ③最高情報セキュリティ責任者(又は情報セキュリティ統括責任者)・情報セキュリティ委員会に報告 ④事実関係の調査、原因の究明及び影響範囲の特定を行う ⑤影響を受ける可能性のある本人への連絡及び関係する機関等へ連絡・対応指示 ⑥個人情報等を漏えいさせた医療保険者等の制度所管省庁(厚生労働省、財務省、総務省、文部科学省)及び個人情報保護委員会への報告 ⑦事実関係、再発防止策等の公表		

IV その他のリスク対策 ※

1. 監査		
①自己点検	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
具体的なチェック方法	<山形市における措置> 情報セキュリティに関する自己点検を年に1回実施する。 特定個人情報の取扱いに関する自己点検を年に1回実施する。 <中間サーバ・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・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、定期的に自己点検を実施することとしている。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、必要な自己点検を行う。	
②監査	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的な内容	<山形市における措置> 「情報セキュリティポリシー」及び「山形市の保有する個人情報の適切な管理のための措置に関する要領」に基づく監査を定期的または必要に応じて実施する。 <中間サーバ・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・プラットフォームについて、定期的に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。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、必要な監査を行う。	
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的な方法	<山形市における措置> 情報セキュリティに関する自己点検を実施する。 地方公共団体情報システム機構が主催する情報セキュリティ及び個人情報保護に関する研修を各職員が受講する。 <介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、適切な指導を行う。	
3. その他のリスク対策		
<介護情報基盤を活用した情報連携に係る介護保険事務における追加措置> 情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。		

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	山形市市民生活部市民相談課 〒990-8540 山形市旅籠町2-3-25 TEL023-641-1212 内線254		
②請求方法	指定様式による書面の提出により、開示・訂正・追加・削除・利用停止請求を受付している。 山形市公式ホームページ上で個人情報開示請求について案内している。		
	特記事項		
③手数料等	[無 料] <選択肢> 1) 有料 2) 無料 (手数料額、納付方法: ただし、写しの交付を希望する場合はその実費郵送を希望する場合は) (郵送料を含む。)の負担が必要。		
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	・介護保険事業に関する事務	
	公表場所	https://www.city.yamagata-yamagata.lg.jp/shiseijoho/johokokai/1007071/1011384.html	
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	山形市福祉推進部介護保険課 〒990-8540 山形市旅籠町2-3-25 TEL023-641-1212 内線843		
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。 ・個人情報の保護に関する法令等に従い、適正かつ迅速に対応する。		

VI 評価実施手続

1. 基礎項目評価	
①実施日	
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	
②実施日・期間	
③期間を短縮する特段の理由	
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	
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

[illegible]