別紙３

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
26	八王子市　予防接種に関する事務　全項目評価書（素案）

個人のプライバシー等の権利利益の保護の宣言	
八王子市は、予防接種に関する事務における特定個人情報ファイルの取り扱いにあたり、特定個人情報ファイルの取り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
八王子市長

個人情報保護委員会　承認日 【行政機関等のみ】
公表日

［令和６年10月　様式４］

項目一覧

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	予防接種に関する事務
②事務の内容　※	【予防接種に関する事務】 　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基づき、A類疾病及びB類疾病のうち政令で定めるものについて、市内に居住する者に対し予防接種を実施するとともに、接種歴等の情報の管理を行う。また、当該予防接種に起因する健康被害に対する給付を行う。 【特定個人情報保護ファイルを使用する事務の内容】 1.予防接種法による予防接種の実施に関する事務 2.予防接種による健康被害救済の給付の支給に関する事務 3.予防接種による実費の徴収に関する事務 【お知らせ・サービス検索における事務】 ・予防接種に関する事務におけるお知らせについて、郵送と合わせて、マイナポータルのお知らせ機能を用いて保護者に対して通知を行う。 ＜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＞ 1.本市は、情報連携のため、予診情報・予防接種記録管理／請求支払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。 2.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。 3.住民が予防接種時に、従来の紙の予診票に代えて、タブレットに搭載された医療機関用アプリ等においてマイナンバーカードを用いることにより、医療機関は住民が事前に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。 4.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　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	総合健診システム
②システムの機能	1.予防接種実施状況の登録、照会 2.予防接種通知の対象者の抽出、宛名印刷 3.予防接種券の発行
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2	
①システムの名称	中間サーバー
②システムの機能	1.符号管理 　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・管理する機能 2.情報照会 　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)を行う機能 3.情報提供 　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)の提供を行う機能 4.既存システム接続 　中間サーバーと個人情報を保有・管理するシステム(以下、「既存システム」という)との間で宛名システムを通じて情報照会内容、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を連携する機能 5.情報提供等記録管理 　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の記録を生成し、管理する機能 6.情報提供データベース管理 　特定個人情報(連携対象)を副本として、保持・管理する機能 7.データ送受信 　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機能 8.セキュリティ管理 　暗号化・復号機能と、鍵情報及び照会許可用照合リスト情報を管理する機能 9.職員認証・権限管理 　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)へのアクセス制御を行う機能 10.システム管理 　バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う機能
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3	
①システムの名称	団体内統合宛名システム(以下、「宛名システム」という。)
②システムの機能	1.宛名情報管理 　中間サーバー及び既存システムで統一的に利用する団体内統合宛名番号の付番管理、宛名情報等の管理を行う機能 2.中間サーバー連携 　中間サーバー又は中間サーバー端末からの要求に基づき、団体内統合宛名番号と紐付く宛名情報等を通知する機能 3.既存システム連携 　既存システムからの要求に基づき、団体内統合宛名番号と紐付く宛名情報等を通知する機能 　庁内連携システムから中間サーバーに格納すべき情報を取得する機能 4.お知らせ通知機能 　通知を送付する対象者の宛名情報及び通知文、添付ファイルを取り込み、お知らせ通知を中間サーバーを通じてマイナポータルに送信する。
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　（ 中間サーバ、既存システム　　）

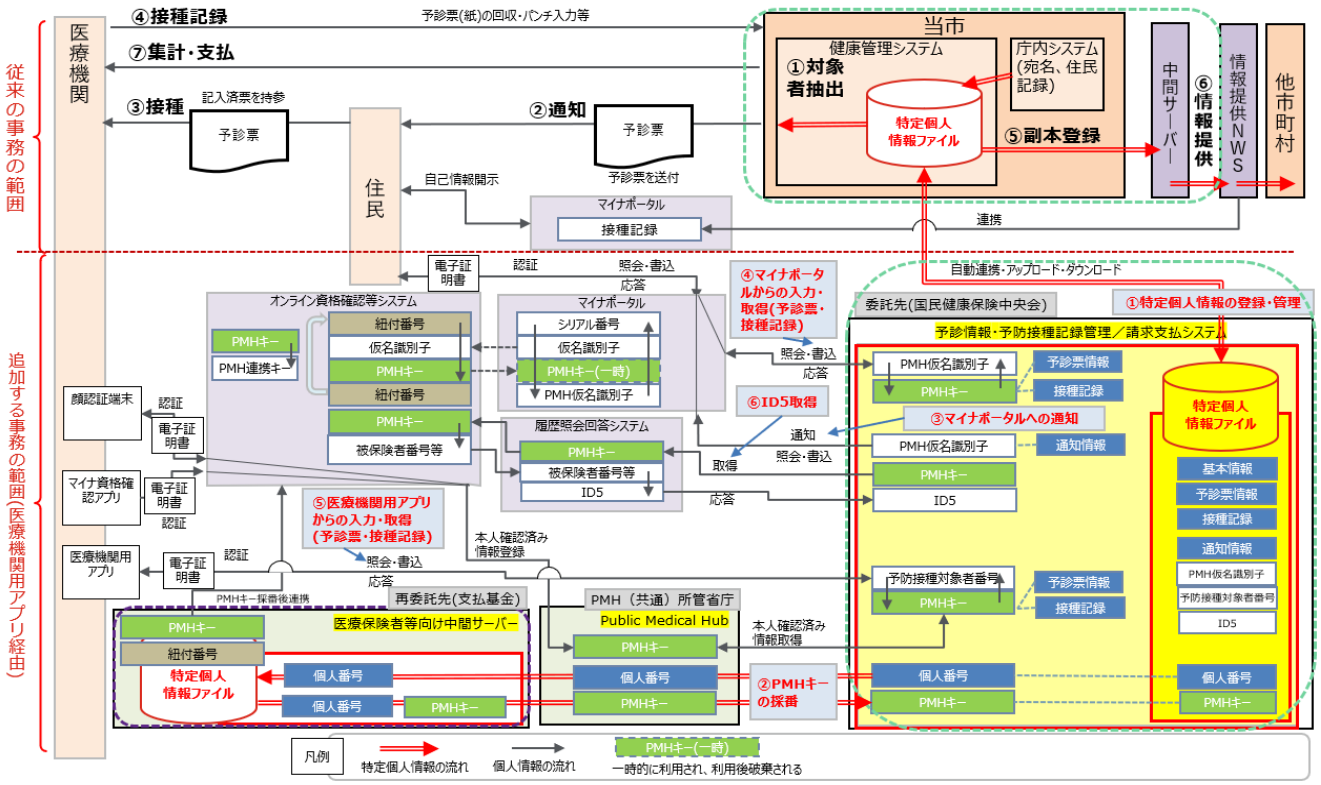
システム4	
①システムの名称	予診情報・予防接種記録管理／請求支払システム
②システムの機能	＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ ①予防接種関連データの登録機能 本市は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・予防接種記録管理／請求支払システムに登録する。また、Public Medical Hubを経由して社会保険診療報酬支払基金（以下、「支払基金」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 予診情報・予防接種記録管理／請求支払システムは、マイナポータルからの予診情報・予防接種記録管理／請求支払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キーと紐付けて予診情報・予防接種記録管理／請求支払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た照会を行う。予診情報・予防接種記録管理／請求支払システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く接種記録・通知をマイナポータルへ提供する。また、マイナポータルへログインして予診票の入力画面から情報を入力することにより、予診情報・予防接種記録管理／請求支払システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐付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） ・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 医療機関用アプリは、予診情報・予防接種記録管理／請求支払システムへ本人確認情報を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐付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、予診情報・予防接種記録管理／請求支払システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐付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 予診情報・予防接種記録管理／請求支払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。予診情報・予防接種記録管理／請求支払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キーと紐づけて予診情報・予防接種記録管理／請求支払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　（総合健診システム、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	
予防接種情報【予防接種に関する事務】 予防接種情報ファイル	
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	予防接種を進めていく中で、接種記録等を確認し、適切な接種間隔で実施していくことが必要となるため。
②実現が期待されるメリット	市外で接種した予防接種の記録を把握することができ、市民及び医療機関からの問合せに対して、正確に回答することが可能となる。
5. 個人番号の利用 ※	
法令上の根拠	【予防接種に関する事務】 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。)第9条第1項別表の14の項、114の項、126の項 番号法別表の主務省令で定める事務を定める命令第10条、第67条の2 【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事務】 番号法第19条第6号(委託先への提供)
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	【予防接種に関する事務】 1.情報提供の根拠 番号法第19条第7号、番号法第19条第8号に基づく主務省令第2条の表26の項、28の項、153の項、154の項 2.情報照会の根拠 番号法第19条第8号に基づく主務省令第2条の表25の項、26の項、27の項、28の項、29の項、153の項
7. 評価実施機関における担当部署	
①部署	健康医療部健康づくり推進課
②所属長の役職名	健康医療部健康づくり推進課長
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、（　　）部については社会保険診療報酬支払基金(支払基金)がPIAを実施するため評価対象外)



（備考）

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診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診情報・予防接種記録管理／請求支払システムにおいて対象者の個人番号を含む対象者情報と予防接種管理情報の紐付け及び登録を行う。（LGWAN回線等経由）
・本市は予診情報・予防接種記録管理／請求支払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。
・予診情報・予防接種記録管理／請求支払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キー採番
・予診情報・予防接種記録管理／請求支払システムは、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診情報・予防接種記録管理／請求支払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ーを経由しPMHキーを採番して予診情報・予防接種記録管理／請求支払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、予診情報・予防接種記録管理／請求支払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
・予診情報・予防接種記録管理／請求支払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、本市は予診情報・予防接種記録管理／請求支払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診情報・予防接種記録管理／請求支払システムへの予診票の事前入力や、予診情報・予防接種記録管理／請求支払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、予診情報・予防接種記録管理／請求支払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		
予防接種に関する事務		
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 ※		【予防接種に関する事務】 八王子市に住民登録している予防接種法または特措法で定められた予防接種の対象者
	その必要性	八王子市が実施する予防接種情報を適正に管理するため。
④記録される項目		[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・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 [○] 4情報（氏名、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>・予防接種記録情報 ）
	その妥当性	【予防接種に関する事務】 ・個人番号・その他識別情報：対象者を正確に特定するため ・4情報、連絡先、その他住民票関係情報：予防接種法又は特措法に基づく接種対象者であることを確認。通知等の発送、連絡のため。 ・健康・医療関係情報：接種記録の管理、未接種者への接種勧奨を適切に行うため。 【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】 ・識別情報（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…予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。 ・業務関係情報（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、予診情報・予防接種記録管理／請求支払システムが、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29年2月1日
⑥事務担当部署		健康医療部健康づくり推進課

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　（ 市民部市民課、福祉事務所 ） [　] 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　（ 他自治体 ） [○] 民間事業者　（ 医療機関 ） [○] その他　（ 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　（ 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	【予防接種に関する事務】 ・識別情報：随時 ・連絡先等情報：随時 ・業務関係情報（接種情報）：随時 【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】 ・予診情報・予防接種記録管理／請求支払システムが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。 ・本市が予診情報・予防接種記録管理／請求支払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、予診情報・予防接種記録管理／請求支払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、予診情報・予防接種記録管理／請求支払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	【予防接種に関する事務】 ・予防接種履歴の管理を適正に行うために、予防接種の実施に係る情報収集を行う必要がある。 ・健康被害に係る給付を適正に行うために、保険給付の支給や障害基礎年金の支給等に係る情報が必要である。 【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 】 （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、予診情報・予防接種記録管理／請求支払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		【予防接種に関する事務】 ・本人から入手する場合、口頭もしくは予診票等の書面で使用目的を明示している。 【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】 ・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。マイナポータル及び医療機関用アプリ又は医療機関での顔認証端末では、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して、本人確認することにより入手する。
⑥使用目的 ※		【予防接種に関する事務】 ・本市への転入者について、転出元市区町村へ接種記録を照会するために特定個人情報を使用する。
	変更の妥当性	
⑦使用の主体	使用部署 ※	健康医療部健康づくり推進課
	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 ※		【予防接種に関する事務】 ・本市への転入者について、転出元市区町村へ接種記録を照会するために特定個人情報を使用する。 【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】 ・情報連携のため、本市は、予診情報・予防接種記録管理／請求支払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、予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対してオンライン資格確認等システムと予診情報・予防接種記録管理／請求支払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を経由して予診情報・予防接種記録管理／請求支払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診情報・予防接種記録管理／請求支払システムで共有されることで予診情報・予防接種記録管理／請求支払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診情報・予防接種記録管理／請求支払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 ※	【予防接種に関する事務】 ・氏名、生年月日、住所で突合し、接種対象者の確認を行う。
	情報の統計分析 ※	【予防接種に関する事務】 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。 【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】 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 ※	
⑨使用開始日		平成29年2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		【予防接種に関する事務】 総合健診システム保守業務
①委託内容		総合健診システムの保守
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	[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 ※	予防接種法又は特措法に定められる予防接種の対象者
	その妥当性	八王子市が実施する予防接種情報を適正に管理するため。
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 （ システム内で確認 ）
⑤委託先名の確認方法		下記、「⑥委託者名」の項の記載より確認できる。
⑥委託先名		株式会社両備システムズ
再委託	⑦再委託の有無 ※	[再委託しない] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑧再委託の許諾方法	
	⑨再委託事項	

委託事項2		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各事務における特定個人情報ファイルの一部の取扱
①委託内容		予診情報・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
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	[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 ※	予防接種法又は特措法に定められる予防接種の対象者
	その妥当性	予診情報・予防接種記録管理／請求支払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、予診情報・予防接種記録管理／請求支払システムに格納された特定個人情報は、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、東京都国民健康保険団体連合会（以下、東京都国保連合会という。）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。
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		下記、「⑥委託先名」の項の記載より確認できる。
⑥委託先名		東京都国保連合会
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	書面又は電磁的方法による承諾
	⑨再委託事項	【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】 ・予診情報・予防接種記録管理／請求支払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。

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 （ 1 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県知事又は市町村長
①法令上の根拠	番号法第19条第8号別表第2（16の2項）
②提供先における用途	予防接種法又は特措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	予防接種履歴
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	総合健診システムに予防接種の情報が記録されている者
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	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があった都度
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[ ] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[ ] 庁内連携システム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] 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 ※		【予防接種に関する事務】 ＜八王子市における措置＞ 1. データについては、定められた方法により入室管理を行っているサーバー室に設置しているサーバーの内部に保管する。なお、サーバーは施錠可能なラックに格納し、サーバー使用時以外は施錠する。また、サーバーへのアクセスは定められた方法により認証し、限られた者しかアクセスできない。 2. 住民からの届出書等については、施錠可能なキャビネットに保管し、使用時以外は施錠する。 【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保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 2. 特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 【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。 【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】 予診情報・予防接種記録管理／請求支払システムは、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。なお、以下のとおりセキュリティ対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・論理的に区分された当市区町村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。 ・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を利用している。
②保管期間	期間	[5年] ＜選択肢＞ 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	

③消去方法	【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。 【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等にしたがって確実にデータを消去する。 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。 【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】 ・本市の領域に保管されたデータのみ、予診情報・予防接種記録管理／請求支払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

＜予防接種情報ファイル＞

【住民情報】
1.異動事由　2.異動日　3.異動届出日　4.個人番号　5.個人番号予備　6.世帯番号　7.世帯番号予備　8.カナ氏名　9.漢字氏名　10.通称カナ氏名　11.通称名　12.生年月日　13.性別　14.続柄1　15.続柄2　16.続柄3　17.続柄4　18.住民になった日　19.住民になった届出日　20.住民でなくなった日　21.住民でなくなった届出日　22.住定日　23.住定日届出日　24.住民区分　25.外国人判定　26.前住所　27.転出先住所　28.住所コード　29.町内会コード　30.地番　本番　31.地番　枝番　32.地番　末番　33.方書コード　34.方書名称　35.郵便番号　36.住所日本語　37.送付用宛先人氏名　38.送付用予備1　39.送付用予備2　40.送付用予備3　41.送付用予備4　42.送付用予備5　43.個人予備1　44.個人予備5　45.作成日（西暦）　46.外国人住民日　47.第30条45規定区分　48.在留資格　49.在留期間等　50.在留期間等終了日　51.在留カード等番号　52.個人番号　53.統合宛名番号

【乳幼児等】
1.宛名番号　2.接種コード　3.接種回数　4.接種・予診日　5.更新者　6.更新日　7.更新時間　8.年度　9.性別　10.接種日年齢　11.年度末年齢　12.基準日年齢　13.受診時国保区分　14.対象外判定　15.接種判定　16.混合接種　何種　17.請求日（月）　18.実施医療機関　19.接種番号　20.接種会場　21.問診医　22.接種医　23.所属　24.Lot.No　25.接種量　26.発赤　反応長径　27.発赤　反応短径　28.硬結　反応長径　29.硬結　反応短径　30.二重発赤　反応長径　31.二重発赤　反応短径　32.所見　33.判定　34.精密検査結果　35.抗体価検査　36.特記事項　37.未接種理由　38.予診フラグ　39.実施区分　40.受付日　41.自己負担有無　42.集団個別区分　43.特定高齢者候補者区分　44.コースコード　45.支払先コード　46.削除FLG　47.ロックFLG　48.決済済みFLG　49.決済コース　50.予診独自フラグ　51.接種独自フラグ　52.医師の判断　53.肺炎球菌種類

【成人用肺炎球菌・帯状疱疹等】
1.西暦年度　2.宛名番号　3.接種・予診日　4.更新者　5.更新日　6.更新時間　7.性別　8.接種日年齢　9.年度末年齢　10.基準日年齢　11.受診時国保区分　12.請求日（月）　13.実施医療機関　14.接種番号　15.接種会場　16.問診医　17.接種医　18.接種判定　19.lot.No　20.接種量　21.実費徴収区分　22.接種済証交付有無　23.65歳未満接種理由　24.未接種理由　25.予診フラグ　26.接種区分　27.特記事項　28.受付日　29.事故負担有無　30.集団個別区分　31.特定高齢者候補者区分　32.コースコード　33.支払先コード　34.削除FLG　35.ロックFLG　36.決済済みFLG　37.決済コース　38.予診独自フラグ　39.接種独自フラグ　40.医師の判断　41.対象外判定

【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
1.個人番号　2.PMHキー　3.PMH仮名識別子　4.基本5情報（カナ・氏名・住所・生年月日・性別）5.保護者氏名　6.自治体コード　7.自治体業務ID　8.連携ファイル名　9.連携日時　10.連携処理ステータス/エラー内容　11.制御フラグ（リカバリー/不開示/閲覧停止）12.変更区分　13.消除の異動日　14.その他管理番号　15.ID等（予防接種対象者番号）16.その他区分等（接種対象者区分/減免区分）
(2)ユーザー情報
17.機関マスタID　18.機関ユーザーID　19.メールアドレス　20.ユーザー氏名　21.ユーザー区分　22.ユーザー権限ID　23.個人番号閲覧可能フラグ　24.ユーザー削除フラグ
(3)予診票情報
25.項目ID　26.管理ID　27.更新日時　28.回答ID　29.回答内容　30.回答処理ステータス　31.回答日時　32.接種不可フラグ　33.予防接種設定ID　34.予防接種管理ID　35.組み合わせ番号　36.強制失効日　37.勧奨情報（ルールID、勧奨日）
(4)予防接種記録情報
38.予防接種記録ID　39.予防接種管理ID　40.接種日　41.接種同意フラグ　42.医療機関コード　43.医師名　44.実施場所　45.実施区分　46.接種区分　47.GTINコード　48.ワクチンメーカー名　49.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）　50.ロット番号　51.接種量　52.接種部位　53.接種方法　54.ワクチン有効期限　55.要注意接種フラグ　56.特別の事情　57.海外接種フラグ　58.更新日時　59.最新/削除フラグ　60.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	
予防接種情報ファイル	
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	【予防接種事務における措置】 申請等の窓口において申請内容や本人確認書類の確認を行い、対象者以外の情報の入手防止に努める。 【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】 ・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既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムに連携し、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	【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】 ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予診情報・予防接種記録管理／請求支払システムへは、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。
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	【予防接種事務における措置】 Ⅱ 特定個人情報ファイルの概要(住民基本台帳ファイル) 3. 特定個人情報の入手・保管における入手以外は行わない。 【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】 ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予診情報・予防接種記録管理／請求支払システムへは、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。 ・予診情報・予防接種記録管理／請求支払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。
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	【予防接種事務における措置】 窓口で特定個人情報を入手する際は個人番号カード（または免許証、パスポート）等の本人確認書類に基づき、対面で本人確認を行う。 【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】 ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をは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。

個人番号の真正性確認の措置の内容	【予防接種事務における措置】 　上記のとおり本人確認を必ず行うとともに、提供される特定個人情報の正確性についても申告書とシステムに登録された情報を確認して突合を行う。 【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】 ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をは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。
特定個人情報の正確性確保の措置の内容	【予防接種事務における措置】 ・上記のとおり本人確認とともに特定個人情報の照合を行っている。 ・既存住基システムを介し、最新の住所情報等を取得している。 ・入力後は原本と照合を行い、入力内容に誤りがないかをチェックしている。 【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】 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	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	【予防接種事務における措置】 　セキュリティ対策がされたシステムを使用している。また、職員へのセキュリティ教育において、情報の管理についても注意徹底するようにしている。 【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】 ・予診情報・予防接種記録管理／請求支払システムと支払基金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、予診情報・予防接種記録管理／請求支払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、事務に必要のない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	個人番号利用業務以外の業務から住民情報の要求があった場合は、個人番号が含まれない情報のみを提供し、個人番号には一切アクセスできないようアクセス制御を行っている。
事務で使用するその他のシステムにおける措置の内容	【予防接種に関する事務】 権限の管理を行っており、個人番号利用事務実施者以外は、個人番号による検索及び個人番号の参照ができないようシステムで制御している。 【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】 ・予診情報・予防接種記録管理／請求支払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。 ・予診情報・予防接種記録管理／請求支払システムでは、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診情報・予防接種記録管理／請求支払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	1.システムへのログイン記録、個人を特定した検索及び特定後の操作ログの記録を行う。 2.人事異動等によりアクセス権限がなくなる場合は、速やかに利用権限の変更・抹消の処理を行う。
リスクへの対策は十分か	［　十分である　］　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
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	【予防接種に関する事務】 1.ユーザーIDとパスワードにより認証を行う。 2.ユーザーごとに利用可能な機能を制限することで不正利用が行えない対策を実施する。 【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】 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、予診情報・予防接種記録管理／請求支払システムのアクセス権限を管理する管理者を定める。 ・予診情報・予防接種記録管理／請求支払システムのログインはユーザID・パスワードで行う。 ・予診情報・予防接種記録管理／請求支払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。 ・予診情報・予防接種記録管理／請求支払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。 ・既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払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	【予防接種事務における措置】 更新があればその都度、発行、管理をしている。 【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】 ・予診情報・予防接種記録管理／請求支払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	【予防接種事務における措置】 職員の業務内容に応じてシステムのアクセス権限を設定している。年度の途中でも必要があればその都度見直しを行っている。 【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】 ・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	【予防接種事務における措置】 システム操作履歴を記録し、必要な場合には、当該操作に関わるログを確認できるようにしている。 【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		【予防接種事務における措置】 操作ログを取得しているため、業務外利用をした場合には特定可能であることを職員に周知し、業務外利用を抑止している。 【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】 ・本市は、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。 ・本市は、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。
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		【予防接種事務における措置】 　データの移行は許可されたUSBメモリしか利用できない。USBメモリの使用記録や使用後のデータ削除を徹底する。また、USBメモリのウイルスチェックも行う。 【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】 ・既存システム（各業務システム）から特定個人情報を抽出したCSVファイルを予診情報・予防接種記録管理／請求支払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。 ・本市の既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払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。 ・予診情報・予防接種記録管理／請求支払システムでは、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		
【新型コロナウイルス感染症対策に係る予防接種事務における追加措置】 ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。		

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		【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】 本市は、予診情報・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における特定個人情報の取扱いを東京都国保連合会に委託し、東京都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	実務に携わる職員と取扱い範囲を限定している。 【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。
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	ログ等の記録を一定期間保存する。 【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】 ・予診情報・予防接種記録管理／請求支払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	【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】 ・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	VRSまたは市の電子計算機に記録された時に到達したとみなす。 【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】 ・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		[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	不要となったときは速やかに、消去または廃棄しなければならないとしている。 【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】 ・委託契約終了後は予診情報・予防接種記録管理／請求支払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		[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	・第三者に漏えいしてはならない。 ・管理に必要な措置を講ずるものとする。 ・目的の範囲を超える複製、改変の原則禁止。 【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】 東京都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	【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】 ・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、点検結果について東京都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】 ・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

1.委託先における特定個人情報ファイルの不正な閲覧、更新のリスク
①委託に係る実施体制の提出を義務付ける。
②委託業者に対し、機密保持誓約書を提出させる。

2.委託元と委託先間の特定個人情報の不正な提供等のリスク
①八王子市情報セキュリティポリシーにおいて、個人情報を提供する場合は、所属長の許可を必要とする。
②特定個人情報ファイルの委託先への提供時に、セキュリテイ管理者の許可を得た後、定められた方法により暗号化を行う。また、どのような情報をいつだれに提供したか記録を残す。

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		
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	・提供については、番号法第19条各号に該当する場合以外の提供を禁止する。 ・移転については、番号法第9条第2項に基づく条例に規定された事務以外の事務への移転を禁止する。	
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： 不適切な方法で提供・移転が行われるリスク		
リスクに対する措置の内容	【予防接種事務における措置】 ・システムでの提供・移転については、不適切な方法で行われないようシステム上で担保する。 ・システム以外での提供・移転の場合は、複数職員での確認により不適切な方法がおきないよう担保する。	
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： 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	【予防接種事務における措置】 ・システムでの提供・移転については、不適切な方法で行われないようシステム上で担保する。 ・システム以外での提供・移転の場合は、複数職員での確認により不適切な方法がおきないよう担保する。	
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		
【予防接種事務における措置】 ・システムでの提供・移転については、不適切な方法で行われないようシステム上で担保する。 ・システム以外での提供・移転の場合は、複数職員での確認により不適切な方法がおきないよう担保する。		

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	【中間サーバー・ソフトウェアにおける措置】 1.情報照会機能（※1）により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可用照合リスト（※2）との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応する。 2.中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証のほかに、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。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法別表第2及び第19条第15号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
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	【中間サーバー・ソフトウェアにおける措置】 中間サーバーは、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・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 【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（LGWAN等）を利用することにより、安全性を確保する。 2.中間サーバーと団体については仮想専用線等の技術を利用し、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	
リスクに対する措置の内容	【中間サーバー・ソフトウェアにおける措置】 中間サーバーは、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・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
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	【中間サーバー・ソフトウェアにおける措置】 1.中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応する（※）。 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る。 3.情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減する。 4.中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証のほかに、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 【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（LGWAN等）を利用することにより、漏えい・紛失のリスクに対応する。 2.中間サーバーと団体については仮想専用線等の技術を利用し、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する。 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できない。
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	【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ほかに、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（LGWAN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する。 2.中間サーバーと八王子市については仮想専用線等の技術を利用し、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する。 3.中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理する。
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	【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ほかに、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（LGWAN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する。 2.中間サーバーと八王子市については仮想専用線等の技術を利用し、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する。 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	【中間サーバー・ソフトウェアにおける措置】 1.情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応する。 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する。 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システムの原本と照合するためのデータを出力する機能を有する。 （※）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		
【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ほかに、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する。 【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（LGWAN等）を利用することにより、安全性を確保する。 2.中間サーバーと八王子市については仮想専用線等の技術を利用し、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する。 3.特定個人情報を管理するデータベースは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	【八王子市における措置】 1.申請書等について、入力及び照合した後は、施錠できるキャビネットに保管する。 2.セキュリティ区域を明確にし、入退室管理を行う。 3.許可された者のみ、定められた方法によりサーバー室への入室が可能となっている。 4.サーバー室内には監視設備として監視カメラを設置する。 5.バックアップ媒体は、サーバー室内の施錠管理されている場所で保管する。 6.停電（落雷等）によるデータ消失を防ぐため、各サーバーに無停電電源装置を付設する。 7.バックアップ媒体の外部保管委託を行っている。 【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有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。 なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・日本国内でデータを保管している。 【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。 【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】 予診情報・予防接種記録管理／請求支払システムは、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	【八王子市における措置】 1.コンピュータウイルス対策ソフトウェアを導入し、ウイルスチェックを行っている。また、最新の不正プログラムに対応するため、定期的にウイルスパターンの更新を行っている。 2.不正アクセスを防止するため、ファイアウォールを設置する。 3.セキュリティホールの緊急度に応じてセキュリティパッチを適用する。 【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.導入する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。 【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。 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及びミドルウエアについて、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。 【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】 予診情報・予防接種記録管理／請求支払システムは、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。 ・予診情報・予防接種記録管理／請求支払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、予診情報・予防接種記録管理／請求支払システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予診情報・予防接種記録管理／請求支払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。 ・本市の端末と予診情報・予防接種記録管理／請求支払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	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　　2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　　2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[　　発生なし　　]	＜選択肢＞ 1）発生あり　　2）発生なし
その内容	ー	
再発防止策の内容	ー	
⑩死者の個人番号	[　　保管している　　]	＜選択肢＞ 1）保管している　　2）保管していない
具体的な保管方法	生存者の個人番号と同様の方法で保管する。	
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：　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	定期的に総合健診システムのデータベースの更新を行う。 【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】 ・本特定個人情報ファイルの個人情報は、住基及び住民登録外者の異動情報を取得し、内部番号を基に最新の情報に反映されるため、古い情報のまま保管され続けるリスクは存在しない。	
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
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	1.不要となった特定個人情報をシステム内で消去する。 2.ディスク交換やハードウェア更改等の際は、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 3.USBメモリを使用して特定個人情報の提供・移転を行う場合、使用後、速やかにUSBメモリ内のデータを消去する。 【ガバメントクラウドにおける措置】 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。 【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】 ・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		
その他のリスク：他人のIDの使用 そのリスクに対する措置：他人のID等を使用しないように、また他人にID等を使用されないよう厳格な管理について研修を通して職員等に徹底させる。		

Ⅳ　その他のリスク対策 ※

1. 監査		
①自己点検	［　　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
具体的なチェック方法	1.評価書の記載内容どおりの運用ができているか、定期的に自己点検を実施する。 2.運用状況の変更などによる各種マニュアルの見直しを定期的に実施する。 【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する。 【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】 本市は、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
具体的な内容	八王子市情報セキュリティポリシー等に基づき、以下の観点による内部監査を随時実施し、監査結果を踏まえて体制や規定を改善する。 ①評価書記載事項と運用実態のチェック ②個人情報保護に関する規定、体制整備 ③個人情報保護に関する人的安全管理措置 ④職員の役割責任の明確化、安全管理措置の周知・教育 ⑤個人情報保護に関する技術的安全管理措置 【中間サーバー･プラットフォームにおける措置】 ①運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行う。 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。 【ガバメントクラウドにおける措置】 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、ISMAPにおいて、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。 【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】 本市は、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	［　　十分に行っている　　］	＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
具体的な方法	1.研修計画を立て、研修を実施する。 2.全庁的な研修として、職員等については、年に1回以上の情報セキュリティ研修を実施する。 3.人事異動等により新たに配属された職員等に対し、研修マニュアルにより研修を実施する。 4.研修した内容については、職員等の理解度をチェックする。理解度が達していない場合には、繰り返し研修を行い、理解度を高める。 5.セキュリティ事故の情報を庁内で共有する。 6.職員等に対しては、個人情報保護に関する研修の受講を義務付ける。 【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･プラットフォームの運用に携わる従業者及び事業者に対し、セキュリティ研修等を実施する。 2.中間サーバー･プラットフォームの業務に就く場合は、運用規則等について研修を行う。 【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】 本市は、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

個人情報の取扱いに関しては、八王子市個人情報保護条例、八王子市情報セキュリティポリシー等に準ずる。

【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）、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。

　記憶媒体を用いて特定個人情報ファイルを移送する際のリスクとして、次のとおり対策を講じる。
①磁気テープ保管先への移動における紛失リスク：保管委託業者との契約において、その移動中の紛失リスクを減らすため、移動経路、移動方法、取扱人数等に関するセキュリティ上の措置について、契約書に明記する。
②委託先がUSBメモリ等を自社事業所に持ち帰る過程での紛失リスク：特定個人情報ファイルの委託先への提供時に、セキュリティ管理者の許可を得た後、定められた方法により暗号化を行う。また、どのような情報をいつだれに提供したか記録を残す。

【ガバメントクラウドにおける措置】
ガバメントクラウド上での業務データの取扱いについては、当該業務データを保有する地方公共団体及びその業務データの取扱いについて委託を受けるASP又はガバメントクラウド運用管理補助者が責任を有する。
ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。
具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。

【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】
　本市は、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	〒192-0046　東京都八王子市明神町三丁目19番2号　東京たま未来メッセ庁舎・会議室棟5階 八王子市保健所 健康医療部健康づくり推進課 〒192-8501　東京都八王子市元本郷町3丁目24番1号 八王子市役所本庁舎1階　公文書管理課内　情報公開・個人情報保護コーナーでも受け付ける
②請求方法	必要事項を記載した開示・訂正・利用停止に関する請求書を請求先に提出する。
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：手数料は無料。写しを作成する場合はコピー代、郵送する場合は写しの送付に要する費用（コピー代、切手代など））
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	「八王子市個人情保護ファイル」を公表する。事務名は「予防接種に関する事務」である。
公表場所	〒192-8501　東京都八王子市元本郷町3丁目24番1号 八王子市役所本庁舎1階　公文書管理課内　情報公開・個人情報保護コーナーでも受け付ける
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	〒192-0046　東京都八王子市明神町三丁目19番2号　東京たま未来メッセ庁舎・会議室棟5階 八王子市保健所 健康医療部健康づくり推進課 電話042-645-5102
②対応方法	問合せの内容及びその対応について、記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	
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	パブリックコメント
②実施日・期間	令和8年（2026年）7月16日～8月17日
③期間を短縮する特段の理由	期間短縮なし
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	八王子市情報公開・個人情報審議会による第三者点検を実施した。
③結果	八王子市情報公開・個人情報保護審議会において、予防接種に関する事務の特定個人情報保護評価書を審査した結果、特定個人情報保護評価指針の定める実施手順等に適合した評価手続きが実施されており、その内容については評価の目的等に照らし妥当であると認める。
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	