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
19	予防接種事務　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

岡山市は、予防接種事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を発生させるリスクを軽減させるために適切な措置を講じ、もって個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	本評価書は保健管理システムを新システムに移行すること等に伴い、特定個人情報保護評価を再実施したものである。 現行システムの稼働期間中は令和7年8月8日公表の評価書の内容も併せて、適切に特定個人情報を取り扱う。

評価実施機関名

岡山県岡山市長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

［令和7年5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	予防接種事務
②事務の内容　※	予防接種事務は、定期及び新型インフルエンザ特別措置法に基づく予防接種等の実施や結果の管理を行うものである。 予防接種法、新型インフルエンザ特別措置法及び行政手続における特定の個人を識別するための番号の利用等に関する法律（以下「番号法」という。）の規定に従い、特定個人情報を以下の事務において取り扱う。 ①予防接種に関する記録 ・定期及び新型インフルエンザ特別措置法に基づき予防接種を行ったときは、予防接種の記録を作成することとなっており、実施後は記録を作成しその保存を行う。 ②A類疾病に係る予防接種対象者の管理 ・A類疾病に係る定期の予防接種の対象者には、予防接種手帳を発行し、対象者の管理を行う。 ③A類疾病に係る定期の予防接種対象者への個別通知による接種勧奨 ④B類疾病に係る定期の予防接種に対する被接種者自己負担金の減免 ・自己負担金の減免を行う場合は申請に基づき対象の確認を行い、要件に合致するものに対し自己負担金の減免券を発行する。 ⑤新型インフルエンザ予防接種の対象者の把握・特定と管理を行う。 ⑥予防接種に係る費用の支払い ・岡山市が実施した定期の予防接種に係る費用を実施した医療機関へ支払うための集計を行う。 ⑦新型コロナウイルスワクチン特例臨時接種に関する記録 ・予防接種の接種記録等を管理する。 ⑧予防接種による健康被害が生じた場合の健康被害救済の給付 ・予防接種等を受けた者が疾病にかかり、障害の状態又は死亡に至った場合に、定められた医療費及び医療手当の給付を行う。 番号法においては、主務省令第2条の表に基づいて情報保有機関は情報提供ネットワークシステムに接続し、各情報保有機関が保有する個人情報について情報連携を行うことが必要とされている。 健康管理システムと共通基盤システムの間でデータ（副本）の受け渡しを行い、共通基盤システムが中間サーバを介して（※1）、情報提供ネットワークシステムと接続することで、符号の取得（※2）や各情報保有機関で保有する特定個人情報の照会と提供等を実現する。 （※1）岡山市では、共通基盤システムが庁内連携・団体内統合宛名システムとしての機能を有し、一括して中間サーバーとの情報連携を行う。 （※2）セキュリティの観点により、特定個人情報の照会と提供の際は「個人番号」を直接利用せず「符号」を取得して利用する。 ＜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＞ ・本市区町村は、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。 ・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。 ・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。 ・本市区町村は、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	健康管理システム（健康かるて）
②システムの機能	①発行管理 ・予防接種手帳やクーポン券等の発行管理を行う。 ・B類予防接種自己負担金減免券の発行管理を行う。 ②対象者管理 ・A類予防接種対象者の中で個別勧奨を行う対象者の抽出を行う。 ③接種者入力 ・予防接種の実施後の記録の入力を行う。 ④接種履歴 ・予防接種の記録情報の確認を行う。 ⑤各種統計資料作成 ・予防接種の記録を基に各種統計資料の作成を行う。
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2～5	
システム2	
①システムの名称	共通基盤システム（庁内連携機能・団体内統合宛名機能、番号制度情報連携機能）
②システムの機能	1. システム間連携機能 :庁内業務システム間のデータを連携する機能。 2. 運用管理機能 :外字配信、リモート管理、時刻同期、ウィルス管理、パッチ管理等を管理する機能。 3. 共通インフラ機能 :共有ファイルサーバー及びファイヤーウォール設定を管理する機能。 4. 認証管理機能 :シングルサインオン、アカウント管理等の認証を管理する機能。 5. 団体内統合宛名管理機能 :団体内統合宛名番号管理する機能及び符号取得を実現する機能。 6. 番号制度情報連携機能（システム間連携） :業務システム⇔中間サーバ間の情報連携データを中継する機能。 7. 番号制度情報連携機能（オンライン機能） :オンライン画面にて情報連携を実現する機能。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [○] その他　（ 中間サーバー、庁内各業務システム　）

システム3	
①システムの名称	中間サーバーシステム
②システムの機能	1．符号管理機能 ：情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 2．情報照会機能 ：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．情報提供機能 ：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．既存システム接続機能 ：中間サーバーと既存システム、団体内統合宛名システム及び住基システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携するための機能。 5．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、管理する機能。 6．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・管理する機能。 7．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ための機能。 8．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用照合リスト情報を管理する機能。 9．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)へのアクセス制御を行う機能。 10．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　（　　）

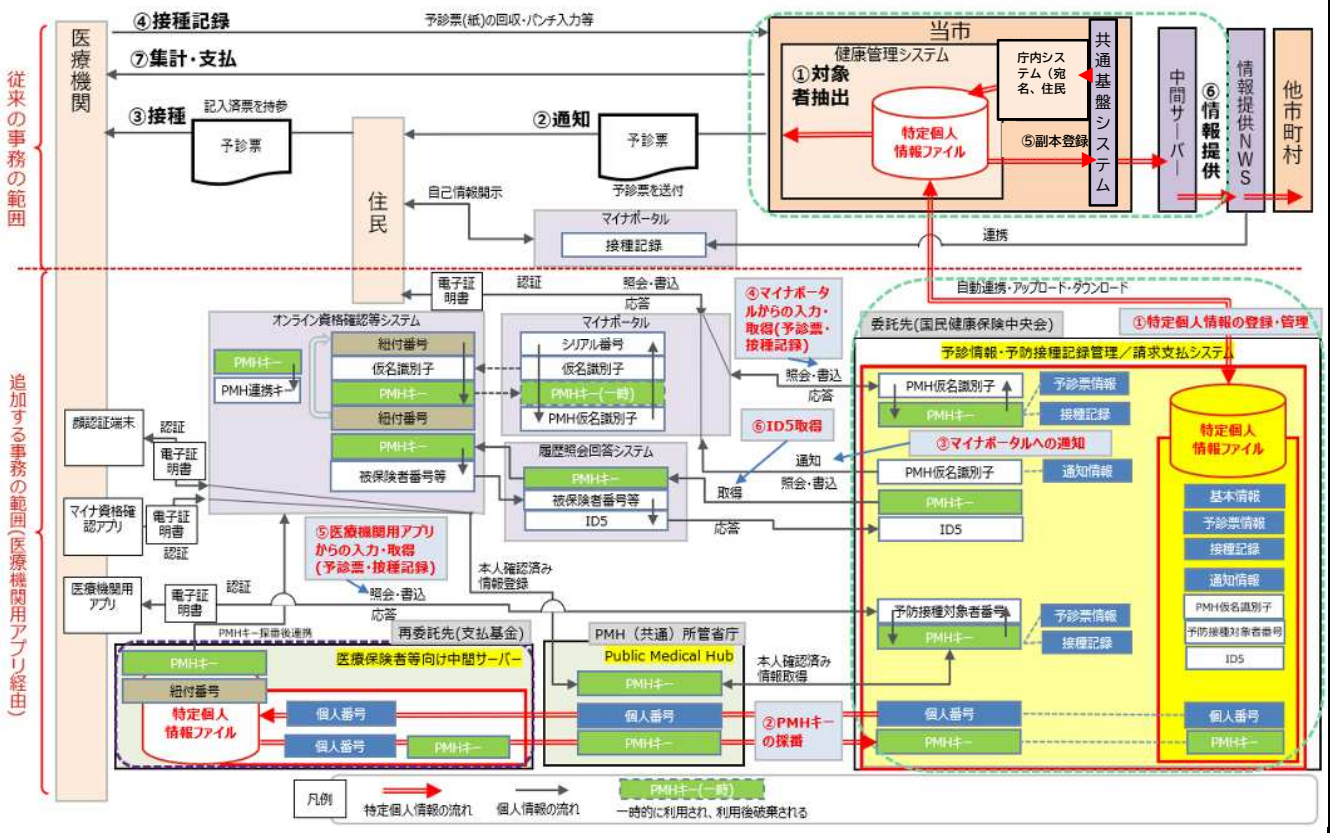
システム4	
①システムの名称	予診情報・予防接種記録管理／請求支払システム
②システムの機能	＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ ①予防接種関連データの登録機能 本市区町村は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市区町村で管理している個人番号、対象者情報、予診票情報及び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　（健康管理システム、マイナポータル、医療機関アプリ、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	
予防接種特定個人情報ファイル	
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	予防接種法に基づく予防接種の実施を適正に実施するため。
②実現が期待されるメリット	接種記録を把握することで、誤った時期・年齢・回数及び接種間隔による接種を防止し、健康被害の発生を防ぐ。
5. 個人番号の利用　※	
法令上の根拠	番号法第9条第1項　別表14、126の項 番号法第19条第6号 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	【情報照会】 番号法第19条第8号に基づく主務省令　第2条の表25、27、28、29、153の項 【情報提供】 番号法第19条第8号に基づく主務省令　第2条の表25、26、153、154の項
7. 評価実施機関における担当部署	
①部署	保健所感染症対策課
②所属長の役職名	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保健管理システムから予防接種対象者を抽出
②予防接種対象者への個別通知による接種勧奨
③予防接種の実施
④接種記録の作成・保存
⑤予防接種情報の副本登録
⑥他市町村へ情報提供
⑦予防接種に係る費用の支払い

＜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＞
①特定個人情報の登録・管理
・本市区町村は、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）
・本市区町村は予診情報・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、本市区町村は予診情報・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		
予防接種特定個人情報ファイル		
2. 基本情報		
①ファイルの種類 ※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲 ※		予防接種の被接種者及び接種対象者
	その必要性	正確かつ適正な予防接種履歴の管理保管を行うに当たり、上記の範囲全てを対象にする必要がある。
④記録される項目		[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
	主な記録項目 ※	・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	・5情報：本人確認のため必要 ・その他識別番号（内部番号）：個人番号との紐付けに必要。 ・その他住民票関係情報、地方税関係情報：自己負担額減免申請確認資料として必要 ・健康医療関係情報：接種記録として管理するために必要 ＜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28年1月1日
⑥事務担当部署		保健福祉局保健所感染症対策課

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　（ 区政推進課、課税管理課 ） [○] 行政機関・独立行政法人等　（ デジタル庁 ） [○] 地方公共団体・地方独立行政法人　（ 他市区町村 ） [○] 民間事業者　（ 医療機関 ） [○] その他　（ 支払基金、国保連合会 ）
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、マイナポータル ）
③入手の時期・頻度	①市内在住者 ・住民の個人番号については、住民記録システムで異動した際に連携し入手する。 ・予防接種の記録については、接種を行った医療機関から月次単位で入手する。 ②市外での接種記録 ・転入手続き時、紙書類（親子手帳の写し等）により入手。 ③予防接種健康被害救済請求 ・申請の都度、紙書類により入手 ④口座登録・連携ファイル関係情報（公金受取口座情報） ・申請の都度、本人による利用希望の意志表示がある場合に随時入手。 <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。 ・本市区町村が予診情報・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、本市区町村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	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） 本市区町村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		予防接種事務における住民基本情報の利用は、番号法及び予防接種法施行規則により明示されている。 本人及び代理人から入手する情報は、書面にて利用目的を明示する。 <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 ※		定期予防接種事実施に係る年齢等接種対象者の要件を正確に把握する必要があるため
	変更の妥当性	—
⑦使用の主体	使用部署 ※	保健福祉局保健所感染症対策課、健康づくり課
	使用者数	[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
⑧使用方法 ※		・予防接種手帳の発行管理 ・B類予防接種自己負担金減免券の発行管理 ・A類予防接種対象者の中で個別勧奨を行う対象者の抽出 ・予防接種の実施後の記録の入力 ・予防接種の記録情報の確認 ・予防接種の記録を基に各種統計資料の作成 ・健康被害救済給付認定申請時の資格確認（住基情報及び接種歴） <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、本市区町村は、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 ※	健康管理システムの内部管理番号と収集した個人情報の内容との突合を行う。
	情報の統計分析 ※	接種状況調査などの統計分析の実施 （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28年1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（健康かるて）保守運用業務委託
①委託内容		健康管理システム（健康かるて）全体の運用及び保守業務を委託する
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 ※	予防接種法等関係法令に定められる予防接種の対象者
	その妥当性	システムの運用・保守作業を実施するために特定個人情報保護ファイル全体を委託の対象にする必要がある。
③委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		岡山市契約情報公開基準に基づく公表及び岡山市情報公開条例に基づく契約書の開示請求により確認することができる。
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2～5		
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　※	予防接種法等関係法令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、岡山県国民健康保険団体連合会（以下、岡山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。
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		岡山県国民健康保険団体連合会
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・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 （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	都道府県知事または市区町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令 第2条の表25、26の項
②提供先における用途	予防接種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	定期予防接種履歴がある他市区町村への転出者
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のあった都度
提供先2～5	
提供先2	厚生労働大臣、都道府県知事または市町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令 第2条の表153、154の項
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	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	新型インフルエンザ等対策特別措置法による予防接種履歴がある他市区町村への転出者
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のあった都度

6. 特定個人情報の保管・消去		
①保管場所　※		＜共通基盤システムにおける措置＞ ・共通基盤システムは、岡山市の管理するデータセンターに設置しており、データセンターへの入館及びサーバー室への入室を厳重に管理している。 ・特定個人情報は、サーバー室に設置された共通基盤システムのデータベース内に保存され、バックアップは共有ストレージ及びLTO媒体に保存される。 ＜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。 <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。 ＜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。
②保管期間	期間	[　　20年以上　　] ＜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	・予防接種法施行令第6条の2において、予防接種に関する記録は少なくとも5年間保存しなければならないと規定されており、市民からの接種歴確認の問い合わせに対応するため長期間保管する必要がある。

③消去方法	＜予防接種事務＞ 予防接種は、ワクチンに応じ接種回数及び接種間隔が定まっており、かつ接種対象年齢が幅広いため、市民からの接種歴確認の問い合わせに対応する必要があることから、健康管理システム上の接種歴は消去しない。 ＜共通基盤システムにおける措置＞ ・共通基盤システムに格納する特定個人情報は、各業務システムの副本データであるため、消去のタイミング等は各業務システム（事務）の運用に準ずる。 ・ディスク交換やハード更改等の際は、共通基盤システムの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊によりデータを完全に消去する。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー･プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（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〉 ・本市区町村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。 ・本市区町村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。 ＜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。

7. 備考

－

（別添２）特定個人情報ファイル記録項目

1,整理番号 2,氏名カナ 3,氏名漢字 4,生年月日 5,性別 6,町丁目 7,番地 8,枝 9,小枝 10,住所 11,方書
12,電話番号 13,世帯番号 14,郵便番号 15,続柄１ 16,続柄２ 17,続柄３ 18,続柄４ 19,取消 20,予備１
21,予備２ 22,予備３ 23,行政区番号 24,住登外フラグ 25,外国人フラグ 26,外国人本名カナ
27,外国人本名漢字 28,小学校 29,中学校 30,国保区分 31,徴収区分 32,課税区分 33,年金区分 34,生保区分
35,住民となった日 36,住民でなくなった日 37,異動 38,異動年月日 39,住民異動 40,住民異動年月日
41,管理番号 42,転入前住所 43,転入前方書 44,転出後住所 45,転出後方書 46,外国人本名使用フラグ
47,集配局 48,届出年月日 49,介護区分 50,後期高齢区分 51,予備４ 52,予備５ 53,予備６ 54,予備７
55,予備８ 56,予備９ 57,送付先住所使用フラグ 58,町丁目２ 59,番地２ 60,枝２ 61,小枝２ 62,住所２ 63,方書２
64,電話番号２ 65,郵便番号２ 66,行政区番号２ 67,小学校２ 68,中学校２ 69,転入前行政区 70,転居日
71,医療機関番号 72,施設番号 73,社会保険番号 74,請求区分 75,医療機関漢字名称 76,医療機関カナ名称
77,郵便番号 78,住所 79,方書 80,電話番号 81,FAX番号 82,市町村コード 83,所在地区分 84,銀行法人名コード
85,銀行支店名コード 86,預金種別 87,口座番号 88,名義人カナ 89,名義人漢字 90,備考 91,取消フラグ
92,医療機関種類 93,健診機関コード 94,口座情報備考 95,整理番号 96,事業番号 97,期・回数区分 98,予防枝番
99,年度 100,事業予定連番 101,受診日 102,会場その他 103,受診種別 104,登録日 105,負担金区分
106,接種医療機関番号 107,接種医療機関その他 108,小学校区分 109,中学校区分 110,接種区分 111,Lot番号
112,接種量 113,ツ反結果区分 114,反応状態区分 115,長径 116,印刷区分 117,印刷日 118,印刷区分（勧奨はがき用）
119,印刷日（勧奨はがき用）120,印刷区分（再勧奨用）121,印刷日（再勧奨用）122,予診医医療機関番号
123,予診医番号 124,接種医医療機関番号 125,接種医番号 126,予診医職員ID 127,予診医職員枝番 128,接種医職員ID
129,接種医職員枝番 130,ワクチンメーカー名コード 131,予診理由 132,備考 133,登録区 134,報告月 135,送付番号
136,健診票番号 137,登録区分 138,医師会コード 139,無効フラグ 140,整理番号 141,年度 142,交付区分
143,交付場所 144,交付理由 145,申請日 146,登録日 147,備考 148,登録区 149,整理番号 150,年度 151,交付区分
152,交付場所 153,交付理由 154,申請日 155,登録日 156,備考 157,登録区 158,申請日 159,交付日
160,登録日 161,備考 162,登録区 163,整理番号 164,年度 165,枝番 166,交付番号 167,交付区分 168,交付場所
169,却下理由 170,発行区分 171,課税有無 172,申請日 173,交付日 174,登録日 175,備考 176,登録区

＜新型コロナウイルスワクチン特例臨時接種に係る予防接種事務＞
・個人番号
・宛名番号
・自治体コード
・接種券番号
・属性情報（氏名、生年月日、性別）
・接種状況（実施／未実施）
・接種回
・接種日
・ワクチンメーカー
・ロット番号
・ワクチン種類（※）
・製品名（※）
・旅券関係情報（旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号）（※）
・証明書ID（※）
・証明書発行年月日（※）
※　新型コロナウイルス感染症予防接種証明書の交付に必要な場合のみ

＜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

・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	
予防接種特定個人情報ファイル	
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	＜健康管理システムにおける措置＞ ・住民、他自治体、医療機関等から入手する申請情報・予防接種実施情報は窓口担当部署の職員による受付、事務担当部署職員による郵送受付等、限定した部署で直接入手することとして、目的外の入手を防止している。 ＜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＞ ・医療機関の受付窓口で本人確認の後、医療機関用アプリ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	＜健康管理システムにおける措置＞ ・情報登録の際には、必要な情報以外の登録を行わないように、二重チェックを実施する。 ・必要な情報以外の登録ができないように、健康管理システムにおいて入力項目等の制御を行っている。 ・ユーザIDによる識別とパスワードによる認証、利用可能な機能の制限等により、権限を有しない者による目的外の入手を防止する。 ＜庁内システム間連携による入手（共通基盤システム庁内連携機能経由）における措置＞ 庁内連携による入手の場合、データ提供元の担当課と入手内容を予め合意している。システム間連携においては予め取り決めた内容以外の情報を入手することはできない。 ＜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、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	＜健康管理システムにおける措置＞ ・届出等を受ける場合は、法令等により定められた様式に限る。また、本人の個人番号カード、通知カード又は身分証明書の提示や窓口での聞き取りにより、本人確認を行う。 ・本人の代理人による申告、届出等を受ける場合は、必要に応じて委任状等の確認を行う。 ・ユーザIDによる識別とパスワードによる認証、利用可能な機能の制限等により、不適切な方法による入手を防止する。 ＜庁内システム間連携による入手（共通基盤システム庁内連携機能経由）における措置＞ 庁内連携による入手の場合、データ提供元・提供先の担当課間で入手方法（方式、頻度、タイミングなど）を予め合意している。システム間連携においては予め取り決めた方法以外で情報を入手することはできない。 ＜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	・本人から届出等を受ける場合は、本人の個人番号カード、通知カード又は身分証明書の提示や窓口での聞き取りにより、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	・提出された書類に記載された個人番号と、システムで保有している情報に相違がある場合は、住民基本台帳ネットワークシステム等を利用し、個人番号の真正性の確認を行う。 ＜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	＜健康管理システムにおける措置＞ ・各種届出等は、提出された原本と入力内容を突合しチェックしている。 ＜庁内システム間連携による入手（共通基盤システム庁内連携機能経由）における措置＞ 庁内連携による入手の場合、共通基盤システムのシステム間連携機能により、情報の移転元業務システムと共通基盤システム及び移転先業務システムで同期を取る仕組みとなっており、情報の順序性・正当性・正確性等を担保している。また、システム間連携データは連携の途中で更新することはできないため、誤った情報に上書きする恐れはない。 ＜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＞ 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が漏えい・紛失するリスク	
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＞ ・窓口においては、職員が書類を直接受理し、入力処理など次の処理過程に責任を持って引き継いでいる。 ・特定個人情報を記録した紙媒体は定められた保管場所で施錠管理等を行い、漏洩・紛失を防止する。保管場所の鍵は、権限をもった者（係長級以上の職員）が管理を行う。 ＜庁内システム間連携による入手（共通基盤システム庁内連携機能経由）における措置＞ 庁内連携による入手の場合、共通基盤システムのシステム間連携制御機能を使用し、連携データがロストしない仕組みを構築している。（何らかの事情でロストが発生した場合は連携エラーとなる仕組みを講じている。） ＜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		＜共通基盤システム（番号制度アプリケーション機能）における措置＞ 共通基盤システムの統合宛名システム機能は符号取得専用の機能であり、各業務システムにむけて宛名情報を連携しない仕組みとしている。このため、事務に必要のない情報と紐付けを行うことはできない。
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＞ ・個人番号と紐付けて管理する情報は業務上必要な情報にシステムの機能として限定しているため、その他の情報と紐付けが行われることはない。 ・番号制度に関する事務（システム）以外からは予防接種情報ファイルを直接参照できないよう、アクセス制御対策を実施している。 ・番号利用事務以外で個人番号が取得されることのないように、番号利用事務（システム）以外で個人番号での検索を行うことはできない。また、番号利用事務（システム）以外では個人番号は画面表示されない。 ＜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＞ ・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区町村の職員について、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		―
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	・対象業務システムを利用する端末は、生体認証及びパスワードによる認証を行っている。 ・対象業務システムを利用する職員を特定し、職員ごとに利用可能な機能を制御（アクセス制御）している。 ・認証に使用するパスワードは、定期的に変更する運用を行っている。 ＜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＞ 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。 ・本市区町村は、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	＜健康管理システムにおける措置＞ ・アクセス権限の発効及び失効は、システム管理者または代理の者が行うため、その他の者が自由に発効及び失効を行うことができない。 ・年度当初に人事情報を元にアクセス権限の一括更新を行い、人事異動や退職等による権限の発効及び失効を実施する。 ・年度途中にアクセス権限の変更が必要な場合は、システム管理者または代理の者が速やかに権限の発効及び失効を行う。 ＜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。 ・本市区町村において、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＞ ・ユーザIDごとのアクセス権限については、システム管理者が管理を行っている。 ・アクセス権限については、システム管理者が定期的に確認を実施している。 ＜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＞ ・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＞ ・システムの操作履歴（アクセスログ（失敗時を含む）・操作ログ）を記録する。 ・不正な操作が無いことについて、操作履歴により適時確認する。 ＜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＞ ・本市区町村は、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		・従事者の利用可能な権限を事務分担に応じて、制限している。 ・システム利用職員への研修（情報セキュリティ研修等）において、事務外利用の禁止等について指導する。 ・職員以外の従事者（委託先等）には、当該事項について個人情報の取扱委託に関する覚書及び特定個人情報の取扱委託に関する覚書を締結し、従事者への周知・徹底を義務付けている。 ・システムの操作履歴（アクセスログ）を記録し、定期的にチェックを行う。 ＜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＞ ・本市区町村は、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。本市区町村は、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。 ・本市区町村は、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	・特定個人情報ファイルの複製は必要最低限とし，実施を特定の環境のみに制限する。また，職員に対しては，情報セキュリティ研修を行うとともに，目的外のファイル複製を行わないよう指導する。 ・委託先に対して、個人情報の取扱委託に関する覚書及び特定個人情報の取扱委託に関する覚書を締結し、従事者への周知・徹底を義務付けている。 <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> ・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。 ・本市区町村の既存システム（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	
その他、特定個人情報の使用にあたり、以下の措置を講じる。 ・スクリーンセーバー等を利用して、長時間にわたり特定個人情報を表示させない。 ・端末のディスプレイを、来庁者から見えない位置に置く。 ・個人番号が表示された画面のハードコピーの取得は事務処理に必要となる範囲にとどめ、事務処理完了後にはシュレッダーにて裁断する等、復元できない方法により廃棄する。	

4. 特定個人情報ファイルの取扱いの委託		[　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		委託業者との間で、個人情報の取扱委託に関する覚書及び特定個人情報の取扱委託に関する覚書を締結し、個人情報受託管理責任者の指定及び情報資産を取り扱う全ての従事者名簿（所属、氏名、作業内容、取り扱う情報資産等）の提出を義務付けている。 〈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〉 本市区町村は、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岡山県国保連合会に委託し、岡山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	・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とパスワードにより認証している。 〈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〉 ・本市区町村がアクセス権限の管理状況を確認できる。 ・本市区町村は、アクセス権限を付与する者を必要最小限に限定する。 ・本市区町村は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本市区町村は、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	委託側において利用するユーザIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。 〈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、本市区町村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	・個人情報の取扱委託に関する覚書及び特定個人情報の取扱委託に関する覚書において、保有個人情報の外部提供の禁止を明記している。 ・保有個人情報の管理状況について、必要に応じて検査を実施する。 〈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〉 ・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。 ・本市区町村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	委託している業務については、庁舎内の限られた場所の専用PCを使用して作業を実施しているため、特定個人情報を委託先には提供していない。 〈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〉 ・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。 ・本市区町村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	・委託業務終了後は、返還、物理的破壊により完全に消去しなければならない。 ・委託業者が個人情報ファイルの消去を実施する場合は、その処理内容について報告書を提出させる。 〈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、本市区町村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	委託契約書において、個人情報の取扱委託に関する覚書及び特定個人情報の取扱委託に関する覚書を締結するよう義務付けており、覚書において、以下のことを明記している。 ・保有個人情報の適正管理について最大限の注意を払い、漏えい及び毀棄等の事故を防止するための対策を講じること。 ・保有個人情報を適切に管理するため、個人情報受託管理責任者を置くこと。 ・個人情報の重要性についての認識を深めるとともに、保有個人情報の適正な取扱いに資するための研修・教育を実施すること。 ・保有個人情報をみだりに他人に知らせてはならないこと。 ・原則として、保有個人情報の取扱いの委託の全部又は一部を再委託しないこと。再委託する場合は、あらかじめ書面により申請し、承認を受けること。 ・保有個人情報を不正に利用し、又は毀棄等をしないこと。 ・保有個人情報を、他の従事者（担当以外の者） 及び部外者に提供しないこと。 ・契約に基づいて個人情報を収集する場合は、受託業務の範囲を超えて収集してはならないこと。 ・保有個人情報を複写し、又は複製しないこと。 ・保有個人情報に関し事故が発生したときは、速やかに報告すること。 ・覚書に定める事項に関する遵守状況について、必要に応じて報告させ、又は実地調査することができる。 〈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〉 岡山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
再委託先による特定個人情報ファイルの適切な取扱いの確保		[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
	具体的な方法	再委託する場合は、あらかじめ書面により申請し、承認を受けることとする。 〈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〉 ・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、点検結果について岡山県国保連合会及び本市区町村に年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	
―	

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		

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	＜予防接種事務における措置＞ 照会時に課内決裁を取ることや照会結果記録の定期的な事後チェックを行うことで目的外の入手が行われない措置を講じている。 ＜健康管理システムにおける措置＞ （業務システム側から共通基盤システムを介して情報照会を行う場合） ・ユーザIDによる識別とパスワードによる認証、情報提供ネットワークシステムへの情報照会が可能な権限の制限等により、不正な操作による情報漏えいを防止している。 ・特定個人情報ファイルの情報照会は、共通基盤システムへの通信に限定している。 ＜共通基盤システム（番号制度情報連携機能）における措置＞ ・事務担当課と事務手続きの対応表を作成し、システムに設定している。これにより目的外の情報照会を制限している。 ・共通基盤システムのシステム間連携制御機能により、予め連携機能開発したシステム以外からの情報照会依頼を許可しない措置を講じている。 ＜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、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提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバーの職員認証・権限管理機能（※3）では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※1）情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 （※2）番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。
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	＜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情報連携は、共通基盤システムへの通信に限定し、システムログ（連携日時等）としてストレージに5年間記録している。また、必要に応じてシステム管理者が記録の確認を行う。 ・ストレージを廃棄する際は保存された情報が読み出しできないよう、保管データはKMS（Key Management Service）による暗号化を実施し、システムの利用を停止する段階で、暗号鍵の削除による暗号化消去を行う。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣（デジタル庁）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（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。 ＜本市における全庁的な措置＞ ・本市の中間サーバ連携用サーバは専用のDMZ区画に設置している。また、中間サーバ連携用サーバとの通信は共通基盤システムに限定することで庁内からの不正な通信を遮断するなどして、安全性を確保している。 ・間接的に中間サーバと情報連携を行う各業務システムは番号利用事務系ネットワークに接続しており、インターネット系ネットワークとは論理的に分離することで安全性を確保している。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク3： 入手した特定個人情報が不正確であるリスク	
リスクに対する措置の内容	＜共通基盤システム（番号制度情報連携機能）における措置＞ ・情報照会機能により中間サーバーに情報照会を行う際には、共通基盤システムにおいて照会結果の改変を行わないことで、中間サーバーから入手した情報と同一であることを担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣（デジタル庁）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	＜健康管理システムにおける措置＞ ・ユーザIDによる識別とパスワードによる認証、利用可能な機能の制限等により、権限を有しない者による目的外の情報登録による入手を防止している。 ・特定個人情報ファイルの情報連携は、共通基盤システムへの通信に限定し、システムログ（連携日時等）としてストレージに5年間記録している。また、必要に応じてシステム管理者が記録の確認を行う。 ＜共通基盤システム（番号制度情報連携機能）における措置＞ ・中間サーバーから入手した情報照会結果を業務システムに連携する場合、システム間制御機能にて照会依頼元の連携先システムに連携している。人手を介していないため、誤った業務システムにデータが連携されたり、データを紛失することはない。 ・共通基盤システムのオンライン機能ではアクセス権限設定等により、各事務担当者が入手可能な特定個人情報の制限を行っている。 ・認証管理機能により、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。 ・システムを一定時間使用しなかった場合、自動的にシステムからログアウトする設定としている。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（※）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に結果情報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している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはなない。
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	＜全庁的な措置＞ ・情報提供機能は既存システムには実装せず、中間サーバ・ソフトウェアのみ実装しているため、職員、あるいは既存システムが不正な情報提供を行うことはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（※）により、情報提供ネットワークシステムにおける照会許可用照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可用照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報が不正に提供されるリスクに対応している。 ③機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報が不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （※）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。
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	＜全庁的な措置＞ ・情報提供機能は既存システムには実装せず、中間サーバ・ソフトウェアのみ実装しているため、職員、あるいは各システムが不正な情報提供を行うことはできない。 ＜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＞ ・情報登録の際には、誤った情報の登録を行わないように、二重チェックを実施する。 ・システムの機能により、項目ごとの入力制限（ありえない入力パターンの制限等）や登録前の論理チェックを実施する。 ・特定個人情報ファイルの情報連携は、共通基盤システムへの通信に限定する。 ＜全庁的な措置＞ ・情報提供機能は既存システムには実装せず、中間サーバ・ソフトウェアのみ実装しているため、職員、あるいは各システムが不正な情報提供を行うことはできない。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、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、提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（※）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （※）特定個人情報を副本として保存・管理する機能。
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	＜健康管理システムにおける措置＞ ・特定個人情報を保管するサーバーは、国が推奨するガバメントクラウドに構築し、無停電電源装置の設置、空調管理、耐震・耐火措置等の災害・事故対策をクラウド事業者が行う。 ・特定個人情報を取り扱う業務端末は、セキュリティワイヤによる盗難防止措置を行い、時間経過による画面ロック等のセキュリティ対策を行うこととしている。 ＜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・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。・事前に申請し承認されていない物品、記録媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 <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 ＜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。	
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
	＜健康管理システムにおける措置＞ ・各システ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。 ・各システムではファイアーウォールを導入し、不正アクセス対策を行う。 ・各システムではアクセス制限を行うとともに、必要に応じてログの解析を行う。 ・各システムにて導入している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。 ＜全庁共通の措置（情報連携に使用する端末における措置）＞ ・マイナンバー系ネットワークに接続し、インターネット系やLGWAN接続系端末とは物理的に異なる端末を使用している。 ・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。 ・外部記憶媒体等への書き出しは原則として禁止し、制限している。 ・マイナンバー系ネットワークの各データファイルは自動的に暗号化される仕組みとしている。このため、所定の復号化ソフトを導入していない端末からはデータファイルの中身を閲覧することはできない。 ＜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。・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。・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。 <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>	

	具体的な対策の内容	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。 ・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。 ・本市区町村の端末と予診情報・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。 ・本市区町村の端末と予診情報・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。 ＜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。
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		[　発生あり　] ＜選択肢＞ 1）発生あり　2）発生なし
	その内容	R6.3　旧システムから新システムへのデータ移行不備により、一部データ項目に不具合が生じ、市内対象者に他人の電話番号が印字されたハガキを発送した。
	再発防止策の内容	旧システムから登録データ全件の一覧を出力し、移行元データを再度突合する。 差異があったものについて差異の理由を確認する。 今後、ハガキ出力前にはデータの妥当性の確認を行う。
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	死者の個人番号は、生存者の個人番号と同様の保管、管理を行う。
その他の措置の内容		・ストレージ及び外部媒体を廃棄する際は保存された情報が読み出しできないよう、物理的破壊により完全に消去する。 ・特定個人情報が記載された書類は、施錠ができるロッカーで管理している。
リスクへの対策は十分か		[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている

リスク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	・氏名、住所等の共通宛名情報については、住民記録システムより自動的に異動データを日次連携することにより、最新化する。 ・情報の登録・更新が必要な事象が発生した場合は、担当者が速やかに処理を実施する。 <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	システム管理者の指示を受けた運用管理者が、保管期間を経過したデータについて、個別ファイルごとに、適宜システムから消去する。 <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。 ＜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。
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	
ストレージ及び外部媒体を廃棄する際は保存された情報が読み出しできないよう、物理的破壊により完全に消去する。	

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	＜予防接種事務における措置＞ ・評価書に沿った運用がなされているか、年1回の自己点検でチェックを行う。 ＜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＞ 本市区町村は、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	＜予防接種事務における措置＞ ・特定個人情報に関する監査又は情報セキュリティに関する監査を概ね5年周期で実施する。 ＜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。 ＜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＞ 本市区町村は、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。 ＜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。
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	＜岡山市における措置＞ ・職員に対し、特定個人情報保護研修及び情報セキュリティ研修を年1回以上実施する。 ・委託業者に対し、個人情報の取扱委託に関する覚書を締結し、従事者への研修・教育の実施を義務づける。 ＜中間サーバー・プラットフォームにおける措置＞ ①IPA（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材を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。 ＜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＞ 本市区町村は、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		
＜岡山市における措置＞ ・職員に対し、特定個人情報保護研修及び情報セキュリティ研修を年1回以上実施し、保有個人情報を不正に取り扱った場合の罰則適用等について周知する。なお、違反行為を行った者に対しては、指導を行う。 ・委託業者に対し、個人情報の取扱委託に関する覚書を締結し、従事者への研修・教育の実施や保有個人情報を不正に取り扱った場合の罰則適用等の周知を義務付ける。		

＜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・プラットフォームを活用することにより、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。

＜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＞
本市区町村は、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。

＜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。

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		岡山市総務局総務部行政事務管理課情報公開室 700-8544　岡山県岡山市北区大供一丁目1番1号 問い合わせ先電話番号　086-803-1083
②請求方法		指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
	特記事項	請求方法、指定様式等について岡山市ホームページ上で表示
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	個人情報ファイル簿（予防接種業務で取り扱ったファイル）
	公表場所	岡山市役所本庁舎　2階西側　行政資料室
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		岡山市保健福祉局保健所感染症対策課 700-8546　岡山市北区鹿田町一丁目1番1号 問い合わせ先電話番号　086-803-1262
②対応方法		問い合わせの受付時に受付票を起票し、対応について記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	
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	岡山市パブリックコメント実施要綱に基づきパブリックコメントによる意見聴取を実施する。パブリックコメントの実施に際しては、市ホームページ及び本庁、各区役所にて全文を閲覧できるようにする。
②実施日・期間	
③期間を短縮する特段の理由	_
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	岡山市行政不服・情報公開・個人情報保護審査会による審査
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	