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
6	予防接種の実施等に関する事務

個人のプライバシー等の権利利益の保護の宣言

福山市は、予防接種の実施等に関する事務における特定個人情報ファイルの取扱いにあたり、特定個人情報ファイルの取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態を軽減させるために十分な措置を行い、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

福山市長

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
（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	予防接種の実施等に関する事務
②事務の内容　※	1.事務の概要 ・予防接種法に基づき、伝染のおそれがある疾病の発生及びまん延を予防するために、予防接種を行い、公衆衛生の向上及び増進に寄与することを目的とした事務。 2.事務の内容 (1)予防接種資格を証する書類の発行 ・住民基本台帳の情報を基に、予診票等、予防接種の資格を証する書類を発行・配布する。(A類疾病及びB類疾病の一部を除く。) (2)予防接種実施報告書の検査 ・医療機関から提出される予防接種実施報告書・予診票等を予防接種台帳と突合し、被接種者の資格や実施内容等を検査する。 (3)予防接種履歴の管理 ・予防接種履歴情報を、医療機関等からの報告又は他自治体との連携によって取得し、予防接種台帳に入力して管理する。 (4)予防接種券又は依頼書の発行 ・市外での予防接種を希望する市民について、申請に基づき予防接種履歴を確認して、接種券または依頼書を発行・交付する。 (5)予防接種による健康被害の救済 ・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等の給付を行う。 (6)中間サーバーへの予防接種情報の副本登録と情報提供ネットワークシステムを介した情報照会・提供 ・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(以降「番号法」という。)に基づいて福山市は、予防接種に関する事務において、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特定個人情報について情報照会を行う。また、他機関からの情報照会に対応する為に、予防接種の事務に係る特定個人情報を中間サーバーに登録する。 (7)新型コロナウイルス感染症予防接種証明書の発行 ・被接種者からの申請に基づき、予防接種(特例臨時)を受けたことを証明する書類を発行する。 ＜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。 ・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	健康管理システム
②システムの機能	(1)予防接種履歴の管理・照会機能 (2)予防接種履歴データの取り込み機能 (3)予防接種対象者抽出・出力機能 (4)帳票印刷機能 (5)地域保健・健康増進事業報告書作成機能 (6)統合宛名システム連携機能 (7)接種券付番機能
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2～5	

システム2	
①システムの名称	統合宛名システム
②システムの機能	(1)業務情報連携機能(受信のみ) ・税宛名異動(住登者・住登外者)、福祉宛名異動(住登外者のみ)、及び保険宛名異動(住登外者のみ)情報を準リアル方式(又は条件検索方式)でシステム連携基盤より連携する。 (2)団体内統合宛名番号の管理機能 ・団体内統合宛名番号の付番、基本4情報登録、及び業務宛名番号と個人番号との紐付けを行う。 (3)符号取得のためのシステム連携機能 ・団体内統合宛名番号の付番時、中間サーバへの符号取得要求、符号取得依頼の受付を行う。 (4)中間サーバ連携機能(送信) ・団体内統合宛名番号の変更・抹消・生成を行った場合、更新情報を中間サーバへ自動連携する。 ・中間サーバからの要求により、団体名統合宛名番号をキーに基本4情報を中間サーバに自動送信する。 ・各業務の副本データを中間サーバに自動送信する。 (5)職員認証・権限管理機能 ・利用者を認証し、利用者の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。 (6)システム管理機能 ・バッチの状況管理、稼動状態の通知を行う機能。
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　(中間サーバ　　)

システム3	
①システムの名称	中間サーバ
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「情報提供用個人識別符号(以下「符号」という。)」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」を紐付け、その情報を保管・管理する。 (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・情報提供受領(照会した情報の受領)を行う。 (3)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。 (4)既存システム接続機能 ・中間サーバと既存システム、統合宛名システム、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。 (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、保管・管理する。 (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、保有・管理する。 (7)データ送受信機能 ・中間サーバ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を連携する。 (8)セキュリティ管理機能 ・特定個人情報(連携対象)の暗号化及び復号や、電文への署名付与、電文及び提供許可証に付与されている署名の検証、それらに伴う鍵管理を行う。また、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)から受信した情報提供NWS配信マスター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	住民基本台帳ネットワークシステム
②システムの機能	(1)本人確認情報検索 ・本市コミュニケーションサーバー端末において入力された4情報（氏名、性別、生年月日、住所）の組合せをキーに本人確認情報の検索を行い、検索条件に該当する本人確認情報の一覧を画面上に表示する。 (2)機構への本人確認情報照会 ・全国サーバに対して住民票コード、個人番号又は4情報の組合せをキーとした本人確認情報照会要求を本市コミュニケーションサーバー端末から行い、該当する個人の本人確認情報を受領する。
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　（　）

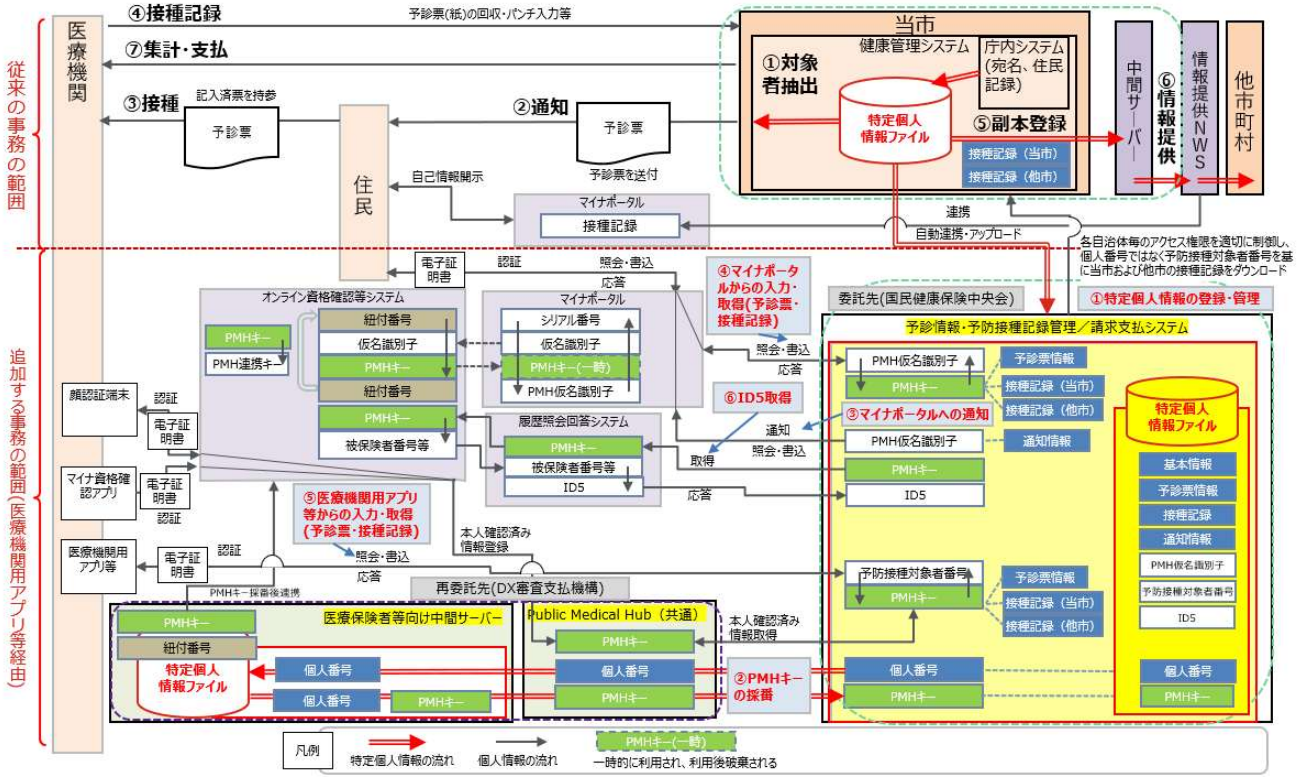
システム5	
①システムの名称	予診情報・予防接種記録管理／請求支払システム
②システムの機能	＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ ①予防接種関連データの登録機能 本市は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・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）

システム6～10	
システム6	
①システムの名称	―
②システムの機能	―
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11～15	
システム16～20	
3. 特定個人情報ファイル名	
予防接種の実施に関する情報	
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	・予防接種の対象者及び接種履歴を正確に把握・管理し、予防接種誤りを防ぐため。 ・予防接種による健康被害が発生した場合、速やかに救済措置を図るため。 ・新型コロナウイルス感染症予防接種証明書（特例臨時）を発行するため。
②実現が期待されるメリット	・個人番号を利用して他自治体等と情報連携することにより、転入出者に係る予防接種履歴を把握し、予防接種の資格等を管理する事ができる。 ・予防接種履歴を把握することで、予防接種の時期・年齢・回数・間隔の誤りを防ぐことができる。 ・予防接種による健康被害が発生した場合、速やかに救済措置を図る事ができる。 ・新型コロナウイルス感染症予防接種証明書（特例臨時）を発行することができる。
5. 個人番号の利用　※	
法令上の根拠	・行政手続における特定の個人を識別するための番号の利用等に関する法律（以降「番号法」という。）第9条第1項　別表の第14の項 ・番号法第19条第6、8、16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
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 ・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25、27、28、29の項 （情報提供） ・番号法第19条第8号 ・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25、26、153、154の項
7. 評価実施機関における担当部署	
①部署	福山市保健福祉局保健部保健予防課
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）

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の登録を行う。（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	
予防接種の実施に関する情報	
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　※	福山市に住民登録がある、又はあった、予防接種法等関連法令に基づく予防接種の対象者。
その必要性	予防接種の対象者及び接種履歴の情報を適正に管理・保管するため。
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 [○] 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	(1)識別情報 ・業務用宛名番号及び団体内統合宛名番号と個人番号の紐づけ管理のために必要である。 (2)連絡先等情報 ・本人特定及び予防接種資格確認のほか、再転入者及び住登外（福山市に住所を保有しない者）者の名寄せ（同一人判定）のために必要である。 (3)業務関係情報 ・予防接種情報は、予防接種の対象者及び接種履歴の情報を適切に管理するために必要である。 ＜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＞ (1)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。 (2)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	2016/01/01
⑥事務担当部署	福山市保健福祉局保健部保健予防課

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　（ 庁内連携により、宛名情報等を入手 ） [　] 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　（ 他自治体から予防接種履歴を入手 ） [○] 民間事業者　（ 医療機関 ） [○] その他　（ 住民基本台帳ネットワークシステム、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　（ 住民基本台帳ネットワークシステム、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	・医療機関等や被接種者から提出を受けた紙媒体の接種記録（予診票）を、月1回程度データ化（パンチ）し、電子記録媒体を用いて健康管理システムに取り込む。 ・各業務システムの宛名情報を、庁内連携によって準リアル方式で取得する。 ・情報提供ネットワークシステムを介して、転入者等に係る予防接種履歴を他自治体から随時取得する。 〈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〉 ・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。 ・国が予診情報・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	・予防接種記録は、予防接種法第9条の3及び予防接種法施行規則第3条の規定により、記録・保管する必要がある。技術面・セキュリティの面から紙媒体としており、また回収の負担から月1回程度のデータ化及び取り込みとしている。 ・宛名情報は接種資格の確認に必須なため、迅速・確実な庁内連携で準リアル方式で取得する。 ・転入者に係る予防接種履歴も資格確認に必須なため、確実かつ迅速な情報提供ネットワークシステムを介して随時取得している。 〈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〉 （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		・予防接種記録を医療機関又は本人から入手する場合は、本人等が記入する予診票にも、市へ接種記録が提出される旨明記されており、署名も得ている。 ・宛名情報は、住民基本台帳法に基づき、取得している。 〈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 ※		予防接種対象者の抽出、予防接種資格の確認、予防接種履歴管理、予防接種による健康被害の救済措置、予防接種に係る証明書の発行
	変更の妥当性	－
⑦使用の主体	使用部署 ※	福山市保健福祉局保健部保健予防課
	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 ※		(1)予防接種履歴の連携 ・転入出者について、情報提供ネットワークシステムを通じて、接種履歴を連携する。 (2)予防接種対象者の抽出 ・生年月日・予防接種履歴から接種対象者を抽出し、予診票の印刷・交付を行う。 (3)健康被害の救済措置 ・予防接種による健康被害が発生した場合、接種状況等を把握し、給付の決定等を行う。 (4)予防接種記録の検査・管理 ・医療機関等から出された予防接種記録をシステムに入力し、資格確認等の検査及び管理を行う。 (5)予防接種に係る証明書の発行 接種記録や本人から提示されたパスポート情報を元に証明書を発行する。 〈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 ※	(1)住民票関係情報と予防接種情報を突合し、年齢・予防接種履歴から接種対象者を抽出する。 (2)医療機関から提出される予防接種記録を住民票関係情報・予防接種履歴と突合し、接種資格等を確認する。 (3)健康被害を受けた者の申請書と予防接種履歴を突合し、接種状況の確認等を行う。
	情報の統計分析 ※	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 ※	・予防接種の実施の決定 ・予防接種健康被害発生時の給付の決定（国が行う）
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		健康管理システム運用保守業務
①委託内容		健康管理システム運用管理、障がい対応及び軽微な仕様変更を行うシステム運用維持管理
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」と同じ。
	その妥当性	・健康管理システムの保守業務、運用支援並びに制度改正に伴う改修作業等は高度に専門的な知識・技術を必要とするため、専門業者への委託が必要である。
③委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[○] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑤委託先名の確認方法		福山市情報公開条例第10条の規定に基づく開示請求を行うことで確認ができる。
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　※	「2.③対象となる本人の範囲」と同じ。
	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、広島県国民健康保険団体連合会（以下、広島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		広島県国保連合会
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 （ 2 ）件 [ ] 移転を行っている （ ）件 [ ] 行っていない
提供先1	市町村長
①法令上の根拠	・番号法第19条第8号 ・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25、153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	福山市に住民登録があった、予防接種法等関連法令に基づく予防接種の対象者。
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	・照会を受けた都度

提供先2～5	
提供先2	都道府県知事
①法令上の根拠	・番号法第19条第8号 ・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26、153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	福山市に住民登録があった、予防接種法等関連法令に基づく予防接種の対象者。
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	・照会を受けた都度
提供先3	厚生労働大臣
①法令上の根拠	・番号法第19条第8号 ・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（平成二十四年法律第三十一号）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	福山市に住民登録があった、予防接種事業の対象者
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	・照会を受けた都度

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 ※		＜本市における措置＞ ・鍵等により入室が制限されている場所（サーバ室）に設置したサーバ内に保管する。 ・サーバ室への入室にあたっては、事前に名前、用務等を確認の上、許可した者以外は入らないよう入室の管理を実施し、入退室を管理簿及びICカードによる入退室の管理を実施している。 ・サーバへのアクセスは、個人認証による制限管理を実施している。 ・なお、紙媒体には個人番号が記載されていない。施錠可能な場所で保管している。 ＜中間サーバにおける措置＞ ・中間サーバはデータセンターに設置されており、データセンターへの入館及びサーバ室への入室を厳重に管理されている。 ・特定個人情報は、サーバ室に設置された中間サーバ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	[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	・予防接種法第9条の3、予防接種法施行規則第4条より電磁的記録として当該定期の予防接種等を行ったときから当該定期の予防接種等を受けた者が死亡した日の翌日から五年を経過する日までの間保存しなければならないとされている。

③消去方法	＜本市における措置＞ ・保管期間を満了したデータはサーバ上から削除している。ディスク交換やハード更改等の際は、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又は専用ソフト等を利用して完全に消去する。 ＜中間サーバにおける措置＞ ・特定個人情報の消去は当市からの操作によって実施されるため、中間サーバの保守・運用を行う事業者が特定個人情報を消去することはない。 ・ディスク交換やハード更改等の際は、中間サーバの保守・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又は専用ソフト等を利用して完全に消去されている。 ＜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。 〈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

1 住民票関係情報（共通）
(1)世帯情報
1.世帯番号、2.処理区分、3.世帯主宛名番号、4.世帯主カナ氏名、5.管内コード、6.小学校区、7.中学校区
(2)個人情報
1.宛名番号、2.世帯番号、3.処理区分、4.カナ氏名、5.漢字氏名、6.通称カナ氏名、7.通称氏名、8.生年月日、9.性別、10.続柄1、11.続柄2、12.続柄3、13.続柄4、14.個人住所コード、15.個人郵便番号、16.個人住所日本語、17.個人方書日本語、18.個人地番 本番、19.個人地番 枝番、20.個人地番 末番、21.異動事由、22.異動日、23.異動届出日、24.住民になった 異動日、25.住民になった 届出日、26.住民でなくなった 異動日、27.住民でなくなった 届出日、28.住定日、29.住定日 届出日、30.住民区分、31.外国人判定、32.国籍、33.転入前住所、34.通称名、35.送 フラグ、36.本名・通称名区分、37.第30条45規定区分、38.在留資格、39.在留期間等(yymmdd)、40.在留期間等終了日、41.在留カード等番号
(3)個人情報履歴
1.宛名番号、2.世帯番号、3.処理区分、4.カナ氏名、5.漢字氏名、6.通称カナ氏名、7.通称氏名、8.生年月日、9.性別、10.続柄1、11.続柄2、12.続柄3、13.続柄4、14.異動事由、15.異動日、16.異動届出日、17.住民になった 異動日、18.住民になった 届出日、19.住民でなくなった 異動日、20.住民でなくなった 届出日、21.住定日、22.住定日 届出日、23.住民区分、24.外国人判定、25.国籍、26.転入前住所、27.送 宛先人氏名、28.送 フラグ、29.第30条45規定区分、30.在留資格、31.在留期間等（yymmdd）、32.在留期間等終了日、33.在留カード等番号、34.個人住所コード、35.個人郵便番号、36.個人住所日本語、37.個人方書日本語、38.個人地番 本番、39.個人地番 枝番、40.個人地番 末番

2 予防接種情報
(1)予防接種共通
1.宛名番号、2.更新者、3.更新日、4.更新時間、5.体質的理由1、6.体質的理由2、7.新型コロナ接種券番号
(2)予防接種各種データ
1.宛名番号、2.性別、3.接種コード、4.接種回数、5.接種・予診日、6.年度、7.接種判定、8.混合接種 何種、9.肺炎球菌種類、10.接種内容、11.請求日（月）、12.実施医療機関、13.Lot.No、14.実施課、15.予診フラグ、16.接種日年齢、17.医師の判断、18.対象外判定、19.特記事項、20.接種日年齢、21.年度末年齢、22.基準日年齢、23.更新者、24.更新日
(3)成人用肺炎球菌
1.西暦年度、2.宛名番号、3.接種・予診日、4.接種日年齢、5.年度末年齢、6.基準日年齢、7.更新者、8.更新日、9.更新時間、10.性別、11.接種日年齢、12.年度末年齢、13.基準日年齢、14.受診時国保区分、15.請求日(月)、16.実施医療機関、17.接種番号、18.接種会場、19.問診医、20.接種医、21.接種判定、22.Lot.No、23.接種量、24.実費徴収区分、25.接種済証交付有無、26.65歳未満接種理由、27.未接種理由、28.予診フラグ、29.接種区分
(4)風しん第5期
1.西暦年度、2.宛名番号、3.実施日、4.更新者、5.更新日、6.更新時間、7.性別、8.クーポン、9.実施区分、10.接種(実施)判定、11.接種日年齢、12.年度末年齢、13.基準日年齢、14.請求日(月)、15.実施医療機関、16.実施医療機関（手入力）、17.抗体検査方法、18.抗体価、19.抗体価範囲、20.抗体価単位、21.抗体検査判定結果、22.抗体検査番号、23.接種番号、24.Lot.No、25.接種量
(5)新型コロナウイルス感染症対策に係る予防接種に関する記録項目
1.個人番号、2.宛名番号、3.自治体コード、4.接種券番号、5.属性情報（氏名、生年月日、性別）、6.接種状況（実施/未実施）、7.接種回（1回目/2回目）、8.接種日、9.ワクチンメーカー、10.ロット番号
(6)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情報
1.業務宛名番号、2.接種日（1回目）、3.接種日（2回目）
＜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
(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	
予防接種の実施に関する情報	
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	・予防接種情報は、医療機関において本人確認を行う事で、対象者以外の情報入手を防止する。 ・各業務システムより、庁内連携システム経由で当日の宛名異動情報を連携し、当ファイルに格納する。この宛名情報を基に予防接種情報を登録するため、対象者以外の情報は入手できない。 ＜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	・保健部保健予防課特定個人情報取扱規定に基づき、職員に情報セキュリティ教育を実施する際、対象者情報であっても業務に不必要な情報へのアクセスは不正アクセスに該当し、番号法及び個人情報の保護に関する法律における罰則規定が適用されうること、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、必要以外の情報入手を防止している。 ・届出・申請用紙等について、あらかじめ定められた様式で提出されることから、必要以外の情報が記載できない。 ＜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。 ・「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	－
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	・番号法及び個人情報の保護に関する法律における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・予防接種に関する事務を取り扱うにあたり、根拠法令である予防接種法及び同施行令等に規定された内容を遵守することで、不適切な方法による情報の入手を防止する。 ・保健部保健予防課特定個人情報取扱規定による情報セキュリティ教育実施の際、根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・入力する情報は法令で定められ、必要な手続きを行ったものに限定する。 ・システムの操作に当たり、情報セキュリティ実施手順に則って、操作履歴の採取・保管及び定期的な確認を行うことで、必要以外の情報の入手を抑止する。 ・本人から情報を取得する場合は、予防接種に係る事務に用いる旨を説明した上で取得する。 ＜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＞ ・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。 ・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	・予防接種情報は、実施をする医療機関において本人確認措置をとったうえで提出される。 ・システムが住民票情報を基に予防接種情報・個人番号を紐づけるため、本人確認措置は不要。 ・他自治体等、本人以外から個人番号の提供を受ける際は、情報提供元が本人に対して個人番号及び4情報が正しいことを確認する。 ＜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＞ ・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。 ・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	・システムが住民票情報を基に予防接種情報・個人番号を紐づけるため、個人番号の真正性は確保されている。 ＜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／請求支払システムが提供した個人番号は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。 ・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	・情報の入力、削除、訂正を行う場合には処理者と点検者を別にし、二重チェックを行うことで正確性を担保する。 ・正確性に疑義が生じた場合は、予防接種法及び同施行令等に基づき適宜調査を行い、必要に応 じてデータを修正することで正確性を担保する。 ＜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＞ 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	・申請書等には個人番号を記入しない。事務が完了し次第、書類は施錠可能な場所へ格納する。 ・紙媒体の予防接種情報のデータ化においては、委託業者と個人情報保護契約を締結している。 ・端末は外部記録媒体の使用が制限されており、基本的には外部ネットワークにも非接続である。 ・特定個人情報を取り扱うソフトウェアの操作に必要なID、パスワードは各所属長から情報システム担当課長への申請により付与するため、操作権限のない者による不正な操作を防止できる。 ＜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		・統合宛名システムは、利用事務・目的ごとにアクセスを厳密に制御する仕組みとなっている。 ・必要な情報以外が紐づけされないよう、システム的に制御が行われている。 ・利用者ごとのユーザID・パスワードによる認証を行うことで、不要なアクセスを防いでいる。
事務で使用するその他のシステムにおける措置の内容		・各システムの連携機能は、限られた情報のみを相手としており、不要な情報とは紐づけできない。 ・健康管理システムも個人番号にアクセスできる権限保有者を限り、不必要な紐づけを防いでいる。 ＜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		－
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	・ユーザーIDによる識別とパスワードによる認証を実施しており、認証後は利用機能及び利用可能情報の権限管理により不正利用ができない対策を実施している。ユーザーIDは職員の人事異動を反映しており、当該事務の最新の担当者のみ利用可能としている。 ・利用する端末について管理しており、不要な端末からの利用ができない制限を実施している。 ＜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	・保健予防課が年度ごとで担当者の権限を申請し、ICT推進課がIDとパスワードを発行している。 ＜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	・保健予防課が作成したアクセス権限と事務の対応表を、ICT推進課が確認してID・パスワードを発行している。 ＜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	・各システムにおいて、システムの操作ログが保存されている。 ＜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		・予防接種事務を取り扱う職員に対してセキュリティ研修を行い、個人情報保護の重要性について教育するとともに、業務外での情報収集の禁止等の指導を徹底する。 ・操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め事務外での使用を防止する。 ＜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、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		・健康管理システムの端末は外部記録媒体が使用制限されており、基本的には外部ネットワークにも接続されていない。 ・データの抽出・複製が可能な権限を有する者を限定している。 ・予防接種事務を取り扱う職員に対してセキュリティ研修を行い、個人情報保護の重要性について教育するとともに、特定個人情報ファイルの不正な複製を厳に禁じる旨の指導を徹底する。 〈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〉 ・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
-

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	相手方の個人情報保護管理体制及びプライバシーマークの有無を確認し、委託先を決めている。 〈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、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広島県国保連合会に委託し、広島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	・アクセスできる者を業務に直接従事する必要がある従事者に限定している。 ・委託契約書において個人情報保護規約を設けている。 ・健康管理システムのユーザ（ID／パスワード）による制御を行っている。 〈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〉 ・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	アクセスログを記録し、システム管理者により定期的に不正アクセス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〉 ・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	・業務の目的を超える個人情報の利用及び第三者への提供を契約書で禁止している。 ・必要があると認める時は調査を行い、報告を求める。 〈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〉 ・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。	
	・番号法等関連法規を遵守する旨の契約をしている。 ・委託先への提供は個人情報であり、特定個人情報へのアクセスは保守においてのみである。 作業時のみVPN技術を用いた専用線を接続し、外部記録媒体の使用が制限されている限定され	

	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	た端末で作業を行う事となっている。 ・必要に応じて委託先に対し個人情報の取扱状況の報告を求め、委託元が調査を行う。 〈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〉 ・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	・外部記録媒体の廃棄時には、あらかじめ福山市の承諾を得たうえで、第三者利用を防ぐ措置をとるよう定めている。 ・必要があると認める時は調査を行い、報告を求める。 〈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〉 ・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	・特定個人情報の収集制限 ・目的外利用、第三者提供の禁止及び持ち出し、複製の制限 ・情報漏えいを防ぐための保管管理に責任を負うとともに、体制を届け出る事 ・業務従事者への周知、教育、監督の義務 ・契約終了時の情報の返還・消去 ・必要に応じて福山市から報告を求め、調査を行うことができる事。 ・再委託の制限 ・委託先の責任者、委託内容、作業者、作業番所の特定 ・業務上知りえた情報の守秘義務 〈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〉 広島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 ・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　　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、点検結果について広島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	＜中間サーバ・ソフトウェアにおける措置＞ ・中間サーバには、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が備わっており、目的外提供やセキュリティリスクに対応している。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止できる。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 安全が保たれない方法によって入手が行われるリスク	
リスクに対する措置の内容	＜中間サーバ・ソフトウェアにおける措置＞ ・中間サーバは、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、照会対象者に係る特定個人情報を安全に入手することを担保する。
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： 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・ソフトウェアにおける措置＞ ・中間サーバは、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、照会対象者に係る特定個人情報を安全に入手することを担保する。
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・ソフトウェアにおける措置＞ ・中間サーバは、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。 ・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。 ・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している。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や不適切なオンライン連携を抑止する仕組みになっている。
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・ソフトウェアにおける措置＞ ・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が実施されている。 ・情報提供を行う際には、情報提供ネットワークシステムから情報提供許可証と情報照会者へたどり着くための経路情報を受信し、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。 ・特に慎重な対応が求められる情報については、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、紙媒体で提供を行うことで、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。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他にログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や不適切なオンライン連携を抑止する仕組みになっている。
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・ソフトウェアにおける措置＞ ・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を管理する機能）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、情報照会者から受信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。 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ＜中間サーバ･プラットフォームにおける措置＞ ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ・中間サーバと団体についてはVPN等の技術を利用して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。 ・中間サーバ・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。
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・ソフトウェアにおける措置＞ ・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信した上で、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。 ・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。 ・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。
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	
－	

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	＜本市における措置＞ ・サーバ設置及び記録媒体保管場所へは管理簿及びICカードで入退室管理を実施する。 ・端末、届書等及びシステムより出力された帳票は、個人番号を含まないが、施錠管理を実施する。 ・出力帳票を廃棄する際は、シュレッダーによる粉砕処理を行う。 ＜中間サーバ･プラットフォームにおける措置＞ ・中間サーバ･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。 ＜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	＜本市における措置＞ ・サーバ及び端末について、ウイルス対策ソフトの定期的パターン更新を実施する。 ・不正アクセス防止策として、ファイアウォール、IDS／IPS（侵入検知）を導入し、ネットワーク制限や監視を実施する。 ＜中間サーバ・プラットフォームにおける措置＞ ・中間サーバ・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・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。 ＜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ついて【第2．1版】」（令和6年7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	
	再発防止策の内容	
⑩死者の個人番号		[　保管している　] <選択肢> 1）保管している　2）保管していない
	具体的な保管方法	・生存者の個人番号と死者の個人番号を区別しないため，生存者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	・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。 〈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	・特定個人情報は電子データのみであり、保管年限を過ぎたデータは自動的に削除される。 ・ディスク交換やハード更改等の際は、サーバ・プラットフォームの保守・運用を行う事業者において、保存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。 ・中間サーバ接続端末及び統合宛名システム用端末の更新の際は、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。 〈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		

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	＜本市における措置＞ ・評価書の記載内容どおりの運用がなされているか、年に1回以上部署内にてチェックする。チェックの結果、不備が生じていることが明らかになった際は、速やかに問題究明にあたり是正する。 ・福山市情報セキュリティ実施手順に基づく各課におけるセキュリティ点検を年に1度実施する。 ＜中間サーバ・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバ・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。 ＜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	＜本市における措置＞ ・福山市情報セキュリティ実施手順に基づき定期的に行う。監査結果を踏まえて安全管理措置（体制、規定を含む。）を改善する。 ＜中間サーバ・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバ・プラットフォームについて、定期的に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	＜本市における措置＞ ・職員（嘱託職員、臨時職員を含む。）に対して、初任時及び一定期間ごとに、個人情報の管理方法等について必要な知識の習得に資するための研修を実施している。 ・機構が実施するe-ラーニングを担当職員が受講することにより、セキュリティ意識の醸成及び自己研鑽につなげている。 ＜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、適切な指導を行う。	

3. その他のリスク対策

＜中間サーバ・プラットフォームにおける措置＞
・中間サーバ・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。
＜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	福山市保健福祉局保健部保健予防課 720－8512　広島県福山市三吉町南二丁目11番22号 084－928－1127
②請求方法	指定様式による書面の提出により開示・訂正・使用停止請求を受け付ける。
特記事項	本市ホームページに請求先、請求方法等を掲載している。
③手数料等	[　　無料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　　）
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	予防接種法に定める定期接種、新型コロナウイルス感染症対策に係る予防接種業務
公表場所	・福山市市政情報室（本庁舎3階） ・福山市ホームページ
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	福山市保健福祉局保健部保健予防課 720－8512　広島県福山市三吉町南二丁目11番22号 084－928－1127
②対応方法	・問合せの受付時に受付票を起票し、対応について記録を残す。 ・情報漏えい等の重大な事案に関する問合せについて、関係先等に事実確認を行うための標準的な処理期間を設ける。

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	「福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を実施した。実施に際しては、パブリックコメントを実施する旨を市の広報誌へ掲載するとともに、市ホームページ及び予防接種事務関連部署にて全文を閲覧できるようにした。
②実施日・期間	2026年（令和8年）10月1日～11月2日
③期間を短縮する特段の理由	短縮なし
④主な意見の内容	なし
⑤評価書への反映	なし
3. 第三者点検	
①実施日	
②方法	
③結果	
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和4年3月4日	個人情報保護評価書の種類	重点項目評価書	全項目評価書	事後	この度，当事務のシステムを新型コロナウイルス感染症対策に係るワクチン接種で使用する事となり，国の求めに応じて個人番号を保持する改修を行う事になった。国のワクチン接種記録システムの詳細は直前まで不明であり，事前に保護評価を行える状況になかった。また，当システム改修により迅速かつ正確な予防接種実施が求められているため，特定個人情報保護評価に関する規則第9条第2項の規定により，緊急時の事後評価の対象となる。
令和5年8月10日	Ⅱ-3-④入手に係る妥当性	・予防接種記録は，予防接種法施行令第6条の2及び予防接種施行規則第2条の7の規定により，記録・保管する必要がある。技術面・セキュリティの面から紙媒体としており，また回収の負担から月1回程度のデータ化及び取り込みとしている。 ・宛名情報は接種資格の確認に必須なため，迅速・確実な庁内連携で準リアル方式で取得する。 ・転入者に係る予防接種履歴も資格確認に必須なため，確実かつ迅速な情報提供ネットワークシステムを介して随時取得している。	・予防接種記録は，予防接種法第9条の3及び予防接種法施行規則第3条の規定により，記録・保管する必要がある。技術面・セキュリティの面から紙媒体としており，また回収の負担から月1回程度のデータ化及び取り込みとしている。 ・宛名情報は接種資格の確認に必須なため，迅速・確実な庁内連携で準リアル方式で取得する。 ・転入者に係る予防接種履歴も資格確認に必須なため，確実かつ迅速な情報提供ネットワークシステムを介して随時取得している。	事後	事前の提出・公表が義務付けられない
令和5年8月10日	Ⅱ-3-⑤本人への明示	・予防接種記録を医療機関又は本人から入手する場合は，本人等が記入する予診票にも，市へ接種記録が提出される旨明記されており，署名も得ている（予防接種法施行令第6条の2）。 ・宛名情報は福山市個人情報保護条例第8条第3項第2号の規定に基づき，取得している。	・予防接種記録を医療機関又は本人から入手する場合は，本人等が記入する予診票にも，市へ接種記録が提出される旨明記されており，署名も得ている。 ・宛名情報は，住民基本台帳法に基づき，取得している。	事後	事前の提出・公表が義務付けられない
令和5年8月10日	Ⅱ-6-②保管期間	・予防接種法施行令第6条の2及び特定個人情報に係る副本登録・更新に係る基本ルールにおいて，5年間のデータ保管が義務付けられている。	・予防接種法第9条の3，予防接種法施行規則第3条及び特定個人情報に係る副本登録・更新に係る基本ルールにおいて，5年間のデータ保管が義務付けられている。	事後	事前の提出・公表が義務付けられない
令和5年8月10日	「Ⅲリスク対策（プロセス）」の「リスクに対する措置の内容」	・保健部保健予防課特定個人情報取扱規定に基づき，職員に情報セキュリティ教育を実施する際，対象者情報であっても業務に不必要な情報へのアクセスは不正アクセスに該当し，番号法及び福山市個人情報保護条例における罰則規定が適用されうること，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，必要以外の情報入手を防止している。 ・届出・申請用紙等について，あらかじめ定められた様式で提出されることから，必要以外の情報が記載できない。	・保健部保健予防課特定個人情報取扱規定に基づき，職員に情報セキュリティ教育を実施する際，対象者情報であっても業務に不必要な情報へのアクセスは不正アクセスに該当し，番号法及び個人情報の保護に関する法律における罰則規定が適用されうること，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，必要以外の情報入手を防止している。 ・届出・申請用紙等について，あらかじめ定められた様式で提出されることから，必要以外の情報が記載できない。	事後	事前の提出・公表が義務付けられない
令和5年8月10日	「Ⅲリスク対策（プロセス）」の「リスクに対する措置の内容」	・番号法及び福山市個人情報保護条例における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・予防接種に関する事務を取り扱うにあたり，根拠法令である予防接種法及び同施行令等に規定された内容を遵守することで，不適切な方法による情報の入手を防止する。 ・保健部保健予防課特定個人情報取扱規定による情報セキュリティ教育実施の際，根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・入力する情報は法令で定められ，必要な手続きを行ったものに限定する。 ・システムの操作に当たり，情報セキュリティ実施手順に則って，操作履歴の採取・保管及び定期的な確認を行うことで，必要以外の情報の入手を抑止する。 ・本人から情報を取得する場合は，予防接種に係る事務に用いる旨を説明した上で取得する。	・番号法及び個人情報の保護に関する法律における罰則規定を広く職員に周知することで不適切な方法による情報入手を防止する。 ・予防接種に関する事務を取り扱うにあたり，根拠法令である予防接種法及び同施行令等に規定された内容を遵守することで，不適切な方法による情報の入手を防止する。 ・保健部保健予防課特定個人情報取扱規定による情報セキュリティ教育実施の際，根拠法令等の規定に基づく正当な資料の入手を指導徹底する。 ・入力する情報は法令で定められ，必要な手続きを行ったものに限定する。 ・システムの操作に当たり，情報セキュリティ実施手順に則って，操作履歴の採取・保管及び定期的な確認を行うことで，必要以外の情報の入手を抑止する。 ・本人から情報を取得する場合は，予防接種に係る事務に用いる旨を説明した上で取得する。	事後	事前の提出・公表が義務付けられない
令和6年12月20日	Ⅰ 基本情報 -5．個人番号の利用	・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（以降「番号法」 という。）第9条第1項　別表第1の第10の項 ・番号法第19条第6号 ・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別表第一の主務省 令で定める事務及び情報を定める命令第10条	・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（以降「番号法」という。）第9条第1項　別表の第14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	事後	事前の提出・公表が義務付けられない

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
令和6年12月20日	Ⅰ 基本情報 -6．情報提供ネットワークシステムによる情報連携	・番号法第19条第8号及び別表第二 （情報提供）…別表第二第16の2及び第16の3の項 （情報照会）…別表第二第16の2，第17，第18及び第19の項 ・行政手続における特定の個人を識別するための番号の利用等に関する法律別表第二の主務省 令で定める事務及び情報を定める命令 （情報提供）…第12条の2第2項，第12条の2の2 （情報照会）…第12条の2，第12条の3，第13条，第13条の2	（情報照会） ・番号法第19条第8号 ・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25、27、28、29の項 （情報提供） ・番号法第19条第8号 ・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25、26の項	事後	事前の提出・公表が義務付けられない
令和6年12月20日	Ⅱ ファイルの概要 -5．特定個人情報の提供・移転（委託に伴うものを除く。） -提供先1-①法令上の根拠	・番号法第19条第8号及び別表第2第16の2の項	・番号法第19条第8号 ・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条表25の項	事後	事前の提出・公表が義務付けられない
令和6年12月20日	Ⅱ ファイルの概要 -5．特定個人情報の提供・移転（委託に伴うものを除く。） -提供先2-①法令上の根拠	・番号法第19条第8号及び別表第2第16の3の項	・番号法第19条第8号 ・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条表26の項	事後	事前の提出・公表が義務付けられない
令和6年12月20日	Ⅱ ファイルの概要 -6．特定個人情報の保管・消去 -①保管場所	（右記を追加）	＜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。	事前	
令和6年12月20日	Ⅱ ファイルの概要 -6．特定個人情報の保管・消去 -③消去方法	（右記を追加）	＜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。	事前	
令和6年12月20日	Ⅲ リスク対策（プロセス） -7．特定個人情報の保管・消去 -⑤物理的対策	（右記を追加）	＜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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅲ リスク対策（プロセス） −7．特定個人情報の保管・消去 −⑥技術的対策	（右記を追加）	＜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。	事前	
令和6年12月20日	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	（右記を追加）	＜Public Medical Hub（PMH）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、Public Medical Hub（PMH）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、マイナポータル等を介して予診票情報の入力、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、マイナンバーカードを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のシステムで用いることにより、医療機関において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。 ・自治体は、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。	事前	
令和6年12月20日	Ⅰ 基本情報 −2．特定個人情報ファイルを	（右記を追加）	Public Medical Hub （PMH）	事前	
令和6年12月20日	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 ②システムの機能	（右記を追加）	＜Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務＞ ①雛形の登録 　予診票項目、通知文言等のひな形をPublic Medical Hub（PMH）へ登録する。 ②情報登録機能及びPMH−ID採番依頼機能等 　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Public Medical Hub（PMH）に登録し、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−IDを自動採番する。すでにPMH−ID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−ID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 　マイナポータルからのPublic Medical Hub（PMH）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−IDと紐付けてPublic Medical Hub（PMH）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。Public Medical Hub（PMH）は、PMH仮名識別子からPMH−IDを特定し、PMH−ID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、Public Medical Hub（PMH）はPMH仮名識別子からPMH−IDを特定し、PMH−ID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） ・識別子の格納機能 　医療機関用アプリはマイナンバーカードの電子証明書のシリアル番号を用いてマイナ	事前	
令和6年12月20日	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 ③他のシステムとの接続	（右記を追加）	その他 （健康管理システム、マイナポータル、医療保険者等向け中間サーバー）	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅱ ファイルの概要 -2. 基本情報 -④記録される項目 -主な記録項目	（右記を追加）	その他 <Public Medical Hub（PMH）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	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	<Public Medical Hub（PMH）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-ID、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 予防接種番号…PMH内で予防接種の種類を区別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、PMHが、外部と情報連携するために必要となる。	事前	
令和6年12月20日	（別添2）ファイル記録項目	（右記を追加）	<Public Medical Hub（PMH）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-ID ・PMH仮名識別子 ・基本5情報（カナ・氏名・住所・生年月日・性別） ・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） (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	事前	
令和6年12月20日	Ⅱ ファイルの概要 -3. 特定個人情報の入手・使用 -①入手元	（右記を追加）	支払基金	事前	
令和6年12月20日	Ⅱ ファイルの概要 -3. 特定個人情報の入手・使用 -②入手方法	（右記を追加）	その他 （医療保険者等向け中間サーバー、医療機関用アプリ、マイナポータル）	事前	
令和6年12月20日	Ⅱ ファイルの概要 -3. 特定個人情報の入手・使用 -③入手の時期・頻度	（右記を追加）	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> ・PMH-IDの採番処理依頼時に都度、医療保険者等向け中間サーバーから特定個人情報を入手する。 ・本市区町村がPMHに登録した予診票のひな形に対して、住民がマイナポータル等を介して接種前に予診票情報を入力することにより個人情報を入手し、事務・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、従来の紙の予診票に代えて、医療機関のタブレットに搭載された医療機関用アプリを用いて、住民がマイナンバーカードで認証して同意することにより、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、事務・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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅱ ファイルの概要 -3. 特定個人情報の入手・使用 -④入手に係る妥当性	（右記を追加）	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> （PMH-ID採番処理依頼時に入手される特定個人情報） ・外部との情報連携のため、PMH-IDの採番処理依頼時に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、事務・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） 入手にあたって、既存事務と同様に予診票の事前入力する事項については、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については、予防接種を実施する医療機関から入手する必要がある。 ・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入力され、入力した情報は、接種を受託する医療機関で確認され、接種の可否を判断する。 ・医療機関では、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・接種記録のオンライン化により住民及び医療機関での利便性の向上及び、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して同意することにより、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。	事前	
令和6年12月20日	Ⅱ ファイルの概要 -3. 特定個人情報の入手・使用 -⑤本人への明示	（右記を追加）	<Public Medical Hub（PMH）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、同意することにより入手する。	事前	
令和6年12月20日	Ⅱ ファイルの概要 -3. 特定個人情報の入手・使用 -⑧使用方法	（右記を追加）	<Public Medical Hub（PMH）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、Public Medical Hub（PMH）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。 ・登録後、Public Medical Hub（PMH）は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub（PMH）が連動するためのPMH-ID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-IDを採番して個人番号と共にPublic Medical Hub（PMH）に応答する。 ・PMH-ID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Public Medical Hub（PMH）で共有されることでPublic Medical Hub（PMH）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（マイナポータル経由）からPublic Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅱ ファイルの概要 -3. 特定個人情報の入手・使用 -⑧使用方法 情報の統計分析	（右記を追加）	<Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	Public Medical Hub（PMH）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	事前	
令和6年12月20日	Ⅱ 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委託事項	（右記を追加）	Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	特定個人情報ファイルの一部	事前	
令和6年12月20日	Ⅱ 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 対象となる本人の数	（右記を追加）	3　10万人以上100万人未満	事前	
令和6年12月20日	Ⅱ 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 対象となる本人の範囲	（右記を追加）	「2.③対象となる本人の範囲」と同じ。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅱ 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 その妥当性	（右記を追加）	Public Medical Hub（PMH）は国（デジタル庁）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-ID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、PMHに格納された特定個人情報は、自動処理により再委託先に情報連携されるため、国（デジタル庁）は特定個人情報にアクセスすることはない。	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	10人以上50人未満	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	その他 （LGWAN又は閉域網回線を用いた提供）	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	下記、「⑥委託先名」の項の記載より確認できる。	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	国（デジタル庁）	事前	
令和6年12月20日	Ⅱ 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 ⑦	（右記を追加）	再委託する	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	書面又は電磁的方法による承諾	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> ・Public Medical Hub（PMH）の運用保守 ・PMH-IDの採番及びPMH-ID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-IDを介して行うため、特定個人情報を取り扱わない。	事前	
令和6年12月20日	Ⅱ 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	（右記を追加）	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> Public Medical Hub（PMH）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または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（デジタル庁）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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅱ ファイルの概要 −6．特定個人情報ファイルの保管・消去 ①保管場所	（右記を追加）	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> Public Medical Hub（PMH）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または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（デジタル庁）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。	事前	
令和6年12月20日	Ⅱ ファイルの概要 −6．特定個人情報ファイルの保管・消去 ③消去方法	（右記を追加）	<Public Medical Hub（PMH）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、Public Medical Hub（PMH）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、古いものから順に自動削除される。	事前	
令和6年12月20日	Ⅲ リスク対策（プロセス） −2．特定個人情報の入手 −リスク1：目的外の入手が行われるリスク	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・PMH−IDの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで対象者以外の情報の入手を防止する。（当該機能は、R6年度中に実装予定） ・医療機関の受付窓口で本人確認の後、医療機関用アプリ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、医療機関用アプリでの入力は、診察室内で更に本人確認を行うことで本人の情報のみがPublic Medical Hub（PMH）へ連携される。 ・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Public Medical Hub（PMH）に連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。	事前	
令和6年12月20日	Ⅲ リスク対策（プロセス） −2．特定個人情報の入手 −リスク1：目的外の入手が行われるリスク	（右記を追加）	＜Public Medical Hub（PMH）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（PMH）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−ID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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅲ　リスク対策（プロセス） -2．特定個人情報の入手 -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	（右記を追加）	＜Public Medical Hub（PMH）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（PMH）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-ID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。 ・Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -2．特定個人情報の入手 -リスク3：入手した個人情報が不正確であるリスク	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）が提供した個人番号を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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -2．特定個人情報の入手 -リスク3：入手した個人情報が不正確であるリスク	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）が提供した個人番号を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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -2．特定個人情報の入手 -リスク3：入手した個人情報が不正確であるリスク	（右記を追加）	＜Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -2．特定個人情報の入手 -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	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）と支払基金の医療保険者等向け中間サーバーは、暗号化された閉域網で接続される。 ・医療機関や住民からPublic Medical Hub（PMH）への連携は、直接接続ではなく、マイナポータルAPI経由の接続のみが認められ、通信内容は、情報漏洩を防止するために暗号化される。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -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	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）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。 ・Public Medical Hub（PMH）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マイナポータルAPI経由でPublic Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -3．特定個人情報の使用 -リスク2 -ユーザ認証の管理 -具体的な管理方法	（右記を追加）	＜Public Medical Hub（PMH）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、Public Medical Hub（PMH）のアクセス権限を管理する管理者を定める。 ・Public Medical Hub（PMH）のログインはユーザID・パスワードで行う。 ・Public Medical Hub（PMH）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。 ・Public Medical Hub（PMH）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Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -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 -具体的な管理方法	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）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。 ・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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅲ　リスク対策（プロセス） -3．特定個人情報の使用 -リスク2 -アクセス権限の管理 -具体的な管理方法	（右記を追加）	＜Public Medical Hub（PMH）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。 ・パスワードの有効期限を設定する。 ・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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -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 -具体的な管理方法	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -3．特定個人情報の使用 -リスク3 -リスクに対する措置の内容 -具体的な管理方法	（右記を追加）	＜Public Medical Hub（PMH）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＞ ・特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、事務外の使用を防止している。 ・委託業務については、委託先との契約により、委託業者が従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。本市区町村は、当該教育の実施について履行確認を行う。 ・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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -3．特定個人情報の使用 -リスク4 -リスクに対する措置の内容 -具体的な管理方法	（右記を追加）	<Public Medical Hub（PMH）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Public Medical Hub（PMH）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Public Medical Hub（PMH）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。 ・Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -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 -具体的な管理方法	（右記を追加）	<Public Medical Hub（PMH）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、Public Medical Hub（PMH）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国（デジタル庁）に委託することとする。 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）に基づき、委託先となる国（デジタル庁）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -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	（右記を追加）	<Public Medical Hub（PMH）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。 ・アクセス権限を付与する者を必要最小限に限定する。 ・アクセス権限を付与する範囲を必要最小限に限定する。 ・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、再委託先（PMH-ID採番や運用保守）のみに付与される。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -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 -具体的な方法	（右記を追加）	<Public Medical Hub（PMH）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> ・特定個人情報の取り扱いのログを保存し、提供を求めることができる。 ※再委託先（PMH-ID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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅲ　リスク対策（プロセス） −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	（右記を追加）	<Public Medical Hub（PMH）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（再委託も含む。）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（再委託先も含む。）から他者への提供が行われていないことを確認できる。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） −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	（右記を追加）	<Public Medical Hub（PMH）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（再委託先も含む。）から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） −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	（右記を追加）	<Public Medical Hub（PMH）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> ・委託契約終了後は保管していた全ての特定個人情報を消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、消去について、本市区町村は報告を受けることができ、それにより消去状況について確認が可能となる。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） −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	（右記を追加）	<Public Medical Hub（PMH）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> 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	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） −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	再委託していない	十分に行っている	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） −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	（右記を追加）	<Public Medical Hub（PMH）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> ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるデジタル庁が、再委託先における特定個人情報ファイルの管理状況の定期的な点検（年１回程度又は随時）を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、年１回デジタル庁から報告を受ける。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） −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	（右記を追加）	<Public Medical Hub（PMH）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。 委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅲ　リスク対策（プロセス） -7．特定個人情報の保管・消去 -⑤物理的対策 -具体的な対策の内容	（右記を追加）	<Public Medical Hub（PMH）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> Public Medical Hub（PMH）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または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を利用している。<Public Medical Hub（PMH）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> Public Medical Hub（PMH）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または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を利用している。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -7．特定個人情報の保管・消去 -⑤技術的対策 -具体的な対策の内容	（右記を追加）	<Public Medical Hub（PMH）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> Public Medical Hub（PMH）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または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。 ・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（デジタル庁）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、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Public Medical Hub（PMH）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Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -7．特定個人情報の保管・消去 -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	（右記を追加）	<Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅲ　リスク対策（プロセス） -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	（右記を追加）	<Public Medical Hub（PMH）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、古いものから順に自動削除される。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年12月20日	Ⅳ　その他のリスク対策 −1．監査 −①自己点検	（右記を追加）	＜Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅳ　その他のリスク対策 −1．監査 −②監査	（右記を追加）	＜Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅳ　その他のリスク対策 −2．従業者に対する教育・啓発	（右記を追加）	＜Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅳ　その他のリスク対策 −3．その他のリスク対策	（右記を追加）	＜Public Medical Hub（PMH）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。	事前	
令和6年12月20日	Ⅵ−1.①実施日	2021/6/23	2024/12/20	事後	事前の提出・公表が義務づけられない
令和6年12月20日	Ⅵ−2.②実施日・期間	2021年（令和3年）9月29日～2021年（令和3年）10月28日	2024年（令和6年）10月1日～31日	事後	事前の提出・公表が義務づけられない
令和6年12月20日	Ⅵ−3.①実施日	2021年（令和3年）11月19日	2024年（令和6年）11月15日	事後	事前の提出・公表が義務づけられない
令和8年3月2日	表紙 ー個人のプライバシー等の権利利益の保護の宣言 ー特記事項	評価書本編は、健康管理システムの標準準拠システム移行後の内容を踏まえて記載。 標準準拠システム移行前の内容を踏まえた評価は、別紙1に記載している。	ー	事後	事前の提出・公表が義務づけられない
令和8年3月2日	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 　庁内連携システム ②システムの機能 　庁内システムの連携を効率的に行う。 　(1)転送機能 　(2)文字コード変換 　(3)業務コード変換機能 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 [O]既存住民基本台帳システム [O]宛名システム等 [O]税務システム [O]その他（公営住宅管理システム、教育事務システム、選挙管理システム、健康管理システム、受益者負担金システム、土木使用料システム、福祉総合システム、保険系システム、戸籍システム、統合宛名システム、子ども・子育て支援システム）	ー	事後	事前の提出・公表が義務付けられない
令和8年3月2日	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6	システム5	事後	事前の提出・公表が義務付けられない
令和8年3月2日	Ⅰ 基本情報 −5．個人番号の利用	・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（以降「番号法」という。）第9条第1項　別表の第14の項	・行政手続における特定の個人を識別するための番号の利用等に関する法律（以降「番号法」という。）第9条第1項　別表の第14の項	事後	事前の提出・公表が義務付けられない
令和8年3月2日	Ⅱ ファイルの概要 −6．特定個人情報の保管・消去 −③消去方法 −＜ガバメントクラウドにおける措置＞	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。	ー	事後	事前の提出・公表が義務づけられない
令和8年3月2日	Ⅳ　その他のリスク対策 −2．従業者に対する教育・啓発 −具体的な方法	（右記を追加）	＜本市における措置＞	事後	事前の提出・公表が義務づけられない

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
令和8年3月2日	Ⅵ　評価実施手続 −1．基礎項目評価	2024/12/20	2026/1/26	事後	事前の提出・公表が義務づけられない
令和8年3月2日	別紙1　標準準拠システム移行前の評価書	別紙1　標準準拠システム移行前の評価書	ー	事後	事前の提出・公表が義務づけられない
	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	(1)予防接種資格を証する書類の発行（B類疾病） ・予防接種法に定めるB類疾病の一部について、予防接種対象者を抽出し、必要書類を発行・交付する。なお、A類疾病は母子手帳等で資格を窓口確認しており、接種券発行は行わない。 (2)予防接種実施報告書の検査 ・医療機関から提出される予防接種実施報告書・予診票等を予防接種台帳と突合し、被接種者の資格や実施内容等を検査する。 (3)予防接種履歴の管理 ・予防接種履歴情報を、医療機関等からの報告又は他自治体との連携によって取得し、健康管理システムに入力して管理する。 (4)予防接種券又は依頼書の発行 ・市外での予防接種を希望する市民について、申請に基づき予防接種履歴を確認して、接種券または依頼書を発行・交付する。 (5)予防接種による健康被害の救済 ・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等の給付を行う。 ＜Public Medical Hub（PMH）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、Public Medical Hub（PMH）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、マイナポータル等を介して予診票情報の入力、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、マイナンバーカードを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のシステムで用いることにより、医療機関において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。 ・自治体は、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。	1.事務の概要 ・予防接種法に基づき、伝染のおそれがある疾病の発生及びまん延を予防するために、予防接種を行い、公衆衛生の向上及び増進に寄与することを目的とした事務。 2.事務の内容 (1)予防接種資格を証する書類の発行 ・住民基本台帳の情報を基に、予診票等、予防接種の資格を証する書類を発行・配布する。（A類疾病及びB類疾病の一部を除く。） (2)予防接種実施報告書の検査 ・医療機関から提出される予防接種実施報告書・予診票等を予防接種台帳と突合し、被接種者の資格や実施内容等を検査する。 (3)予防接種履歴の管理 ・予防接種履歴情報を、医療機関等からの報告又は他自治体との連携によって取得し、予防接種台帳に入力して管理する。 (4)予防接種券又は依頼書の発行 ・市外での予防接種を希望する市民について、申請に基づき予防接種履歴を確認して、接種券または依頼書を発行・交付する。 (5)予防接種による健康被害の救済 ・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等の給付を行う。 (6)中間サーバーへの予防接種情報の副本登録と情報提供ネットワークシステムを介した情報照会・提供 ・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（以降「番号法」という。）に基づいて福山市は、予防接種に関する事務において、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特定個人情報について情報照会を行う。また、他機関からの情報照会に対応する為に、予防接種の事務に係る特定個人情報を中間サーバーに登録する。 (7)新型コロナウイルス感染症予防接種証明書の発行 ・被接種者からの申請に基づき、予防接種（特例臨時）を受けたことを証明する書類を発行する。 ＜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。 ・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。	事前	
	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	Public Medical Hub　（PMH）	予診情報・予防接種記録管理／請求支払システム	事前	
	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システムの機能	＜Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務＞ ①雛形の登録 予診票項目、通知文言等のひな形をPublic Medical Hub（PMH）へ登録する。 ②情報登録機能及びPMH-ID採番依頼機能等 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Public Medical Hub（PMH）に登録し、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-IDを自動採番する。すでにPMH-ID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-ID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 マイナポータルからのPublic Medical Hub（PMH）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-IDと紐付けてPublic Medical Hub（PMH）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。Public Medical Hub（PMH）は、PMH仮名識別子からPMH-IDを特定し、PMH-ID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、Public Medical Hub（PMH）はPMH仮名識別子からPMH-IDを特定し、PMH-ID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） ・識別子の格納機能 医療機関用アプリはマイナンバーカードの電子証明書のシリアル番号を用いてマイナポータル経由でPublic Medical Hub（PMH）に接続する。医療機関用アプリからのPublic Medical Hub（PMH）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-IDと紐付けてPublic Medical Hub（PMH）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 医療機関用アプリは、マイナンバーカードの電子証明書のシリアル番号を用いてマイナポータル経由で、Public Medical Hub（PMH）へPMH仮名識別子を利用した照会を行う。Public Medical Hub（PMH）は、PMH仮名識別子からPMH-IDを特定し、PMH-IDに紐付く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、Public Medical Hub（PMH）はPMH仮名識別子からPMH-IDを特定し、PMH-IDに紐付く接種記録を登録する。	＜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＞ 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-ID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-IDを自動採番する。すでにPMH-ID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-ID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-ID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-IDを特定し、PMH-ID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-IDを特定し、PMH-IDに紐付く予診票情報を登録する。 ④情報連携機能（医療機関用アプリ等） ・本人確認情報の格納機能 予防接種対象者が、認証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-IDを特定し、PMH-ID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-ID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-ID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。	事前	
	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 ③他のシステムとの接続	その他（健康管理システム、マイナポータル、医療保険者等向け中間サーバー）	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）	事前	
	Ⅰ 基本情報 −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	（右記を追加）	・新型コロナウイルス感染症予防接種証明書（特例臨時）を発行するため。	事前	

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 −4．特定個人情報ファイルを取り扱う理由 ②実現が期待されるメリット	（右記を追加）	・新型コロナウイルス感染症予防接種証明書（特例臨時）を発行することができる。	事前	
	Ⅰ 基本情報 −5．個人番号の利用 法令上の根拠	・行政手続における特定の個人を識別するための番号の利用等に関する法律（以降「番号法」という。）第9条第1項　別表の第14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	・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（以降「番号法」という。）第9条第1項　別表の第14の項 ・番号法第19条第6、8、16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	事前	
	Ⅰ 基本情報 −6．情報提供ネットワークシステムによる情報連携 ②法令上の根拠	（情報照会） ・番号法第19条第8号 ・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25、27、28、29の項 （情報提供） ・番号法第19条第8号 ・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25、26の項	（情報照会） ・番号法第19条第8号 ・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25、27、28、29の項 （情報提供） ・番号法第19条第8号 ・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25、26、153、154の項	事前	
	（別添１）事務の内容		概要全体図の一部修正	事前	
	（別添１）事務の内容 （備考）	①特定個人情報の登録・管理 ・情報連携のため、本市区町村は、Public Medical Hub（PMH）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。（LGWAN回線等経由） ・PMHから接種記録等、必要な情報をダウンロードし、既存システムへの取込、支払等の事務処理を行う。 ・PMH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−ID採番 ・PMHは、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMH−IDの採番処理を依頼し、医療保険者等向け中間サーバーは、PMH−IDを採番してPMHに回答する。医療保険者等向け中間サーバーは、PMH−IDと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムは、紐付番号をキーに仮名識別子とPMH−ID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−IDと紐付けて、PMHに連携する。（連携後、マイナポータル上からPMH−IDは削除される。）以降、③④⑤が可能となる。 ③マイナポータルへの通知 ・PMHからマイナポータル経由で住民向けの通知を行うため、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PMHへの予診票の事前入力や、PMHから接種記録や通知情報を閲覧/取得する。 ⑤医療機関からの入力・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、マイナポータル経由で、接種時に住民から本人同意を得て、事前入力された予診票及び接種記録の閲覧/取得/入	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の登録を行う。（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。	事前	
	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 主な記録項目	その他（<Public Medical Hub（PMH）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	事前	
	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	<Public Medical Hub（PMH）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−ID、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 予防接種番号…PMH内で予防接種の種類を区別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、PMHが、外部と情報連携するために必要となる。	<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> (1)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。 (2)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。	事前	
	Ⅱ　特定個人情報ファイルの概要 −3．特定個人情報の入手・使用 ①入手元	民間事業者（医療機関・支払基金） その他（住民基本台帳ネットワークシステム）	民間事業者（医療機関） その他（住民基本台帳ネットワークシステム、DX審査支払機構）	事前	

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．特定個人情報の入手・使用 ②入手方法	（その他欄に右記を追加）	Public Medical Hub、医療機関用アプリ等、マイナポータル	事前	
	Ⅱ　特定個人情報ファイルの概要 －3．特定個人情報の入手・使用 ③入手の時期・頻度	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> ・PMH-IDの採番処理依頼時に都度、医療保険者等向け中間サーバーから特定個人情報を入手する。 ・本市区町村がPMHに登録した予診票のひな形に対して、住民がマイナポータル等を介して接種前に予診票情報を入力することにより個人情報を入手し、事務・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、従来の紙の予診票に代えて、医療機関のタブレットに搭載された医療機関用アプリを用いて、住民がマイナンバーカードで認証して同意することにより、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、事務・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。	<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。 ・国が予診情報・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。	事前	
	Ⅱ　特定個人情報ファイルの概要 －3．特定個人情報の入手・使用 ④入手に係る妥当性	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> （PMH-ID採番処理依頼時に入手される特定個人情報） ・外部との情報連携のため、PMH-IDの採番処理依頼時に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、事務・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） 入手にあたって、既存事務と同様に予診票の事前入力する事項については、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については、予防接種を実施する医療機関から入手する必要がある。 ・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入力され、入力した情報は、接種を受託する医療機関で確認され、接種の可否を判断する。 ・医療機関では、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・接種記録のオンライン化により住民及び医療機関での利便性の向上及び、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して同意することにより、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。	<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。	事前	
	Ⅱ　特定個人情報ファイルの概要 －3．特定個人情報の入手・使用 ⑤本人への明示	<Public Medical Hub（PMH）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、同意することにより入手する。	<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して、本人確認することにより入手する。	事前	
	Ⅱ　特定個人情報ファイルの概要 －3．特定個人情報の入手・使用 ⑥使用目的	（右記を追加）	予防接種に係る証明書の発行	事前	

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．特定個人情報の入手・使用 ⑧使用方法	(1)～(4)省略 <Public Medical Hub（PMH）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、Public Medical Hub（PMH）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。 ・登録後、Public Medical Hub（PMH）は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub（PMH）が連動するためのPMH-ID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-IDを採番して個人番号と共にPublic Medical Hub（PMH）に応答する。 ・PMH-ID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Public Medical Hub（PMH）で共有されることでPublic Medical Hub（PMH）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（マイナポータル経由）からPublic Medical Hub（PMH）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。	(1)～(4)省略 (5)予防接種に係る証明書の発行 接種記録や本人から提示されたパスポート情報を元に証明書を発行する。 <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。	事前	
	Ⅱ　特定個人情報ファイルの概要 －3．特定個人情報の入手・使用 ⑧使用方法 情報の統計分析	<Public Medical Hub（PMH）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。	<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。	事前	
	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 委託の有無	1件	2件	事前	
	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	Public Medical Hub（PMH）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	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	事前	
	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	Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務	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	事前	
	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	Public Medical Hub（PMH）は国（デジタル庁）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-ID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、PMHに格納された特定個人情報は、自動処理により再委託先に情報連携されるため、国（デジタル庁）は特定個人情報にアクセスすることはない。	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、広島県国民健康保険団体連合会（以下、広島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。	事前	
	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	国（デジタル庁）	広島県国保連合会	事前	

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 －4．特定個人情報ファイルの取扱いの委託 委託事項2 再委託 ⑨再委託事項	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> ・Public Medical Hub（PMH）の運用保守 ・PMH-IDの採番及びPMH-ID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-IDを介して行うため、特定個人情報を取り扱わない。	<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> ・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。	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先1 ④提供する情報の対象となる本人の数	1万人以上10万人未満	10万人以上100万人未満	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先2 ④提供する情報の対象となる本人の数	1万人以上10万人未満	10万人以上100万人未満	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3	（右記を追加）	厚生労働大臣	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3 ①法令上の根拠	（右記を追加）	・番号法第19条第8号 ・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154の項	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3 ②提供先における用途	（右記を追加）	新型インフルエンザ等対策特別措置法（平成二十四年法律第三十一号）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	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3 ③提供する情報	（右記を追加）	予防接種履歴	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3 ④提供する情報の対象となる本人の数	（右記を追加）	10万人以上100万人未満	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3 ⑤提供する情報の対象となる本人の範囲	（右記を追加）	福山市に住民登録があった、予防接種事業の対象者	事前	

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 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3 ⑥提供方法	（右記を追加）	[〇]情報提供ネットワークシステム	事前	
	Ⅱ　特定個人情報ファイルの概要 －5．特定個人情報の提供・移転（委託に伴うものを除く。） 提供先3 ⑦時期・頻度	（右記を追加）	・照会を受けた都度	事前	
	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	<Public Medical Hub（PMH）を活用した情報連携に係る予防接種事務> Public Medical Hub（PMH）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または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（デジタル庁）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。	<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。	事前	
	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 　期間	5年	20年以上	事前	
	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 　その妥当性	・予防接種法第9条の3、予防接種法施行規則第3条及び特定個人情報に係る副本登録・更新に係る基本ルールにおいて、5年間のデータ保管が義務付けられている。	・予防接種法第9条の3、予防接種法施行規則第4条より電磁的記録として当該定期の予防接種等を行ったときから当該定期の予防接種等を受けた者が死亡した日の翌日から五年を経過する日までの間保存しなければならないとされている。	事前	
	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	<Public Medical Hub（PMH）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、Public Medical Hub（PMH）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、古いものから順に自動削除される。	<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> ・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。	事前	

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
	（別添2）特定個人情報ファイル記録項目	＜Public Medical Hub（PMH）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-ID ・PMH仮名識別子 ・基本5情報（カナ・氏名・住所・生年月日・性別） ・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） (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 ・予防接種予定動奨ID ・予防接種設定ID ・予防接種予定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 ・予防接種予定ID ・履歴ID ・接種日 ・接種同意フラグ ・医療機関コード ・医師名 ・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 ・ロット番号 ・接種量 ・ワクチン有効期限 ・特別の事情 ・更新日時 ・最新/削除フラグ	＜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ID ・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 ・委注医師接種フラグ ・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）	事前	
	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（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 　対象者以外の情報の入手を防止するための措置の内容	＜Public Medical Hub（PMH）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＞ ・PMH-IDの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで対象者以外の情報の入手を防止する。（当該機能は、R6年度中に実装予定） ・医療機関の受付窓口で本人確認の後、医療機関用アプリ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、医療機関用アプリでの入力は、診察室内で更に本人確認を行うことで本人の情報のみがPublic Medical Hub（PMH）へ連携される。 ・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Public Medical Hub（PMH）に連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。	＜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。	事前	
	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（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 　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	＜Public Medical Hub（PMH）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（PMH）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-ID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。	＜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。 ・「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。	事前	

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（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2 　リスクに対する措置の内容	＜Public Medical Hub（PMH）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（PMH）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-ID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。 ・Public Medical Hub（PMH）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。	＜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。 ・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。	事前	
	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（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3 　入手の際の本人確認の措置の内容	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）が提供した個人番号を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。	＜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。 ・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。	事前	
	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（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3 　個人番号の真正性確認の措置の内容	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）が提供した個人番号を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。	＜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。 ・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。	事前	
	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（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3 　特定個人情報の正確性確保の措置の内容	＜Public Medical Hub（PMH）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。	＜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。	事前	
	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（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4 　リスクに対する措置の内容	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）と支払基金の医療保険者等向け中間サーバーは、暗号化された閉域網で接続される。 ・医療機関や住民からPublic Medical Hub（PMH）への連携は、直接接続ではなく、マイナポータルAPI経由の接続のみが認められ、通信内容は、情報漏洩を防止するために暗号化される。	＜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。	事前	

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	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）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。 ・Public Medical Hub（PMH）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マイナポータルAPI経由でPublic Medical Hub（PMH）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。	＜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。	事前	
	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 　ユーザ認証の管理 　具体的な管理方法	＜Public Medical Hub（PMH）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、Public Medical Hub（PMH）のアクセス権限を管理する管理者を定める。 ・Public Medical Hub（PMH）のログインはユーザID・パスワードで行う。 ・Public Medical Hub（PMH）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。 ・Public Medical Hub（PMH）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Public Medical Hub（PMH）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。	＜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。	事前	
	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 　アクセス権限の発行・失効の管理 　具体的な管理方法	＜Public Medical Hub（PMH）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＞ ・Public Medical Hub（PMH）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。 ・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。	＜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。	事前	
	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 　具体的な管理方法	＜Public Medical Hub（PMH）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。 ・パスワードの有効期限を設定する。 ・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。	＜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。	事前	
	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 　具体的な管理方法	＜Public Medical Hub（PMH）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。 ・パスワードの有効期限を設定する。 ・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。	＜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。	事前	

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3 　リスクに対する措置の内容	＜Public Medical Hub（PMH）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＞ ・特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、事務外の使用を防止している。 ・委託業務については、委託先との契約により、委託業者が従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。本市区町村は、当該教育の実施について履行確認を行う。 ・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。	＜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、委託業者が従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。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。	事前	
	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 　リスクに対する措置の内容	＜Public Medical Hub（PMH）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Public Medical Hub（PMH）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Public Medical Hub（PMH）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。 ・Public Medical Hub（PMH）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。	＜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。	事前	
	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	＜Public Medical Hub（PMH）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、Public Medical Hub（PMH）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国（デジタル庁）に委託することとする。 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）に基づき、委託先となる国（デジタル庁）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。	＜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広島県国保連合会に委託し、広島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。	事前	
	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	＜Public Medical Hub（PMH）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。 ・アクセス権限を付与する者を必要最小限に限定する。 ・アクセス権限を付与する範囲を必要最小限に限定する。 ・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、再委託先（PMH-ID採番や運用保守）のみに付与される。	＜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。	事前	
	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 　具体的な方法	＜Public Medical Hub（PMH）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＞ ・特定個人情報の取り扱いのログを保存し、提供を求めることができる。 ※再委託先（PMH-ID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。	＜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。	事前	

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 　特定個人情報ファイルの提供ルール 　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の遵守の確認方法	<Public Medical Hub（PMH）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（再委託も含む。）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（再委託先も含む。）から他者への提供が行われていないことを確認できる。	<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。	事前	
	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の遵守の確認方法	<Public Medical Hub（PMH）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（再委託先も含む。）から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。	<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。	事前	
	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の遵守の確認方法	<Public Medical Hub（PMH）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> ・委託契約終了後は保管していた全ての特定個人情報を消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、消去について、本市区町村は報告を受けることができ、それにより消去状況について確認が可能となる。	<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。	事前	
	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	<Public Medical Hub（PMH）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> 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	<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> 広島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 ・実地の監査、調査等に関する事項	事前	
	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	<Public Medical Hub（PMH）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> ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるデジタル庁が、再委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、年1回デジタル庁から報告を受ける。	<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、点検結果について広島県国保連合会及び本市に年1回報告を行う。	事前	
	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	<Public Medical Hub（PMH）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。 委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。	<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。	事前	

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 ⑤物理的対策 　具体的な対策の内容	<Public Medical Hub（PMH）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> Public Medical Hub（PMH）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または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を利用している。	<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	事前	
	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	<Public Medical Hub（PMH）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> Public Medical Hub（PMH）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または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。 ・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（デジタル庁）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、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Public Medical Hub（PMH）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Public Medical Hub（PMH）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。	<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。	事前	
	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2 リスクに対する措置の内容	<Public Medical Hub（PMH）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。	<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。	事前	
	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 消去手順 手順の内容	<Public Medical Hub（PMH）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、古いものから順に自動削除される。	<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。	事前	

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
	Ⅳ　その他のリスク対策 －1．監査 ①自己点検 　具体的なチェック方法	＜Public Medical Hub（PMH）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。	＜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。	事前	
	Ⅳ　その他のリスク対策 －1．監査 ②監査 　具体的な内容	＜Public Medical Hub（PMH）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。	＜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。	事前	
	Ⅳ　その他のリスク対策 －2．従事者に対する教育・啓発 　従業者に対する教育・啓発 　具体的な方法	＜Public Medical Hub（PMH）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。	＜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。	事前	
	Ⅳ　その他のリスク対策 －3．その他のリスク対策	＜Public Medical Hub（PMH）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。	＜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。	事前	
	Ⅴ　開示請求、問合せ ④個人情報ファイル簿の公表 　個人情報ファイル名	（右記を追加）	新型コロナウイルス感染症対策に係る予防接種業務	事前	
	Ⅵ　評価実施手続 －1．基礎項目評価 ①実施日	2026/1/26		事前	
	Ⅵ　評価実施手続 －2．国民・住民等からの意見の聴取 ①方法	「福山市パブリックコメント実施要項」に基づき、パブリックコメントを実施した。実施に際しては、パブリックコメントを実施する旨を報道提供するとともに、市ホームページ及び市内公共施設にて全文を閲覧できるようにした。	「福山市パブリックコメント実施要項」に基づき、パブリックコメントを実施した。実施に際しては、パブリックコメントを実施する旨を市の広報誌へ掲載するとともに、市ホームページ及び予防接種事務関連部署にて全文を閲覧できるようにした。	事前	
	Ⅵ　評価実施手続 －2．国民・住民等からの意見の聴取 ②実施日・期間	2024年（令和6年）10月1日～10月31日	2026年（令和8年）10月1日～11月2日	事前	