

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
87	新潟市 新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務 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

新潟市は、新型インフルエンザ等対策特別措置法による予防接種の実施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低減させるために十分な措置を講ずることにより、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

新潟市長

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	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務
②事務の内容 ※	新型インフルエンザ等が発生した場合に、特定接種や住民に対する予防接種、予診票の発行等を行う。新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務において、情報提供ネットワークシステムを接続し、各情報保有機関が保有する特定個人情報について情報連携を行う。 ＜予診情報・予防接種記録管理／請求支払システム（以下、「予予・請求システムという。」）を活用した情報連携に係る予防接種事務＞ ・本市は、情報連携のため、予予・請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 ・住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 ・医療機関は予防接種時に、医療機関用アプリ等において住民が入力した予診票情報、接種記録の取得/閲覧/入力が可能となる。 ・本市は、医療機関から入力された予診票情報、接種記録の取得及び住民への通知が可能となる。
③対象人数	[30万人以上] ＜選択肢＞ 1) 1,000人未満 3) 1万人以上10万人未満 5) 30万人以上 2) 1,000人以上1万人未満 4) 10万人以上30万人未満

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	新潟市健康管理システム
②システムの機能	○. 予防接種データ管理機能 予防接種対象者抽出、予防接種入力、予防接種連続入力、予防接種結果入力バッチ、接種別一覧、個人別一覧、予防接種履歴管理 ○. 他団体提供用データ(中間サーバー格納用データ)の団体内統合宛名システムへ転送機能 情報提供ネットワークシステムを通じて、他団体へ提供するために作成した中間サーバー格納用データを、団体内統合宛名システムへ送信する。団体内統合宛名システムは、中間サーバー格納用データを中間サーバーへ転送する。また、異動発生時の更新後の情報も同様に中間サーバーへ転送する団体内統合宛名システムへ送信する。 ○. 予予・請求システム連携機能 Public Medical Hubを経由して、住民情報(対象者データ)を提供し、同システムからデジタル予診票や接種記録の情報を受け取る。
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 (団体内統合宛名システム、予予・請求システム) [○] 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2～5

システム2

①システムの名称	ガバクラデータ連携システム
②システムの機能	既存業務システム間における庁内での情報転送を行うための情報連携システムである。 ※情報授受は、業務ごとに予め定義された専用領域を介して、既存業務システムから専用領域へアクセスして情報を取得する。なお、情報はファイル単位で連携する。専用領域は、あらかじめアクセスできるデータを各業務システムごとに制御しているため、各業務システムは許可されていないデータの取得ができない仕組みとなっている。 1. 庁内情報の連携 情報移転システムで作成した庁内移転用データを移転元の専用領域から取得し、移転先の専用領域へデータ転送を行う。 ※庁内移転用データには個人番号が含まれるが、個人番号を利用しない業務システムに対しては個人番号を含まないデータ内容で庁内移転用データを渡す。 2. セキュリティの管理 既存業務システムからのアクセスを制御するため、ID/パスワードの管理を行う。 3. 情報連携記録の管理 情報連携記録の生成・管理を行う。

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 （ 既存業務システム ）
システム3	
①システムの名称	団体内統合宛名システム
②システムの機能	団体内統合宛名システムは、個人番号・宛名コード・統合宛名番号の紐付け管理、及び庁内情報連携等の機能を提供する。 - 番号の管理 統合宛名番号の新規付番、及び個人番号・統合宛名番号・宛名コードの関連付けを行う。 - 統合宛名番号の検索 住所・氏名等を検索条件とした統合宛名番号検索を行う。 - 中間サーバー格納用データの中継 各業務システムにおいて、他団体へ提供するために作成した中間サーバー格納用データを、中間サーバーへ転送する。また、異動発生時の更新情報も同様に行う。 - 情報提供ネットワークシステムとの情報連携 各業務システムからの情報提供ネットワークシステムあて情報照会要求メッセージを中間サーバーへ転送し、情報提供ネットワークシステムからの照会結果を中間サーバーから受け取り、照会元の各業務システムへ転送またはデータを書き込む。 - 職員認証・権限の管理 団体内統合宛名管理システム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限を行う。 - 情報連携記録の管理 情報連携記録の生成・管理を行う。
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 （ 中間サーバー、既存業務システム ）
システム4	
①システムの名称	中間サーバー
②システムの機能	中間サーバーは、情報提供ネットワークシステム・団体内統合宛名システム間のデータ受け渡しをすることで、符号の取得や他情報保有機関間の特定個人情報照会・提供の機能を提供する。 - 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「統一識別番号」とを紐付け、その情報を保管・管理する。 - 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（連携対象）の情報照会及び情報提供受領（照会した情報の受領）を行う。 - 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（連携対象）の提供を行う。 - 各業務システム接続機能 中間サーバーと各業務システム、団体内統合宛名システム及び住民記録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（連携対象）、符号取得のための情報等について連携する。 - 情報提供等記録管理機能 特定個人情報（連携対象）の照会、又は提供があった旨の情報提供等記録を生成し、管理する。 - 情報提供データベース管理機能 特定個人情報（連携対象）を副本として、保持・管理する。 - データ送受信機能 中間サーバーと情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会、情報提供、符号取得のための情報等について連携する。 - セキュリティ管理機能 暗号化／復号機能と、鍵情報及び照会許可照合リスト情報を管理する。 - 職員認証・権限管理機能 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（連携対象）へのアクセス制限を行う。 - システム管理機能 バッチの状況管理、業務統計情報の集計、稼働状態の通知、保管期限切れ情報の削除を行う。

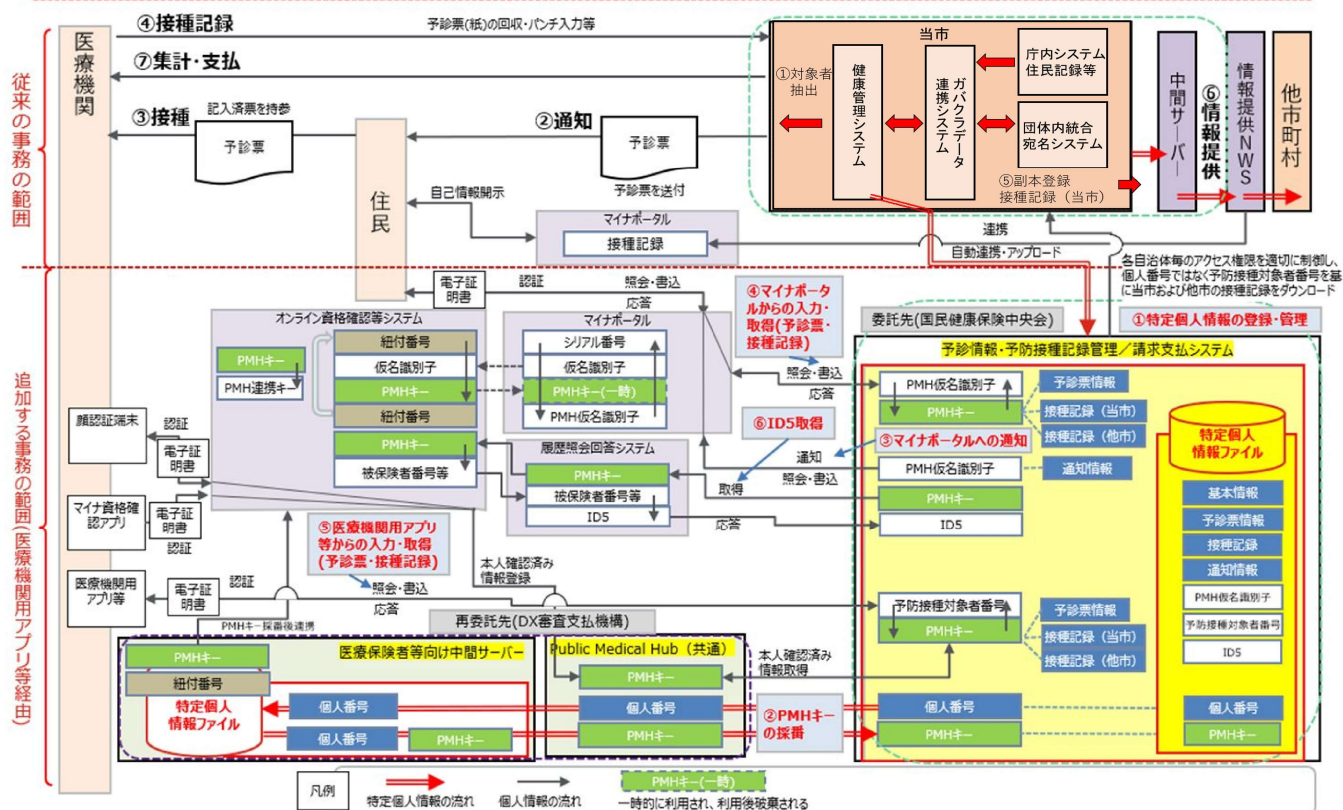
③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☐ その他 ()
システム5	
①システムの名称	予予・請求システム
②システムの機能	①予防接種関連データの登録機能 本市は、健康管理システムからの情報連携又は予予・請求システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予予・請求システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予予・請求システムは、本市で管理している個人番号、対象者情報、予診票情報及び接種記録を予予・請求システムに登録する。また、Public Medical Hubを経由して医療情報基盤・診療報酬審査支払機構（以下、「DX審査支払機構」という。）の医療保険者等向け中間サーバーと連動し、PMHキーを自動採番する。すでにPMHキーが採番済みの個人番号であれば、採番は行わずに既存のPMHキーを利用する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 予予・請求システムは、マイナポータルからの予予・請求システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予予・請求システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナナンバーカードの電子証明書のシリアル番号に紐づくPMH仮名識別子を利用した照会を行う。予予・請求システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐づく接種記録・通知をマイナポータルへ提供する。また、予予・請求システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐づく予診票情報を登録する。 ④情報連携機能（医療機関用アプリ等） ・本人確認情報の格納機能 予防接種対象者が、顔認証端末又はマイナ資格確認アプリを利用してマイナナンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリ等は、予予・請求システムへ本人確認情報を利用した照会を行う。予予・請求システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐づく予防接種対象者番号をキーに予診票情報を医療機関用アプリ等に提供する。また、医療機関が接種記録の入力画面から情報を入力することにより、予予・請求システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐づく接種記録を登録する。 ⑤情報連携機能（履歴照会回答システム） ・識別子の格納機能 予予・請求システムは接種記録等の情報を予防接種DBIに連携し、予防接種DBIにおいて予防接種の有効性・安全性等の調査・研究を行う。予予・請求システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐づけて予予・請求システムに連携する。
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 (健康管理システム、マイナポータル、医療機関用アプリ、電子カルテ等、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム)
3. 特定個人情報ファイル名	
新型インフルエンザ等対策特別措置法による予防接種事業情報ファイル	
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	予防接種法及び新型インフルエンザ等対策特別措置法による予防接種においては、制度上、対象者の確認及び接種履歴や未接種者の把握のため、特定個人情報ファイルを取り扱う必要がある。
②実現が期待されるメリット	予防接種の対象者であることの確認、接種記録の管理等により、未接種者を迅速に把握でき、感染症の発生及びまん延防止につながる。

5. 個人番号の利用 ※	
法令上の根拠	1、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（番号利用法） ・第9条第1項 別表 第126項 2、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律別表の主務省令で定める事務を定める命令（別表省令） ・第67条の3
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	≪情報提供・照会≫ 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第19条第8号に基づく利用 特定個人情報の提供に関する命令第2条の表 第153項
7. 評価実施機関における担当部署	
①部署	保健衛生部保健所保健管理課
②所属長の役職名	保健管理課長
8. 他の評価実施機関	

(別添1) 事務の内容

予防接種事務の概要 全体図

従来の事務では、①～⑦の流れで健康管理システム・中間サーバに情報が登録・連携される。今回利便性の向上のため、予防接種における住民からの予診票入力及び接種記録の取得、医療機関からの予診票取得、接種記録の入力等のオンライン化を事務の範囲に追加する。追加する事務では、①②の流れで、情報が連携され、住民がマイナポータル経由、医療機関が医療機関用アプリ等経由でオンライン化(③④⑤⑥)が実現できる。()部が評価対象の事務、()部については医療情報基盤・診療報酬審査支払機構(DX審査支払機構)がPIAを実施するため評価対象外)



(備考)

<従来の事務>

(1) 予防接種情報の管理事務

- ・予防接種委託医療機関から提出された予防接種券・予診票をもとに対象者の確認を行い、予防接種の履歴データを入力する。
- ・情報提供ネットワークシステムを介し、他自治体から転入者等の予防接種の履歴データを入手する。また、情報提供ネットワークシステムを介し、予防接種の履歴データを他自治体に提供する。

(2) 接種勧奨事務

- ・予防接種未完了者に個別勧奨を行う。

(3) 予防接種記録の提供

- ・住民からの依頼により接種記録を提供する。

<追加する事務>

① 特定個人情報の登録・管理

- ・本市は、健康管理システムからの情報連携又は予予・請求システム画面への直接入力により、予予・請求システムにおいて対象者の個人番号を含む対象者情報の登録を行う。(LGWAN回線等経由)
- ・本市は予予・請求システムから接種記録等、必要な情報を自動連携またはダウンロードし、健康管理システム等への取込を行う。
- ・予予・請求システムへ登録された個人情報へのアクセスは適切に制御される。

② PMHキー採番

- ・予予・請求システムは、Public Medical Hubに対して個人番号を連携することで、オンライン資格確認等システムと予予・請求システムが連動するためのPMHキーの採番処理を依頼する。
- ・Public Medical Hubは、医療保険者等向け中間サーバを経由しPMHキーを採番して予予・請求システムに回答する。
- ・医療保険者等向け中間サーバは、PMHキーと個人番号を紐付けて、PMHキーと紐付番号を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、紐付番号をキーに仮名識別子とPMHキーを紐付けて、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、仮名識別子、PMHキーと紐付けて、予予・請求システムに連携する。(連携後、マイナポータル上からPMHキーは削除される。)以降、③④⑤⑥が可能となる。

③マイナポータルへの通知

・予予・請求システムからマイナポータル経由で住民向けの通知を行うため、本市は予予・請求システムを利用してマイナポータルに識別子(PMH仮名識別子)と通知情報を登録する。

④マイナポータルからの入力・取得(予診票・接種記録)

・住民は、マイナポータル経由で予予・請求システムへの予診票の事前入力や、予予・請求システムから接種記録や通知情報を閲覧/取得する。

⑤医療機関用アプリ等からの入力・取得(予診票・接種記録)

・医療機関が医療機関用アプリ等を利用し、接種時に住民からマイナンバーカードによる本人確認を経て、事前入力された予診票及び接種記録の閲覧/取得/入力を行う。

⑥ID5取得

・予防接種DBへの接種記録等の連携時に個人を特定する識別子情報として、予予・請求システムが履歴照会回答システム経由でID5を取得する。

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	
新型インフルエンザ等対策特別措置法による予防接種事業情報ファイル	
2. 基本情報	
①ファイルの種類 ※	システム用ファイル ☐ システム用ファイル ☐ 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 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上
③対象となる本人の範囲 ※	☐ 必要性 新型インフルエンザ等対策特別措置法に規定する予防接種の対象者 新型インフルエンザ等対策特別措置法及び関係法令において接種記録の管理が必要とされること、また、個人の接種履歴を管理することにより、未接種者を正確に把握し、勧奨を行うために必要となる。
④記録される項目	10項目以上50項目未満 ☐ 10項目未満 ☐ 10項目以上50項目未満 ☐ 50項目以上100項目未満 ☐ 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、氏名の振り仮名、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 (予防接種記録情報)
その妥当性	①個人番号、その他識別情報(PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5): 対象者を正確に特定するために保有 ②5情報、連絡先、その他住民票関係情報: 正確な本人特定のため、予防接種券・予診票に記入された情報と突合するために保有、また接種勧奨に使用するために保有 ③その他(予防接種記録情報): 予防接種事務の適切な実施にあたり必要となる情報を管理し、予予・請求システムが、外部と情報連携するために必要
全ての記録項目	別添2を参照。
⑤保有開始日	令和3年6月1日
⑥事務担当部署	保健衛生部保健所保健管理課

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 （ 市民生活部市民生活課 ） [☐] 行政機関・独立行政法人等 （ ） [☐] 地方公共団体・地方独立行政法人 （ ） [☒] 民間事業者 （ 医療機関 ） [☒] その他 （ DX審査支払機構 ）
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 （ Public Medical Hub、医療機関用アプリ等、マイナポータル ）
③入手の時期・頻度	住民情報は、住民登録に係る申請受付時に随時入手する。 予防接種情報は、市民が接種する都度、月1回定期的に医療機関から医師会を通じて予防接種券・予診票を受領し入手する。 ＜予予・請求システムを活用した情報連携に係る予防接種事務＞ ・予予・請求システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・国が予予・請求システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本市が個人情報を入手し、予予・請求システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等又は医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予予・請求システムにおいて個人番号と結びついて特定個人情報となる。
④入手に係る妥当性	個人を特定し、適正に予防接種情報を管理する必要がある。 ＜予予・請求システムを活用した情報連携に係る予防接種事務＞ (PMHキー採番処理依頼時に入手される特定個人情報) ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 (その他:個人情報として入手し、予予・請求システムにおいて個人番号と結び付き特定個人情報となる情報) 本市が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入手し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証(本人確認)の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。
⑤本人への明示	本人から入手する情報については、使用目的を本人に明示したうえで入手する。 また、庁内連携ネットワークシステムからの入手については、番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表 第153項にて明示されている。(新型インフルエンザ等対策特別措置法による予防接種の実施に関する関する事務) ＜予予・請求システムを活用した情報連携に係る予防接種事務＞ 本人又は本人の代理人から入手する情報については、利用目的を明示した上で入手している。マイナポータル等では、本人又は本人の代理人が画面に表示された利用目的を確認することによって、本人確認とする。

⑥使用目的 ※		予防接種事業を実施するうえでの本人確認を行うため、本特定個人情報ファイルにおいて住民の情報を保有する。予防接種履歴を入手・保管し、適正な事務を行う。	
	変更の妥当性		
⑦使用の主体	使用部署 ※	保健衛生部保健所保健管理課、各区役所健康福祉課、各地域保健福祉センター	
	使用者数	[100人以上500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 ※		(1) 予防接種情報の管理事務 予防接種委託医療機関から提出された予防接種券・予診票に記載された者が新型インフルエンザ等対策特別措置法に規定する接種対象者であるか確認し、予防接種履歴を入力・管理する。 他自治体保管の予防接種履歴を入手し、本市保管の予防接種履歴を他自治体に提供する。 (2) 接種勧奨事務 予防接種についての情報を個別勧奨をとおしてお知らせする。 ＜予予・請求システムを活用した情報連携に係る予防接種事務＞ ・情報連携のため、本市は、予予・請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ・登録後、予予・請求システムは、Public Medical Hubに対してオンライン資格確認等システムと予予・請求システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予予・請求システムに応答する。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予予・請求システムで共有されることで予予・請求システムからマイナポータルへの通知、マイナポータルや医療機関用アプリ等から予予・請求システムの予診票情報及び接種記録の取得/閲覧/入力等といった情報連携が可能となる。	
	情報の突合 ※	予防接種券・予診票に記入された予防接種番号、住所、氏名、生年月日等と突合し、新型インフルエンザ等対策特別措置法による接種対象者かどうか確認する。	
	情報の統計分析 ※	個人番号を用いた統計分析は行わない。 ＜予予・請求システムを活用した情報連携に係る予防接種事務＞ 特定の個人を判別するような情報の統計や分析は行わない。	
	権利利益に影響を与え得る決定 ※	新型インフルエンザ等対策特別措置法による接種対象者であるかの決定を行う。	
⑨使用開始日		令和3年6月1日	

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		委託する <選択肢> 1) 委託する 2) 委託しない (2) 件
委託事項1		健康管理システム運用保守
①委託内容		健康管理システム運用業務(システム資源の維持管理、障害復旧対応等)
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 ※	「2、③対象となる本人の範囲」と同上。
	その妥当性	保守運用業務の範囲は、ハードウェア、ソフトウェア、運用業務としての電算処理にわたり、システム上保有する全てのファイルを取り扱うため
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 ○ その他 (庁舎内でシステムを直接操作)
⑤委託先名の確認方法		新潟市情報公開条例に基づく公開請求により確認することができる。
⑥委託先名		日本コンピューター株式会社
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	契約時に再委託申請書・作業従事者名簿・秘密保持誓約書を提出させ、委託先との契約に含まれている「情報セキュリティの要求事項」「個人情報取扱特記事項」について、再委託先にも遵守を義務付けている。
	⑨再委託事項	上記委託内容と同様。

[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 () 件 [☐] 移転を行っている () 件 [☐] 行っていない
提供先1	番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表に定める情報照会者
①法令上の根拠	番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表
②提供先における用途	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって主務省令で定めるもの
③提供する情報	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務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] <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	「2、③対象となる本人の範囲」と同上
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	情報提供ネットワークシステムを通じて特定個人情報の提供依頼のあった都度

①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[] ＜選択肢＞ 1) 1万人未満 2) 1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	
⑥移転方法	[] 店内連携システム [] 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	

6. 特定個人情報の保管・消去														
①保管場所 ※		＜新潟市における措置＞ 申告書及び届出書等の紙媒体については、許可された者以外入室することのできない執務室内にて保管しており、取り扱いも執務室内に限定している。 窓口業務等を行う部署においては、紙媒体やオンラインの画面が第三者に見えないような配慮を徹底している。 ＜ガバメントクラウド(健康管理システム)における措置＞ ・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。 ・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。 ＜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保管期間	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 colspan="3">10) 定められていない</td> </tr> </table> [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		
	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	予防接種法施行規則第4条において、5年間保管すると定められているが、接種記録確認等の事務のため長期間保管する必要がある。												
③消去方法		＜新潟市における措置＞ ・サーバー上のデータは、削除者等の他業務に影響のないデータについて、システム内で定期的に削除処理を実行する。 ・紙媒体は、文書規定で定められた保存年限を経過したものについて、溶解廃棄処分を行う。 ＜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。 ＜予予・請求システムを活用した情報連携に係る予防接種事務＞ ・本市の領域に保管されたデータのみ、予予・請求システムを用いて消去することができる。 ・本市の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。												
7. 備考														

(別添2) 特定個人情報ファイル記録項目

<基本情報>

1 健診・予防接種番号(宛名コード)、2 カナ氏名、3 生年月日、4 性別、5 漢字氏名、6 年齢、7 郵便番号、8 住所、9 電話番号

<新型インフルエンザ>

1 事業番号、2 期・回数コード、3 予防枝番、4 年度、5 事業予定連番、6 受診日、7 受診会場、8 受診種別コード、9 登録日、10 接種医療機関番号、11 接種医療機関、12 接種区分コード、13 Lot番号、14 接種量、15 印刷コード、16 印刷日、17 予診医医療機関番号、18 予診医番号、19 接種医医療機関番号、20 接種医番号、21 予診医職員ID、22 予診医職員枝番、23 接種医職員ID、24 接種医職員枝番、25 ワクチンメーカー名コード、26 予診理由区分コード、27 備考、28 入力窓口、29 旧市町村コード、30 登録区

<予予・請求システムを活用した情報連携に係る予防接種事務における追加の記録項目>

(1)対象者情報

- ・個人番号
- ・PMHキー
- ・PMH仮名識別子
- ・基本5情報(カナ・氏名・住所・生年月日・性別)
- ・保護者氏名
- ・自治体コード
- ・自治体業務ID
- ・連携ファイル名
- ・連携日時
- ・連携処理ステータス/エラー内容
- ・制御フラグ(リカバリー/不開示/閲覧停止)
- ・変更区分
- ・消除の異動日
- ・その他管理番号・ID等(予防接種対象者番号)
- ・その他区分等(接種対象者区分/減免区分)

(2)ユーザー情報

- ・機関マスタID
- ・機関ユーザーID
- ・メールアドレス
- ・ユーザー氏名
- ・ユーザー区分
- ・ユーザー権限ID
- ・個人番号閲覧可能フラグ
- ・ユーザー削除フラグ

(3)予診票情報

- ・項目ID
- ・管理ID
- ・更新日時
- ・回答ID
- ・回答内容
- ・回答処理ステータス
- ・回答日時
- ・接種不可フラグ
- ・予防接種設定ID
- ・予防接種管理ID
- ・組み合わせ番号
- ・強制失効日
- ・勧奨情報(ルールID、勧奨日)

(4)予防接種記録情報

- ・予防接種記録ID
- ・予防接種管理ID
- ・接種日
- ・接種同意フラグ
- ・医療機関コード
- ・医師名
- ・実施場所
- ・実施区分
- ・接種区分
- ・GTINコード
- ・ワクチンメーカー名
- ・ワクチン名(ワクチン一般名/ワクチン通称/ワクチン販売名)
- ・ロット番号
- ・接種量
- ・接種部位
- ・接種方法
- ・ワクチン有効期限
- ・要注意接種フラグ
- ・特別の事情
- ・海外接種フラグ
- ・更新日時
- ・最新/削除フラグ
- ・その他区分等(接種対象者区分/減免区分)

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		
新型インフルエンザ等対策特別措置法による予防接種事業情報ファイル		
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	<事務における措置> 本人等より入手する際には、身分証明書の提示を受け、必ず本人確認を行う。 <ガバクラデータ連携システムにおける措置> ガバクラデータ連携システムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。 <団体内統合宛名システムにおける措置> 団体内統合宛名システムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・医療機関の受付窓口で本人確認の後、医療機関用アプリ等又は顔認証端末でマイナンバーカードを利用した認証により本人の情報のみが対象者として連携される。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、マイナンバーカードを利用した認証により、本人以外からの情報の入力を防止する。 ・既存事務において本人確認を行った個人番号を健康管理システムから予予・請求システムに連携し、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	<健康管理システムにおける措置> ①利用者によって利用可能な機能を制限し、不必要な情報の入手を抑止している。 <ガバクラデータ連携システムにおける措置> ①情報移転元システムが作成したデータをガバクラデータ連携システムに格納し、既存業務システムからデータにアクセスして情報を取得するシステムであるが、情報移転対象者以外の情報が混入することはない。 ②あらかじめアクセスできるデータを各業務システムごとに制御しているため、既存業務システムは許可されていないデータの取得ができないことを担保している。 ③ガバクラデータ連携システムシステムを利用する各業務システム各々にID／パスワードを設定することで、他システム用の情報データへのアクセスを阻止している。 <団体内統合宛名システムにおける措置> 団体内統合宛名システムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予・請求システムへは、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（PMHキーと個人番号）のみのみが返却されるようシステムの的に制御している。 ・医療機関から医療機関用アプリ等を介して入力される際は、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のみが連携されるようシステムの的に制御している。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、定められたデータ項目のみのみが入力されるようシステムの的に制御している。 ・生年月日等をチェックすることで紐付け誤りを防止する機能（以下、「紐付け誤り防止機能」という。）により、誤った情報が紐付けられるリスクを低減する。	
その他の措置の内容	操作ログを収集し、不正な操作による対象者以外の情報入手を防ぐ。	
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	<健康管理システムにおける措置> ①ID／パスワードに加え、生体認証を実施しており、あらかじめ承認された利用者以外の情報入手を抑制している。 <ガバクラデータ連携システムにおける措置> ①ガバクラデータ連携システムを利用する既存業務システム各々にID／パスワードを設定することで、あらかじめ承認されたシステム以外の情報入手を阻止している。 ②データ授受の動作記録を残すことで、不適切な入手を阻止している。 <団体内統合宛名システムにおける措置> ①接続システムの認証及び団体内統合宛名システム接続端末での職員認証等の機能を備えており、あらかじめ承認されたシステム・職員以外の情報入手を抑制している。 ②団体内統合宛名管理システムへのログイン及びデータ授受の動作記録を残すことで、不適切な入手を抑制している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ①医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予・請求システムへは、システム自動処理により、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（PMHキーと個人番号）のみが返却されるようシステムの的に制御している。 ②予予・請求システムのデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。 ③紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。
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	個人番号カード、または通知カードと身分証明書の提示を受け、必ず本人確認を行う。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 予予・請求システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。 紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。
個人番号の真正性確認の措置の内容	個人番号カード、または通知カードと身分証明書の提示を受け、既に登録された宛名情報の基本4情報と差異がないか比較することにより、個人番号の真正性を確認する。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 予予・請求システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。 紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。
特定個人情報の正確性確保の措置の内容	・上記の通り、入手の各段階で、本人確認とともに、特定個人情報の正確性を確保している。 ・職員にて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。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。
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4： 入手の際に特定個人情報情報が漏えい・紛失するリスク		
リスクに対する措置の内容	＜紙媒体における措置＞ 紙媒体の特定個人情報については、鍵付きの保管スペースで保管している。 ＜電子データにおける措置＞ 特定個人情報に記載された電子データについては、電磁的記録媒体は極力使用しないこととしている。使用する場合は業務時間外の使用を制限しており、鍵付き保管スペースより取り出し、使用終了後は速やかに復元不可能な形式でデータを消去し、保管スペースに返却するとともに、使用記録を残す。また、電磁的記録媒体は許可なく接続しただけでは使用不可となるよう端末に制限がかかっている。 ＜ガバクラデータ連携システムにおける措置＞ システム間は専用回線で接続されており、それ以外への接続はできないシステムとなっている。また、接続された特定機器のみとの通信とすることで、接続システム外への漏えい・紛失を防いでいる。 ＜団体内統合宛名システムにおける措置＞ 団体内統合宛名システムは、中間サーバーや既存業務システムとの接続に専用回線を用いているため、外部に漏れることはない。また、団体内統合宛名システムと団体内統合宛名システム接続端末間の通信を暗号化し、漏えい・紛失を防いでいる。 ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 予予・請求システムとDX審査支払機構の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 健康管理システムは、予予・請求システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。	
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		
—		

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	<団体内統合宛名システムにおける措置> 団体内統合宛名システムでは、情報を利用する事務と事務に必要な情報項目の対応付けをあらかじめ設定しており、設定を超えた範囲の情報を提供することは不可能である。また、システム連携する既存業務システムごとにアクセス制御も行う。	
事務で使用するその他のシステムにおける措置の内容	<健康管理システムにおける措置> 庁内の他システムからアクセスできないよう適切なアクセス制限を講じており、目的を超えた紐付けは行われないようにしている。 <ガバクラデータ連携システムにおける措置> 情報移転元システムが作成したデータを情報移転先システムに中継するシステムであり、移転する情報以外の情報利用はできない。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・予予・請求システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予予・請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予予・請求システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。	
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	・対象既存業務システムを利用する端末は、該当職員個人のパスワードによる認証を行っている。 ・対象既存業務システムを利用する職員を特定し、職員毎に利用可能な機能を制御(アクセス制御)している。 ・認証はID／パスワードに加え、静脈認証も実施しており、権限を有しない者の利用を制限している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市は、予予・請求システムのアクセス権限を管理する管理者を定める。 ・予予・請求システムのログインはユーザID・パスワードで行う。 ・予予・請求システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予予・請求システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・健康管理システムから予予・請求システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。	
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	<健康管理システムにおける措置> ○アクセス権の発行 健康管理システムを所管している所属長に対し、アクセス権を必要とする所属の長が下記の内容を記載した申請を行い、当該既存業務システムを所管している所属長がアクセス権限を設定する。 ・必要なアクセス権限の種類 ・アクセス権限が必要な期間 ・利用する業務名及び業務概要 ・利用目的及び必要とする理由(法令根拠等) ・申請課及び利用課の所属長及び利用者 ○アクセス権の失効 アクセス権は、年度末または必要な期間の満了日に自動削除される。 また、アクセス権が必要な期間の満了日前に異動若しくは退職した場合には手動で削除する。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・予予・請求システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・管理者は、アクセス権限の管理表を作成し、申請者に対して管理表に基づき適切なアクセス権限を付与する。 ・本市において、人事異動や退職等があった際は、異動情報に基づき、不要となったアクセス権限を管理し、失効させる。	
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	<健康管理システムにおける措置> ・権限の妥当性を確認した上で、各業務を所管する事業課からの依頼に応じて必要な権限を付与している。 ・不正アクセスを分析するために、操作履歴の記録を保管する。 ・管理者による定期的な閲覧を実施する。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・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。 ・管理者が定期的に管理表を確認し、必要に応じて見直しを行う。
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	<健康管理システムにおける措置> 特定個人情報へのアクセス記録は、システムがアクセスログ(日時、利用者、利用端末、利用情報)として全件記録している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 本市は、システム上の操作のログを取得し、操作ログを定期的に確認する。
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		従業者が利用可能なシステムは、それぞれの業務分担に応じ制限されており、不必要な情報にはアクセスできない措置を講じている。 新潟市情報セキュリティポリシーにおいて職務以外の目的に使用してはならないと定めており、職員を対象に情報セキュリティに関する研修を行うとともに、コンプライアンス研修によりデータを取り扱うことに対する倫理研修を合わせて実施する。また、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、事務外での使用を防止する。 委託業務については、委託先との契約により、委託業者が従業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。本市は、当該教育の実施について履行確認を行う。再委託先においても同様の取扱とする。
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		ファイルが不正に複製できないようにするため、下記のとおり措置している。 ・特定個人情報については端末に業務用データ出力できない仕様となっている。 ・許可なく電磁的記録媒体を接続した場合に使用不可となるよう端末を制御している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・健康管理システムから特定個人情報を抽出したCSVファイルを予予・請求システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・健康管理システムから予予・請求システムへの特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線(LGWAN又はその他の閉域網回線)を利用した接続のみが認められる。 ・予予・請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。
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		
・端末画面は来所者から見えないようにする。 ・特定個人情報が表示された画面のハードコピーは原則禁止とする。		

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

＜健康管理システムにおける措置＞

委託契約を締結しようとするときは、委託者の情報資産を管理するための組織体制、方法等について確認を行い、加えて、情報資産の秘密を保持する等のため、その代表者及び従事者から情報資産の適正な取扱いに関する誓約書を提出させている。

＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞

本市は、予予・請求システムの利用・情報連携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新潟県国保連合会に委託し、新潟県国保連合会は国保中央会に再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、国保中央会の設備、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

＜健康管理システムにおける措置＞

- ・特定個人情報ファイルの閲覧者・更新者を限定するため事前に委託作業者の名簿を提出させる。
- ・特定個人情報ファイルへのアクセスを行う場合、事前に申請許可された者以外はアクセスできないよう制御し、ユーザID／パスワードにより認証している。

＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞

- ・本市がアクセス権限の管理状況を確認できる。
- ・本市は、アクセス権限を付与する者を必要最小限に限定する。
- ・本市は、アクセス権限を付与する範囲を必要最小限に限定する。
- ・本市は、アクセス権限を付与した者と権限の範囲を適切に管理する。

※特定個人情報に係るアクセス権限は、再々委託先（PMHキー採番や運用保守）のみに付与される。

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

＜健康管理システムにおける措置＞
特定個人情報ファイルにアクセスする場合は、作業者及び作業内容を記載した申請書を提出させ、その全ての申請書を保管する。

＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞
・予予・請求システムは特定個人情報の取り扱いのログを保存し、本市は特定個人情報に係る操作のログを閲覧・出力できる。
※再々委託先（PMHキー採番や運用保守）に係る特定個人情報の取扱いログに限られる。

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
の内容及びルール遵守
の確認方法

＜健康管理システムにおける措置＞
委託先から他社への提供を禁止する旨を契約書に明記している。また、委託先でのデータの保護状況について、必要に応じ委託者が検査を実施できる旨を契約書に明記している。

＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞
・委託先(再委託先及び再々委託先を含む。)から他者への提供は行わない。
・本市は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)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の内容及びルール遵守の確認方法

＜健康管理システムにおける措置＞

委託先の情報資産の保護体制、方法等をあらかじめ調査及び確認するとともに、秘密を保持する等のため、その代表者及び従事者から誓約書を撤収している。加えて、提供するデータの指示された目的以外への使用及び第三者への提示を禁止する旨を契約書に明記している。また、委託先でのデータの保護状況について、必要に応じ委託者が検査を実施できる旨を契約書に明記している。

＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞

- ・委託先（再委託先及び再々委託先を含む。）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。
- ・本市は委託契約に基づき、委託先（再委託先及び再々委託先を含む。）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 ルール内容及び ルール遵守の確認方法	[定めている] ＜選択肢＞ 1) 定めている 2) 定めていない ＜健康管理システムにおける措置＞ 委託契約書に、以下の措置をとる旨を規定している。 ・個人情報を記録した（ハードウェアを含む。）媒体等を廃棄する場合は、電磁的記録の消去、又は記録装置の破砕等を行い、個人情報の復元ができない状態にすること。 ・個人情報を記録した（ハードウェアを含む。）媒体等の破砕等を外部の者に依頼する場合は、情報の消去に係る確認書の提出を受けること。 ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託契約終了後は予予・請求システムに保管していた全ての特定個人情報を国保中央会が消去する。 ・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、本市は消去について国保中央会から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 規定の内容	[定めている] ＜選択肢＞ 1) 定めている 2) 定めていない ＜健康管理システムにおける措置＞ ・データの秘密保持に関する事項 ・再委託の禁止又は制限に関する事項 ・情報資産の指示された目的外への使用及び第三者への提示の禁止に関する事項 ・データの複写及び複製の禁止に関する事項・事故発生時における報告義務に関する事項 ・情報資産の保護状況の検査の実施に関する事項 ・データの授受及び搬送に関する事項 ・委託を受けた事業者等におけるデータの保管及び廃棄に関する事項 ・その他データの保護に関し必要な事項 ・前記各事項の定め違反した場合における契約解除等の措置及び損害賠償に関する事項 ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 新潟県国保連合会及び国保中央会は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員の明確化 ・従業員に対する監督・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 具体的な方法	[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 ＜健康管理システムにおける措置＞ 業務委託等契約と同様に、再委託先の情報資産の保護体制、方法等をあらかじめ調査及び確認するとともに、秘密を保持する等のため、その代表者及び従事者から誓約書を徴収している。 ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・再々委託の相手方は、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。 ・国保中央会が、再々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、再々委託の相手方によるセルフチェックを基本とし、必要に応じて国保中央会が訪問確認を行う。 ・点検後に改善事項がある場合は、国保中央会が改善指示及び改善状況のモニタリングを行う。 ・国保中央会は、点検結果について新潟県国保連合会及び本市に年1回報告を行う。

その他の措置の内容	<予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業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。	
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 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		
リスクへの対策は十分か	[]	<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		
リスクへの対策は十分か	[]	<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		

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	<健康管理システムにおける措置> 健康管理システムへのログインは、生体認証を必要とする利用者登録により制限されており、特定の権限者以外は情報照会・提供ができず、さらに、情報照会・情報提供記録をデータベースに逐一保存することで、不適切な方法で特定個人情報がやりとりされることを防止する。 <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用照合リストを管理する機能。 <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。
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	<健康管理システムにおける措置> ・誤った情報を提供・移転してしまうリスクへの措置 提供・移転する情報のチェックを行い、誤った情報が作成されないことをシステム上で担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 団体内統合宛名システムでは、番号利用法に基づき認められる情報のみ、認められた相手にしか移転できないよう、システムの仕組みとして担保されている。 <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。
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	
<新潟市における措置> 本市では、情報提供ネットワークシステムとの全ての連携(接続)は、中間サーバー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側から、本市の業務システムへのアクセスはできない。 <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。	

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	<新潟市における措置> ・端末、電磁的記録媒体、紙媒体については、許可された者以外入室することのできない執務室内にて保管しており、取り扱いも執務室内に限定している。 ・執務室が無人になる際には、施錠管理を徹底している。 ・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。 <ガバメントクラウド(健康管理システム)における措置> ・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。 ・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。 <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管・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。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 予予・請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「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すクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスの利用

⑥技術的対策	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な対策の内容	<新潟市における措置> ・特定個人情報ファイルにアクセスする業務用端末は、端末側に業務データが残らない方式を採用している。 ・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。 ・健康管理システムおよび業務端末は住民情報等を取り扱う重要システムが利用する専用ネットワークに接続しており、インターネットとは物理的に接続されていない。 <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・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管・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。 <予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 予・請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「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すクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・予・請求システムは論理的に区分された当市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、予・請求システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予・請求システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ・本市の端末と予・請求システムとの通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。
⑦バックアップ	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑧事故発生時手順の策定・周知	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
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	死者の個人番号と生存する個人の個人番号を分けて管理していないため、生存する個人の個人番号と同様の管理を行う。
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that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	保有する基本5情報は、異動があった場合に随時更新しているため、古い情報のまま保管されることはない。	
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3： 特定個人情報that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	<予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・消去が必要となった情報は内部手続を経て消去し、その記録を残す。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。	
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
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		
・端末(パソコン)、記録媒体、紙文書等の情報資産を破棄する場合は、情報を復元できないように処理したうえで破棄する。機器リース終了後による返却の場合も同様とする。 ・紙文書は、シュレッダーにより復元不可能にする。 ・磁気的な記録媒体は、粉碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行ったうえで破棄する。 ・端末(パソコン)等情報機器については、記録措置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによる消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。		

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	<新潟市における措置> ・評価書の記載内容どおりの運用ができていないか、年に1度担当部署において自己点検を実施し、記録を残す。 ・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。 <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、定期的に自己点検を実施し、記録を残す。	
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	<新潟市における措置> ・新潟市情報セキュリティ対策基準に基づき、情報セキュリティ部門による監査を定期的実施し、監査結果を踏まえて体制や規定を改善する。監査手法はアクセスログを無作為に抽出し業務に必要なアクセス行為であったかを抜き打ち的にチェックすることとする。 ・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。 <中間サーバー・プラットフォームにおける措置> ①運用規則に基づき、中間サーバー・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。	
2. 従業員に対する教育・啓発		
従業員に対する教育・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	<新潟市における措置> ・全職員を対象とした情報セキュリティ研修を年に1回実施し、情報セキュリティ意識の向上を図っている。更に、初任者及びセキュリティ責任者については別途、情報セキュリティに関する研修を年に1回実施している。 ・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。 <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(接続運用規定等)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。	
3. その他のリスク対策		
<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リテラシー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。 ・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。 <全体的なリスク対策> 各項目ごとに掲げた対策に加え、ヒューマンエラーがリスクを招くことを認識したうえで、可能な限りのチェック体制を設け、ヒューマンエラーが生じないよう配慮して業務を進める。		

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	新潟市保健衛生部保健所保健管理課 新潟市中央区紫竹山3丁目3番11号 電話:025-212-8123		
②請求方法	新潟市個人情報保護条例第16条に基づき、指定様式による書面の記載した開示・訂正・利用停止請求を受け付ける。		
	特記事項	市のホームページ上に、請求先、請求方法、請求書様式等を掲載する。	
③手数料等	[無 料] <選択肢> 1) 有料 2) 無 料 (手数料額、納付方法:)		
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	新型インフルエンザ等対策特別措置法による予防接種事業情報ファイル	
	公表場所	新潟市保健衛生部保健管理課、総務部総務課市政情報室	
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	新潟市保健衛生部保健所保健管理課 新潟市中央区紫竹山3丁目3番11号 電話:025-212-8123		
②対応方法	・問い合わせがあった場合、問い合わせの内容と対応の経過について記録を残す。 ・情報漏えい等に関する問合せがあった場合は、実施機関において必要な対応を行い、総務部総務課市政情報室、総務部デジタル行政推進課及び総務部行政経営課に報告する。		

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	市報にいがた及び市のホームページ上で意見公募する旨掲載し、市ホームページ、所管課及び市政情報室において案の閲覧及び配布を行う。意見は電子メール、FAX、郵送にて受け付ける。
②実施日・期間	令和8年8月17日から令和8年9月15日まで
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	新潟市情報公開・個人情報保護・公文書管理審議会による点検
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
	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ② 事務の内容		(内容追記) <予診情報・予防接種記録管理／請求支払システム(以下、「予予・請求システム」という。)>を活用した情報連携に係る予防接種事務 ・本市は、情報連携のため、予予・請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 ・住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 ・医療機関は予防接種時に、医療機関用アプリ等において住民が入力した予診票情報、接種記録の取得/閲覧/入力が可能となる。 ・本市は、医療機関から入力された予診票情報、接種記録の取得及び住民への通知が可能となる。		
	I 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1 ①システムの名称	新潟市保健所情報システム	新潟市健康管理システム		
	I 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1 ②システムの機能		(内容追記) 予予・請求システム連携機能 Public Medical Hubを経由して、住民情報(対象者データ)を提供し、同システムからデジタル予診票や接種記録の情報を受け取る。		
	I 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1 ③他のシステムとの連携		(内容追記) 宛名システム等、その他 予予・請求システム		
	I 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2 ①システムの名称	宛名システム	ガバクラデータ連携システム		
	I 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2 ②システムの機能	既存業務システム間での庁内情報移転のための情報授受のシステムである。 ※情報授受は、既存業務システムからデータにアクセスして情報を取得する。あらかじめアクセスできるデータを各業務システムごとに制御しているため、各業務システムは許可されていないデータの取得ができない仕組みとなっている。 1 既存業務システムからのデータ受取・保存 情報移転元システムで作成した庁内移転用データを受信し、副本として保存する。また、住民記録システム、宛名システムのみ随時(リアルタイム)で異動データを受信し、差分情報として取得した宛名異動のデータを保存する。 2 庁内情報の連携 既存業務システムからの情報要求に応じて、あらかじめ定められた項目のみ当該者の情報抽出・情報提供を行う。 ※庁内移転用データには個人番号が含まれるが、個人番号を利用しない業務システムに対しては個人番号を含まないデータ内容で庁内移転用データを渡す。 3 セキュリティの管理 既存業務システムからのアクセスを制御するため、ID/パスワードの管理を行う。 4 情報連携記録の管理 情報連携記録の生成・管理を行う。	既存業務システム間における庁内での情報転送を行うための情報連携システムである。 ※情報授受は、業務ごとに予め定義された専用領域を介して、既存業務システムから専用領域へアクセスして情報を取得する。なお、情報はファイル単位で連携する。専用領域は、あらかじめアクセスできるデータを各業務システムごとに制御しているため、各業務システムは許可されていないデータの取得ができない仕組みとなっている。 1. 庁内情報の連携 情報移転元システムで作成した庁内移転用データを移転元の専用領域から取得し、移転先の専用領域へデータ転送を行う。 ※庁内移転用データには個人番号が含まれるが、個人番号を利用しない業務システムに対しては個人番号を含まないデータ内容で庁内移転用データを渡す。 2. セキュリティの管理 既存業務システムからのアクセスを制御するため、ID/パスワードの管理を行う。 3. 情報連携記録の管理 情報連携記録の生成・管理を行う。		
	I 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5 ①システムの名称		予予・請求システム		

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
	I 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5 ②システムの名称		①予防接種関連データの登録機能 本市は、健康管理システムからの情報連携又は予防・請求システム画面への直接入力により、予防接種項目、接種動向における通知文言等の予防接種関連データを予防・請求システムへ登録する。 ②情報登録機能及びPMHキー探番依頼機能等 予防・請求システムは、本市で管理している個人番号、対象者情報、予防接種情報及び接種記録を予防・請求システムに登録する。また、Public Medical Hubを経由して医療情報基盤・診療報酬審査支払機構（以下、「DX審査支払機構」という。）の医療保険者等向け中間サーバーと連携し、PMHキーを自動探番する。すでにPMHキーが探番済みの個人番号であれば、探番は行わずに既存のPMHキーを利用する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 予防・請求システムは、マイナポータルからの予防・請求システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予防・請求システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナンバーカードの電子証明書のシリアル番号に紐付くPMH仮名識別子を利用してマイナポータルで予防・請求システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐づく接種記録・通知をマイナポータルへ提供する。また、予防・請求システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐づく予防接種情報を登録する。 ④情報連携機能（医療機関用アプリ等） ・本人確認情報の格納機能 予防接種対象者が、顔認証端末又はマイナ資格確認アプリを利用してマイナンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリ等は、予防・請求システムへ本人確認情報を利用した照会を行う。予防・請求システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐づく予防接種対象者番号をキーに予防接種情報を医療機関用アプリ等に提供する。また、医療機関が接種記録の入力画面から情報を入力することにより、予防・請求システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐づく接種記録を登録する。 ⑤情報連携機能（履歴照会回答システム） ・識別子の格納機能 予防・請求システムは接種記録等の情報を予防接種DBに連携し、予防接種DBにおいて予防接種の有効性・安全性等の調査・研究を行う。予防・請求システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐づけて予防・請求システムに連携する。		
	I 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5 ②システムの名称		（内容追記）健康管理システム、マイナポータル、医療機関用アプリ、電子カルテ等、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム		
	I 基本情報 5. 個人番号の利用	1、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（番号法） ・第9条第1項 別表 第126項 2、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律別表の主務省令で定める事務を定める命令（別表省令） ・第67条の2	1、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律（番号法） ・第9条第1項 別表 第126項 2、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律別表の主務省令で定める事務を定める命令（別表省令） ・第67条の3		
	I 基本情報＞別添1 事務の内容		全体図を修正		
	I 基本情報＞別添1 事務の内容		（内容追記） （備考）＜追加する事務＞ ①特定個人情報の登録・管理 ・本市は、健康管理システムからの情報連携又は予防・請求システム画面への直接入力により、予防・請求システムにおいて対象者の個人番号を含む対象者情報の登録を行う。（LGWAN回線等経由） ・本市は予防・請求システムから接種記録等、必要な情報を自動連携またはダウンロードし、健康管理システム等への取込を行う。 ・予防・請求システムへ登録された個人情報へのアクセスは適切に制御される。 ②PMHキー探番 ・予防・請求システムは、Public Medical Hubに対して個人番号を連携することで、オンライン資格確認等システムと予防・請求システムが連携するためのPMHキーの探番処理を依頼する。 ・Public Medical Hubは、医療保険者等向け中間サーバーを経由しPMHキーを探索して予防・請求システムに回答する。 ・医療保険者等向け中間サーバーは、PMHキーと個人番号を紐付けて、PMHキーと紐付番号を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、紐付番号をキーに仮名識別子とPMHキーを紐付けて、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、仮名識別子、PMHキーと紐付けて、予防・請求システムに連携する。（連携後、マイナポータル上からPMHキーは削除される。）以降、③④⑤⑥が可能となる。 ③マイナポータルへの通知 ・予防・請求システムからマイナポータル経由で住民向けの通知を行うため、本市は予防・請求システムを利用してマイナポータルに識別子（PMH仮名識別子）と通知情報を登録する。 ④マイナポータルからの入力・取得（予防票・接種記録） ・住民は、マイナポータル経由で予防・請求システムへの予防票の事前入力や、予防・請求システムから接種記録や通知情報を閲覧/取得する。 ⑤医療機関用アプリ等からの入力・取得（予防票・接種記録） ・医療機関が医療機関用アプリ等を利用し、接種時に住民からマイナンバーカードによる本人確認を経て、事前入力された予防票及び接種記録の閲覧/取得/入力を行う。 ⑥ID5取得 ・予防接種DBへの接種記録等の連携時に個人を特定する識別子情報として、予防・請求システムが履歴照会回答システム経由でID5を取得する。		
	II 特定個人情報ファイルの概要 2基本情報 ④記録される項目		（内容追記）その他 予防接種記録情報		

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
	Ⅱ 特定個人情報ファイルの概要 2 基本情報 ④ 記録される項目 その妥当性	①個人番号、その他識別情報：対象者を正確に特定するために保有 ②5情報、連絡先、その他住民票関係情報：正確な本人特定のため、予防接種券・予診票に記入された情報と突合するために保有、また接種勧奨に使用するために保有 ③健康・医療関係情報：予防接種履歴管理を適正に行うために保有	①個人番号、その他識別情報（PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5）： 対象者を正確に特定するために保有 ②5情報、連絡先、その他住民票関係情報：正確な本人特定のため、予防接種券・予診票に記入された情報と突合するために保有、また接種勧奨に使用するために保有 ③その他（予防接種記録情報）： 予防接種事務の適切な実施にあたり必要となる情報を管理し、予予・請求システムが、外部と情報連携するために必要		
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の入手・使用 ① 入手元		（項目追加）・本人または本人の代理人・民間事業者（医療機関）・その他 DX審査支払機構		
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の入手・使用 ② 入手方法		（項目追加）その他 Public Medical Hub、医療機関用アプリ等、マイナポータル （項目削除）情報提供ネットワークシステム		
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の入手・使用 ③ 入手の時期・頻度	住民情報は、住民登録に係る申請受付時に随時入手する。 予防接種情報は、市民が接種する都度、月1回定期的に医療機関から医師会を通じて予防接種券・予診票を受領し入手する。加えて、転入者等については転入時、転入から一定期間後、接種勧奨通知事務前等に情報提供ネットワークシステムを介して入手する。	住民情報は、住民登録に係る申請受付時に随時入手する。 予防接種情報は、市民が接種する都度、月1回定期的に医療機関から医師会を通じて予防接種券・予診票を受領し入手する。		
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の入手・使用 ③ 入手の時期・頻度		（内容追記）〈予予・請求システムを活用した情報連携に係る予防接種事務〉 ・予予・請求システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入力する。 ・国が予予・請求システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本市が個人情報を入力し、予予・請求システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等又は医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予予・請求システムにおいて個人番号と結びついて特定個人情報となる。		
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の入手・使用 ④ 入手に係る妥当性		（内容追記）〈予予・請求システムを活用した情報連携に係る予防接種事務〉 （PMHキー採番処理依頼時に入手される特定個人情報） ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 （その他：個人情報として入手し、予予・請求システムにおいて個人番号と結び付き特定個人情報となる情報） 本市が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入力し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証（本人確認）の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。		
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の入手・使用 ⑤ 本人への明示	本人から入手する情報については、使用目的を本人に明示したうえで入手する。 また、庁内連携・情報提供ネットワークシステムからの入手については、番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表 第153項にて明示されている。（新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務）	本人から入手する情報については、使用目的を本人に明示したうえで入手する。 また、庁内連携ネットワークシステムからの入手については、番号法第19条第8号に基づく利用特定個人情報の提供に関する命令第2条の表 第153項にて明示されている。（新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務）		
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の入手・使用 ⑤ 本人への明示		（内容追記）〈予予・請求システムを活用した情報連携に係る予防接種事務〉 本人又は本人の代理人から入手する情報については、利用目的を明示した上で入手している。マイナポータル等では、本人又は本人の代理人が画面に表示された利用目的を確認することによって、本人確認とする。		

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
	Ⅱ 特定個人情報ファイルの概要 3. 特定個人情報保護の 入手・使用 ⑧使用方法		(内容追記)＜予予・請求システムを活用した情報連携に係る予防接種事務＞ ・情報連携のため、本市は、予予・請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予防接種情報及び予防接種管理情報の紐付け及び登録を行う。 ・登録後、予予・請求システムは、Public Medical Hubに対してオンライン資格確認等システムと予予・請求システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予予・請求システムに回答する。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予予・請求システムで共有されることで予予・請求システムからマイナポータルへの通知、マイナポータルや医療機関用アプリ等から予予・請求システムの予防接種情報及び接種記録の取得/閲覧/入力等といった情報連携が可能となる。		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託	1件	2件		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1	保健所情報システム運用保守	健康管理システム運用保守		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ①委託内容	保健所情報システム運用業務(システム資源の維持管理、障害復旧対応等)	健康管理システム運用業務(システム資源の維持管理、障害復旧対応等)		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ④委託先への特定個人情報ファイルの提供方法	専用線	選択から削除		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ④委託先への特定個人情報ファイルの提供方法		(内容追記)その他 庁舎内でシステムを直接操作		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2		予予・請求システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ①委託内容		予防接種・予防接種記録管理/請求支払システムの利用・情報連携業務及び運用保守業務		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 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		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ②取扱いを委託する特定個人情報ファイルの範囲 その妥当性		予予・請求システムは公益社団法人国民健康保険中央会(以下、国保中央会という。)が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。 ただし、予予・請求システムに格納された特定個人情報、自動処理により再々委託先(これ以降の全ての委託を含む。以下、同じ。)に情報連携されるため、新潟県国民健康保険団体連合会(以下、新潟県国保連合会という。)及び国保中央会は特定個人情報にアクセスすることはない。		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ③委託先における取扱者数		10人以上50人未満		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ④委託先への特定個人情報ファイルの提供方法		その他 LGWAN又は閉域網回線を用いた提供		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑤委託先名の確認方法		下記、「⑥委託先名」の項の記載より確認できる。		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑥委託先名		新潟県国保連合会		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑧再委託の許諾方法		書面または電磁的方法による承諾		
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項2 ⑨再委託事項		・「アド」請求システムの運用保守 ・PMHキーの採番及びPMHキーを介した医療機関用アプリ等・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。		

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
	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	<新潟市における措置> 特定個人情報を管理しているサーバーはデータセンターに設置しており、設置場所は以下の物理的対策を行っている。 ・建物及びサーバー室までの経路に機械警備システムを導入し、入室可能な者の特定及び入室の管理を行っている。 ・サーバー室の入口付近に監視カメラを設置し、入退出者を管理している。 ・サーバー室内に設置したサーバーは、全て鍵付のサーバーラックに設置している。 ・帳票を出力する印刷室についても、サーバー室と同様な機械警備及び監視カメラによる入室管理を行っている。 ・該当システム基盤のサーバーログインは、ID／パスワードによる認証が必要で、限られたメンバーしか操作できない。	<新潟市における措置> ・申告書及び届出書等の紙媒体については、許可された者以外入室することできない執務室内にて保管しており、取り扱いも執務室内に限定している。 ・窓口業務等を行う部署においては、紙媒体やオンラインの画面が第三者に見えないような配慮を徹底している。 <ガバメントクラウド(健康管理システム)における措置> ・サーバー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。 ・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。		
	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ②保管期間	予防接種法施行令第6条の2において、5年間保管すると定められているが、接種記録確認等の事務のため長期間保管する必要がある。	予防接種法施行規則第4条において、5年間保管すると定められているが、接種記録確認等の事務のため長期間保管する必要がある。		
	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③消去方法		(内容追記) <予予・請求システムを活用した情報連携に係る予防接種事務> ・本市の領域に保管されたデータのみ、予予・請求システムを用いて消去することができる。 ・本市の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、 ・消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。		
	Ⅱ 特定個人情報ファイルの概要 (別添2)ファイル記録項目		(内容追記)<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加の記録項目> (1)対象者情報 ・個人番号・PMHキー・PMH仮名識別子・基本5情報(カナ・氏名・住所・生年月日・性別)・保護者氏名・自治体コード・自治体業務ID・連携ファイル名・連携日時・連携処理ステータス/エラー内容・制御フラグ(リカバリ/不開示/閲覧停止)・変更区分・削除の異動日・その他管理番号・ID等(予防接種対象者番号)・その他区分等(接種対象者区分/減免区分) (2)ユーザー情報 ・機関マスタID・機関ユーザーID・メールアドレス・ユーザー氏名・ユーザー区分・ユーザー権限ID・個人番号閲覧可能フラグ・ユーザー削除フラグ (3)予診票情報 ・項目ID・管理ID・更新日時・回答ID・回答内容・回答処理ステータス・回答日時・接種不可フラグ・予防接種設定ID・予防接種管理ID・組み合わせ番号・強制失効日・勸奨情報(ルールID、勸奨日) (4)予防接種記録情報 ・予防接種記録ID・予防接種管理ID・接種日・接種同意フラグ・医療機関コード・医師名・実施場所・実施区分・接種区分・GTINコード・ワクチンメーカー名・ワクチン名(ワクチン一般名/ワクチン通称/ワクチン販売名)・ロット番号・接種量・接種部位・接種方法・ワクチン有効期限・要注意接種フラグ・特別の事情・海外接種フラグ・更新日時・最新/削除フラグ・その他区分等(接種対象者区分/減免区分)		
	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 2. 特定個人情報の入手リスク1 対象者以外の情報の入手を防止するための措置の内容	<統合DBシステムにおける措置> 統合DBシステムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。	<ガバラデータ連携システムにおける措置> ガバラデータ連携システムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。		
	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 2. 特定個人情報の入手リスク1 対象者以外の情報の入手を防止するための措置の内容	<団体内統合宛名システムにおける措置> 団体内統合宛名システムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。	削除		

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
	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 2. 特定個人情報の入手リスク1 対象者以外の情報の入手を防止するための措置の内容	<保健所情報システムにおける措置> ①利用者によって利用可能な機能を制限し、 unnecessary 情報の入手を抑制している。 <統合DBシステムにおける措置> ①情報移転元システムが作成したデータを統合DBシステムに格納し、既存業務システムからデータにアクセスして情報を取得するシステムであるが、情報移転対象者以外の情報が混入することはない。 ②あらかじめアクセスできるデータを各業務システムごとに制御しているため、既存業務システムは許可されていないデータの取得ができないことを担保している。 ③統合DBシステムを利用する各業務システム各々にID／パスワードを設定することで、他システム用の情報データへのアクセスを阻止している。 <団体内統合宛名システムにおける措置> 団体内統合宛名システムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。	<健康管理システムにおける措置> ①利用者によって利用可能な機能を制限し、 unnecessary 情報の入手を抑制している。 <ガバラデータ連携システムにおける措置> ①情報移転元システムが作成したデータをガバラデータ連携システムに格納し、既存業務システムからデータにアクセスして情報を取得するシステムであるが、情報移転対象者以外の情報が混入することはない。 ②あらかじめアクセスできるデータを各業務システムごとに制御しているため、既存業務システムは許可されていないデータの取得ができないことを担保している。 ③ガバラデータ連携システムシステムを利用する各業務システム各々にID／パスワードを設定することで、他システム用の情報データへのアクセスを阻止している。 <団体内統合宛名システムにおける措置> 団体内統合宛名システムから情報を入手する際には、当該対象者の宛名コードを指定することを必須としており、当該対象者の情報であることを担保している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予・請求システムへは、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（PMHキーと個人番号）のみが返却されるようシステム的に制御している。 ・医療機関から医療機関用アプリ等を入力される際は、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連携されるようシステム的に制御している。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、定められたデータ項目のみが入力されるようシステム的に制御している。 ・生年月日等をチェックすることで紐付け誤りを防止する機能（以下、「紐付け誤り防止機能」という。）により、誤った情報が紐付けられるリスクを低減する。		
	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 2. 特定個人情報の入手リスク2 リスクに対する措置の内容	<保健所情報システムにおける措置> ①ID／パスワードに加え、生体認証を実施しており、あらかじめ承認された利用者以外の情報入手を抑制している。 <統合DBシステムにおける措置> ①統合DBシステムを利用する既存業務システム各々にID／パスワードを設定することで、あらかじめ承認されたシステム以外の情報入手を阻止している。 ②データ授受の動作記録を残すことで、不適切な入手を抑制している。 <団体内統合宛名システムにおける措置> ①接続システムの認証及び団体内統合宛名システム接続端末での職員認証等の機能を備えており、あらかじめ承認されたシステム・職員以外の情報入手を抑制している。 ②団体内統合宛名管理システムへのログイン及びデータ授受の動作記録を残すことで、不適切な入手を抑制している。	<健康管理システムにおける措置> ①ID／パスワードに加え、生体認証を実施しており、あらかじめ承認された利用者以外の情報入手を抑制している。 <ガバラデータ連携システムにおける措置> ①ガバラデータ連携システムを利用する既存業務システム各々にID／パスワードを設定することで、あらかじめ承認されたシステム以外の情報入手を抑制している。 ②データ授受の動作記録を残すことで、不適切な入手を抑制している。 <団体内統合宛名システムにおける措置> ①接続システムの認証及び団体内統合宛名システム接続端末での職員認証等の機能を備えており、あらかじめ承認されたシステム・職員以外の情報入手を抑制している。 ②団体内統合宛名管理システムへのログイン及びデータ授受の動作記録を残すことで、不適切な入手を抑制している。		
	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 2. 特定個人情報の入手リスク2 リスクに対する措置の内容		（内容追記）<予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予・請求システムへは、システム自動処理により、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（PMHキーと個人番号）のみが返却されるようシステム的に制御している。 ・予予・請求システムのデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。		
	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 2. 特定個人情報の入手リスク3 入手の際の本人確認の措置の内容		（内容追記）<予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・予予・請求システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。		
	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 2. 特定個人情報の入手リスク3 個人情報の真正性確認の措置の内容		（内容追記）<予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・予予・請求システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。		
	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 2. 特定個人情報の入手リスク3 特定個人情報の正確性確保の措置の内容		（内容追記） <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。		

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
	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 2. 特定個人情報の入手リスク4 リスクに対する措置の内容	＜宛名システム、統合連携DBシステムにおける措置＞	＜ガバクラデータ連携システムにおける措置＞		
	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 2. 特定個人情報の入手リスク4 リスクに対する措置の内容	＜団体内統合宛名システムにおける措置＞ 団体内統合宛名システムは、中間サーバーや既存業務システムとの接続に専用回線を用いているため、外部に漏れることはない。また、団体内統合宛名システムと団体内統合宛名システム接続端末間の通信を暗号化し、漏えい・紛失を防いでいる。	＜団体内統合宛名システムにおける措置＞ →削除 (内容追記)＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予・請求システムとDX審査支払機構の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 ・健康管理システムは、予予・請求システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。		
	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 3. 特定個人情報の使用リスク1 宛名システム等における措置の内容	＜団体内統合宛名システムにおける措置＞ 団体内統合宛名システムでは、情報を利用する事務と事務に必要な情報項目の対応付けをあらかじめ設定しており、設定を超えた範囲の情報を入手することは不可能である。また、システム連携する既存業務システムごとにアクセス制御も行う。	＜団体内統合宛名システムにおける措置＞ 団体内統合宛名システムでは、情報を利用する事務と事務に必要な情報項目の対応付けをあらかじめ設定しており、設定を超えた範囲の情報を提供することは不可能である。また、システム連携する既存業務システムごとにアクセス制御も行う。		
	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 3. 特定個人情報の使用リスク1 事務で使用するその他のシステムにおける措置の内容	＜保健所情報システムにおける措置＞ 庁内の他システムからアクセスできないよう適切なアクセス制限を講じており、目的を超えた紐付けは行われないようにしている。 ＜統合DBシステムにおける措置＞ 情報移転元システムが作成したデータを情報移転先システムに中継するシステムであり、移転する情報以外の情報利用はできない。	＜健康管理システムにおける措置＞ 庁内の他システムからアクセスできないよう適切なアクセス制限を講じており、目的を超えた紐付けは行われないようにしている。 ＜ガバクラデータ連携システムにおける措置＞ 情報移転元システムが作成したデータを情報移転先システムに中継するシステムであり、移転する情報以外の情報利用はできない。		
	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 3. 特定個人情報の使用リスク1 事務で使用するその他のシステムにおける措置の内容		(内容追記) ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予・請求システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予予・請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予予・請求システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。		
	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 3. 特定個人情報の使用リスク2 ユーザー認証の管理具体的な管理方法		＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市は、予予・請求システムのアクセス権限を管理する管理者を定める。 ・予予・請求システムのログインはユーザID・パスワードで行う。 ・予予・請求システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予予・請求システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・健康管理システムから予予・請求システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。		
	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 3. 特定個人情報の使用リスク2 アクセス権限の発効・失効の管理	○アクセス権の発行 当該既存業務システムを所管している所属長に対し、アクセス権を必要とする所属の長が下記の内容を記載した申請を行い、当該既存業務システムを所管している所属長がアクセス権限を設定する。 ・必要なアクセス権限の種類 ・アクセス権限が必要な期間 ・利用する業務名及び業務概要 ・利用目的及び必要とする理由(法令根拠等) ・申請課及び利用課の所属長及び利用者 ○アクセス権の失効 アクセス権は、必要な期間の満了日に自動削除される。 また、アクセス権が必要な期間の満了日前に異動若しくは退職した場合には手動で削除する。	＜健康管理システムにおける措置＞ ○アクセス権の発行 健康管理システムを所管している所属長に対し、アクセス権を必要とする所属の長が下記の内容を記載した申請を行い、当該既存業務システムを所管している所属長がアクセス権限を設定する。 ・必要なアクセス権限の種類 ・アクセス権限が必要な期間 ・利用する業務名及び業務概要 ・利用目的及び必要とする理由(法令根拠等) ・申請課及び利用課の所属長及び利用者 ○アクセス権の失効 アクセス権は、年度末または必要な期間の満了日に自動削除される。 また、アクセス権が必要な期間の満了日前に異動若しくは退職した場合には手動で削除する。 ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予・請求システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・管理者は、アクセス権限の管理表を作成し、申請者に対して管理表に基づき適切なアクセス権限を付与する。 ・本市において、人事異動や退職等があった際は、異動情報に基づき、不要となったアクセス権限を管理し、失効させる。		

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
	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 3. 特定個人情報の使用リスク2 アクセス権限の管理		(内容追記) <健康管理システムにおける措置> <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・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。 ・管理者が定期的に管理表を確認し、必要に応じて見直しを行う。		
	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 3. 特定個人情報の使用リスク2 特定個人情報の使用の記録	特定個人情報へのアクセス記録は、システムがアクセスログ(日時、利用者、利用端末、利用情報)として全件記録している。	<健康管理システムにおける措置> 特定個人情報へのアクセス記録は、システムがアクセスログ(日時、利用者、利用端末、利用情報)として全件記録している。 <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 本市は、システム上の操作のログを取得し、操作ログを定期的に確認する。		
	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 3. 特定個人情報の使用リスク3 従業者が事務外で使用するリスク		(内容追記) また、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、事務外での使用を防止する。 委託業務については、委託先との契約により、委託業者が従業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。本市は、当該教育の実施について履行確認を行う。再委託先においても同様の取扱とする。		
	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 3. 特定個人情報の使用リスク4 特定個人情報のファイルが不正に複製されるリスク		(内容追記) <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・健康管理システムから特定個人情報を抽出したCSVファイルを予予・請求システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・健康管理システムから予予・請求システムへの特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線(LGWN又はその他の閉域網回線)を利用した接続のみが認められる。 ・予予・請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。		
	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 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認		(内容追記) <健康管理システムにおける措置> <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 本市は、予予・請求システムの利用・情報連携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新潟県国保連合会に委託し、新潟県国保連合会は国保中央会に再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、国保中央会の設備、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。		
	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法		(内容追記) <健康管理システムにおける措置> <予診情報・予防接種記録管理/請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・本市がアクセス権限の管理状況を確認できる。 ・本市は、アクセス権限を付与する者を必要最小限に限定する。 ・本市は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本市は、アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再々委託先(PMHキー採番や運用保守)のみに付与される。		
	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録 具体的な制限方法		(内容追記) <健康管理システムにおける措置> <予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> ・予予・請求システムは特定個人情報の取り扱いのログを保存し、本市は特定個人情報に係る操作のログを閲覧・出力できる。 ※再々委託先(PMHキー採番や運用保守)に係る特定個人情報の取扱いログに限られる。		

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
	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 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		(内容追記)＜健康管理システムにおける措置＞ ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託先(再委託先及び再々委託先を含む。)から他者への提供は行わない。 ・本市は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)から他者への提供が行われていないことを確認できる。		
	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 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		(内容追記)＜健康管理システムにおける措置＞ ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託先(再委託先及び再々委託先を含む。)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。 ・本市は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)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。		
	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 4. 特定個人情報ファイルの取扱いの委託 特定個人情報の消去ルール ルールの内容及びルール遵守の確認方法		(内容追記)＜健康管理システムにおける措置＞ ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託契約終了後は予予・請求システムに保管していた全ての特定個人情報を国保中央会が消去する。 ・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、本市は消去について国保中央会から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。		
	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 4. 特定個人情報ファイルの取扱いの委託 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 規定の内容		(内容追記)＜健康管理システムにおける措置＞ ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 新潟県国保連合会及び国保中央会は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員の明確化 ・従業員に対する監督・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		
	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 4. 特定個人情報ファイルの取扱いの委託 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 具体的な方法		(内容追記)＜健康管理システムにおける措置＞ ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・再々委託の相手方は、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。 ・国保中央会が、再々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、再々委託の相手方によるセルフチェックを基本とし、必要に応じて国保中央会が訪問確認を行う。 ・点検後に改善事項がある場合は、国保中央会が改善指示及び改善状況のモニタリングを行う。 ・国保中央会は、点検結果について新潟県国保連合会及び本市に年1回報告を行う。		
	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 4. 特定個人情報ファイルの取扱いの委託 その他の措置の内容		＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業員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。		
	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 6. 情報提供ネットワークとの接続 リスク5	＜保健所情報システムにおける措置＞	＜健康管理システムにおける措置＞		

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
	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 6. 情報提供ネットワークとの接続 リスク6	<保健所情報システムにおける措置> 保健所情報システムへのログインは、ID／パスワードによる認証を必要とする利用者登録により制限されており、特定の権限者以外は情報照会・提供ができず、さらに、情報照会・情報提供記録をデータベースに逐一保存することで、不適切な方法で特定個人情報やりとりされることを防止する。	<健康管理システムにおける措置> 健康管理システムへのログインは、生体認証を必要とする利用者登録により制限されており、特定の権限者以外は情報照会・提供ができず、さらに、情報照会・情報提供記録をデータベースに逐一保存することで、不適切な方法で特定個人情報やりとりされることを防止する。		
	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 6. 情報提供ネットワークとの接続 リスク7	<保健所情報システムにおける措置> ・誤った情報を提供・移転してしまうリスクへの措置 提供・移転する情報のチェックを行い、誤った情報が作成されないことをシステム上で担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 汎用連携DBシステムでは、番号法に基づき認められる情報のみ、認められた相手にしか移転できないよう、システムの仕組みとして担保されている。	<健康管理システムの運用における措置> ・誤った情報を提供・移転してしまうリスクへの措置 提供・移転する情報のチェックを行い、誤った情報が作成されないことをシステム上で担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 団体内統合宛名システムでは、番号法に基づき認められる情報のみ、認められた相手にしか移転できないよう、システムの仕組みとして担保されている。		
	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. 特定個人情報の保管・消去 リスク1 ⑤物理的対策 具体的な対策の内容	<保健所情報システムにおける措置> ・誤った情報を提供・移転してしまうリスクへの措置 提供・移転する情報のチェックを行い、誤った情報が作成されないことをシステム上で担保する。 ・誤った相手に提供・移転してしまうリスクへの措置 汎用連携DBシステムでは、番号法に基づき認められる情報のみ、認められた相手にしか移転できないよう、システムの仕組みとして担保されている。	<新潟市における措置> ・端末、電磁的記録媒体、紙媒体については、許可された者以外入室することのできない執務室内にて保管しており、取り扱いも執務室内に限定している。 ・執務室が無人になる際には、施錠管理を徹底している。 ・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。 <ガバメントクラウド(健康管理システム)における措置> ・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。 ・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。		
	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. 特定個人情報の保管・消去 リスク1 ⑤物理的対策 具体的な対策の内容		(内容追記)<予予・請求システムを活用した情報連携に係る予防接種事務における追加措置> 予予・請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「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すクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスの利用		
	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. 特定個人情報の保管・消去 リスク1 ⑥技術的対策 具体的な対策の内容	<新潟市における措置> ・特定個人情報ファイルを管理しているサーバーは、インターネット等の外部ネットワークから隔離されたネットワーク上に設置している。 ・特定個人情報ファイルを管理している全てのサーバーには、ウイルス対策ソフトを導入しており、パターンファイルも最新版が適用されるよう管理している。 ・特定個人情報ファイルにアクセスする業務用端末は、端末側に業務データが残らない方式を採用している。	<新潟市における措置> ・特定個人情報ファイルにアクセスする業務用端末は、端末側に業務データが残らない方式を採用している。 ・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。 ・健康管理システムおよび業務端末は住民情報等を取り扱う重要システムが利用する専用ネットワークに接続しており、インターネットとは物理的に接続されていない。		

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
	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. 特定個人情報の保管・消去 リスク1 ⑥技術的対策 具体的な対策の内容		(内容追記) ＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 予予・請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度 (ISMAP) において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「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すクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・予予・請求システムは論理的に区分された当市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、予予・請求システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予予・請求システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ・本市の端末と予予・請求システムとの通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップ (内容追記)＜予予・請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・消去が必要となった情報は内部手続を経て消去し、その記録を残す。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。		
	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. 特定個人情報の保管・消去 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		サーバー、端末(パソコン)、記録媒体、紙文書等の情報資産を破棄する場合は、情報を復元できないように処理したうえで破棄する。機器リース終了後による返却の場合も同様とする。 ・紙文書は、シュレッダーにより復元不可能にする。 ・磁気的な記録媒体は、粉碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行ったうえで破棄する。 ・サーバー、端末(パソコン)等情報機器については、記録措置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによる消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。 端末(パソコン)、記録媒体、紙文書等の情報資産を破棄する場合は、情報を復元できないように処理したうえで破棄する。機器リース終了後による返却の場合も同様とする。 ・紙文書は、シュレッダーにより復元不可能にする。 ・磁気的な記録媒体は、粉碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行ったうえで破棄する。 ・端末(パソコン)等情報機器については、記録措置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによる消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。		
	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. 特定個人情報の保管・消去 リスク3 特定個人情報の保管・消去におけるその都のリスク及びそのリスクに対する措置		サーバー、端末(パソコン)、記録媒体、紙文書等の情報資産を破棄する場合は、情報を復元できないように処理したうえで破棄する。機器リース終了後による返却の場合も同様とする。 ・紙文書は、シュレッダーにより復元不可能にする。 ・磁気的な記録媒体は、粉碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行ったうえで破棄する。 ・サーバー、端末(パソコン)等情報機器については、記録措置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによる消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。 端末(パソコン)、記録媒体、紙文書等の情報資産を破棄する場合は、情報を復元できないように処理したうえで破棄する。機器リース終了後による返却の場合も同様とする。 ・紙文書は、シュレッダーにより復元不可能にする。 ・磁気的な記録媒体は、粉碎処理、電磁気破壊、データ消去ソフトウェアによるデータ消去を行ったうえで破棄する。 ・端末(パソコン)等情報機器については、記録措置に対し、物理破壊、磁気破壊、データ消去ソフトウェアによる消去を行う。 ・データ消去を業者に委託した場合は、消去作業証明書を提出させる。		
	Ⅳ その他のリスク対策 1. 監査 ①自己点検		(内容追記)＜予予・請求システムを活用した情報連携に係る予防接種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。		
	Ⅳ その他のリスク対策 1. 監査 ②監査		(内容追記)＜予予・請求システムを活用した情報連携に係る予防接種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。		
	Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発		(内容追記)＜予予・請求システムを活用した情報連携に係る予防接種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。		
	Ⅳ その他のリスク対策 3. その他のリスク対策		(内容追記)＜予予・請求システムを活用した情報連携に係る予防接種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。		