

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
8	明石市 予防接種に関する事務 全項目評価書

個人のプライバシー等の権利利益の保護の宣言

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

特記事項

—

評価実施機関名

明石市長

個人情報保護委員会 承認日【行政機関等のみ】

公表日

項目一覧

I 基本情報
（別添1）事務の内容
II 特定個人情報ファイルの概要
（別添2）特定個人情報ファイル記録項目
III 特定個人情報ファイルの取扱いプロセスにおけるリスク対策
IV その他のリスク対策
V 開示請求、問合せ
VI 評価実施手続
（別添3）変更箇所

I 基本情報

1. 特定個人情報ファイルを取り扱う事務

①事務の名称	予防接種に関する事務
②事務の内容 ※	予防接種法(昭和23年6月30日法律第68号)及び新型インフルエンザ等対策特別措置法(平成24年5月11日法律第31号)に基づき、市内に居住する者に対し予防接種を実施するとともに、接種歴等の情報管理・報告や給付の支給に対する事務等を行う。 ＜予診情報・予防接種記録管理／請求支払システム(以下「予予請求システム」という。)を活用した情報連携に係る予防接種事務＞ ・本市は、情報連携のため、予予請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 ・住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 ・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 3) 1万人以上10万人未満 5) 30万人以上 2) 1,000人以上1万人未満 4) 10万人以上30万人未満

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1	
①システムの名称	健康かるてV8
②システムの機能	①照会機能 選択した対象者が受けた予防接種の種類、接種日、実施医療機関名等を表示する。個人の属性(氏名、生年月日等)が表示される。 ②入力機能 選択した対象者が受けた予防接種の種類、接種日、実施医療機関名等を入力する。 ③予防接種対象者等への発行機能 指定した予防接種の対象者を抽出し、一覧表、予防接種券(シール)等出力する。
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 [] 住民基本台帳ネットワークシステム [○] 宛名システム等 [] その他 () [○] 庁内連携システム [] 既存住民基本台帳システム [] 税務システム
システム2	
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 申告書等の受付などを行う際、窓口における本人確認のため、提示された個人番号カード等を基に住基ネットが保有する本人確認情報に照会を行い、確認結果を画面上に表示する機能。 ②本人確認情報検索 統合端末において入力された5情報(氏名、氏名の振り仮名、住所、性別、生年月日)の組み合わ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機能。 ③地方公共団体情報システム機構への情報照会 全国サーバに対して個人番号又は5情報の組み合わせをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する機能。
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 住民基本台帳ネットワークシステム [] 宛名システム等 [] その他 () [] 庁内連携システム [○] 既存住民基本台帳システム [] 税務システム

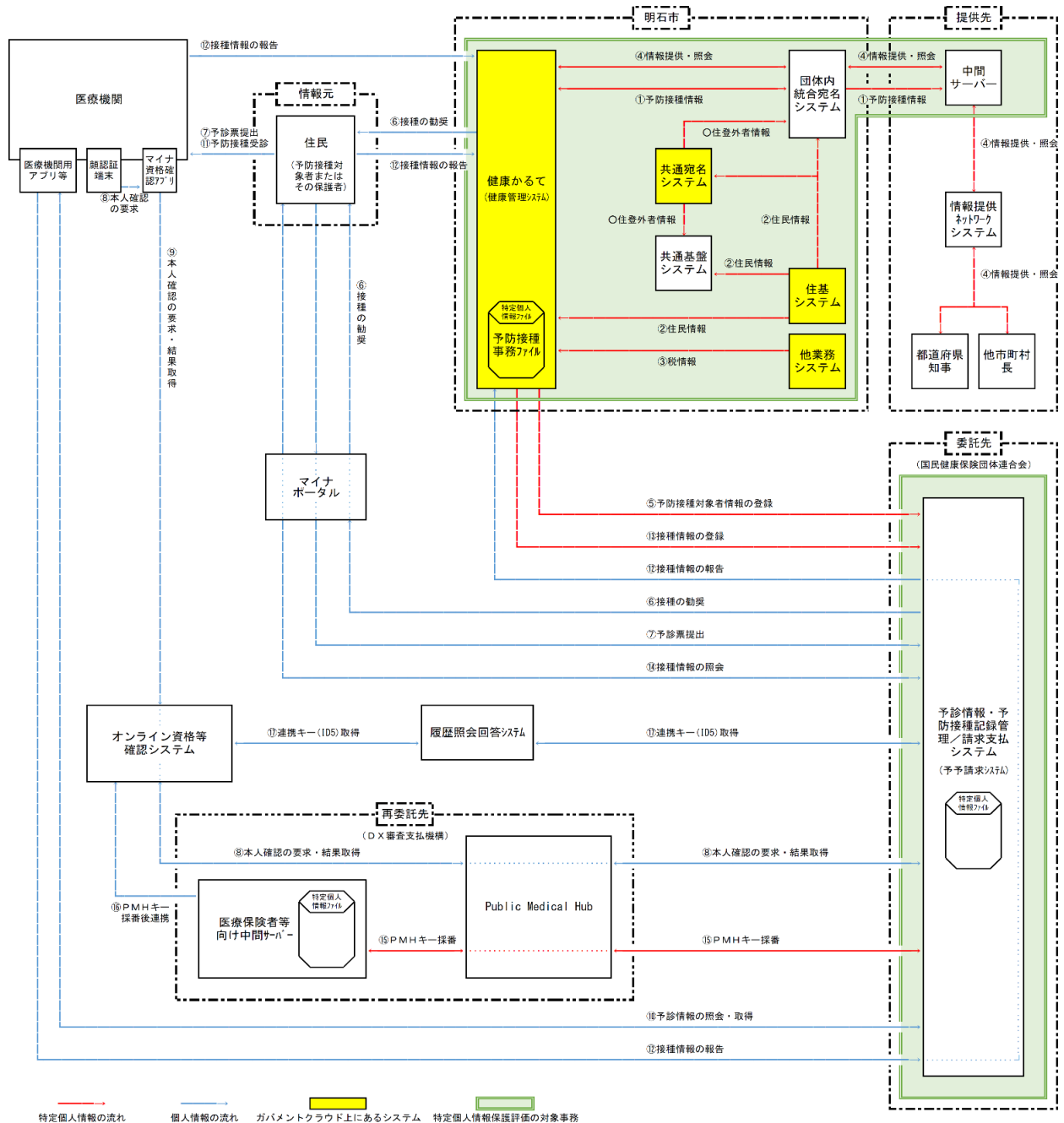
システム3	
①システムの名称	共通基盤システム（庁内連携システムと同義）
②システムの機能	①統合データベース機能 各事務システムが共通で参照する業務データの副本を一元管理する機能。 ② データ連携機能 ア 各事務システム間のデータ連携について、データ提供事務システムよりデータを受け取り、データ利用事務システムに合わせた連携用データを作成し、格納する機能。 イ 標準準拠システムに移行した各事務システムとのデータ連携について、ガバメントクラウド上で連携データを格納する機能。 ③共通データ管理機能 全庁的に利用する共通データ情報を管理する機能。
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 庁内連携システム [] 住民基本台帳ネットワークシステム [○] 既存住民基本台帳システム [] 宛名システム等 [○] 税務システム [○] その他 （ 各事務システム(パッケージシステム))
システム4	
①システムの名称	団体内統合宛名システム（宛名システム等と同義）
②システムの機能	①宛名管理機能 個人番号で同一人判定を行い、団体内統合宛名番号（以下「統合宛名番号」という。）を採番し、管理する機能。 ②情報提供機能 各事務の情報を中間サーバーに連携する機能。 ③情報照会機能 宛名コードで対象者を検索し、他自治体への情報提供を依頼し、結果をオンラインにて表示する機能。
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 庁内連携システム [] 住民基本台帳ネットワークシステム [○] 既存住民基本台帳システム [] 宛名システム等 [○] 税務システム [○] その他 （ 中間サーバー、各事務システム(パッケージシステム))

システム5	
①システムの名称	中間サーバー
②システムの機能	①符号管理機能 情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 ②情報照会機能 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領(照会した情報の受領)を行う機能。 ③情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う機能。 ④既存システム接続機能 中間サーバーと既存システム、団体内統合宛名システム及び住基システムとの間で情報照会内容、情報提供内容、特定個人情報(連携対象)、符号取得のための情報等について連携するための機能。 ⑤情報提供等記録管理機能 特定個人情報(連携対象)の照会、又は提供があった旨の情報提供等記録を生成し、管理する機能。 ⑥情報提供データベース管理機能 特定個人情報(連携対象)を副本として、保持・管理する機能。 ⑦データ送受信機能 中間サーバーと情報提供ネットワークシステム(インターフェイスシステム)との間で情報照会、情報提供、符号取得のための情報等について連携するための機能。 ⑧セキュリティ管理機能 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、電文及び情報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 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能。 ⑩システム管理機能 バッチの状況管理、業務統計情報の集計、稼働状態の通知、保管期限切れ情報の削除、機関別設定情報の管理を行う機能。 ⑪自己情報提供機能 情報提供ネットワークシステムを介して自己情報に対する提供の求めを受領し、当該の特定個人情報(連携情報)及び自己情報提供用添付ファイルの提供を行う機能。 ⑫お知らせ機能 お知らせ情報提供対象者へのお知らせ情報の送信依頼に対し、情報提供ネットワークシステムを介して、お知らせ情報の提供を行う。また、お知らせ情報提供対象者へ提供したお知らせ情報に対する状況確認依頼に対し、情報提供ネットワークシステムを介して回答結果の受領を行う機能。
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6	
①システムの名称	予予請求システム
②システムの機能	①予防接種関連データの登録機能 本市は、健康管理システムからの情報連携又は予予請求システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予予請求システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予予請求システムは、本市で管理している個人番号、対象者情報、予診票情報及び接種記録を予予請求システムに登録する。また、Public Medical Hubを経由して医療情報基盤・診療報酬審査支払機構（以下、「DX審査支払機構」という。）の医療保険者等向け中間サーバーと連動し、PMHキーを自動採番する。すでにPMHキーが採番済みの個人番号であれば、採番は行わずに既存のPMHキーを利用する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 予予請求システムは、マイナポータルからの予予請求システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予予請求システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナナンバーカードの電子証明書のシリアル番号に紐付くPMH仮名識別子を利用した照会を行う。予予請求システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く接種記録・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、予予請求システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐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ナンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリ等は、予予請求システムへ本人確認情報を利用した照会を行う。予予請求システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐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、予予請求システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐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 予予請求システムは接種記録等の情報を予防接種DBに連携し、予防接種DBにおいて予防接種の有効性・安全性等の調査・研究を行う。予予請求システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐づけて予予請求システムに連携する。
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 庁内連携システム [] 住民基本台帳ネットワークシステム [] 既存住民基本台帳システム [] 宛名システム等 [] 税務システム [☒] その他 （ 健康かるてV8、マイナポータル、医療機関用アプリ等、Public Medical Hub、 ） 履歴照会回答システム
3. 特定個人情報ファイル名	
予防接種事務ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	予防接種の対象者及び接種履歴を正確に把握し、適正な管理を行うために必要である。また、対象者の所得状況を判断し、公平・公正な実費徴収を行うためにも必要である。
②実現が期待されるメリット	現行の予防接種の対象者であることの確認及び受けた予防接種の履歴を管理するシステム台帳管理に加え、番号制度と結びつけることにより、転入転出時等における効率的な事務が可能となる。また、情報提供ネットワークを通じて他市町村の地方税情報等を照会することが可能となり、実費徴収に関する面で、低所得者対策として講じている自己負担金免除の手続きが簡素化され、市民の負担軽減につながる。

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に関する法律（平成25年法律第27号）（以下「番号法」という。）第9条第1項及び別表の項番14、126 番号法別表の主務省令で定める事務を定める命令（平成26年内閣府・総務省令第5号）第10条、第67条の2 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ 明石市個人番号の利用に関する条例（平成27年12月28日条例第34号） ※令和9年9月頃条例改正予定
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	＜情報提供の根拠＞ 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（令和6年デジタル庁・総務省令第9号）第2条項番25、26、153、154 ＜情報照会の根拠＞ 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条項番25、27、28、29、153
7. 評価実施機関における担当部署	
①部署	福祉局あかし保健所保健予防課 ／ こども局子育て支援室こども健康課
②所属長の役職名	課長 ／ 課長
8. 他の評価実施機関	
—	

(別添1) 事務の内容



(備考)

- ① 予防接種関係情報を、団体内統合宛名システムに連携する。
- ② 住基システムから、住民情報を連携する。
- ③ 他業務システムから、税情報を連携する。
- ④ 必要に応じて、団体内統合宛名システムから、他自治体へ予防接種関係情報、税情報等の情報照会を行う。
- ⑤ 予防接種対象者情報を、予防請求システムに連携する。
- ⑥ 接種の勧奨を行う。(接種券を印刷し送付する。)
- ・ 予防請求システムを用いて接種勧奨を行う場合は、登録された予防接種対象者情報を基に同システムからマイナポータルに通知を送信する。
- ・ 予防請求システムを用いず接種勧奨を行う場合は、健康管理システムから接種券を印刷し送付する。
- ⑦ 予診票を提出する。
- ・ 電子予診票を利用する場合は、マイナポータルより予診情報を入力し予防請求システムに登録する。
- ・ 電子予診票を利用しない場合は、紙予診票を医療機関等に提出する。
- ⑧ 顔認証アプリから、マイナ資格確認アプリ等を通じ予防接種対象者の本人確認を要求する。
- ⑨ マイナ資格確認アプリ等から、オンライン資格確認等システム及びPublic Medical Hubを通じ予防請求システムに本人確認を要求しその結果を取得する。
- ⑩ 医療機関アプリ等から予防請求システムに登録された予診情報を照会し取得する。(電子予診票利用の場合のみ。)
- ⑪ 医療機関等で予防接種を受ける。

⑫接種情報の報告を行う。

- ・予予請求システムを利用して予防接種事務を行う全国集合契約に参加している医療機関等は予予請求システムに接種情報を登録し、明石市は予予請求システムより接種情報を受領する。
- ・予予請求システムを利用する全国集合契約に参加しておらず直接明石市と予防接種事務を行う契約をしている医療機関等は、接種券または予診票により接種情報を明石市へ提出する。
- ・上記に該当しない医療機関で予防接種を受けた住民は、予診票等により接種情報を明石市へ提出する。

⑬接種情報を予予請求システムに連携する。(予予請求システム以外から接種情報を取得した場合のみ。)

⑭マイナポータルより予予請求システムに登録された接種情報を照会し取得する。

⑮予予請求システムは、予防接種対象者にかかるPMHキーを、Public Medical Hubを通じ医療保険者向け中間サーバーに採番依頼し、採番された結果を取得する。

⑯医療保険者向け中間サーバーは、採番されたPMHキーをオンライン資格確認等システムに連携する。

⑰予予請求システムは、厚生労働省が保有する予防接種等関連情報データベースに連携するためのキー「ID③」を、履歴照会回答システムを通じオンライン資格確認システムから取得する。

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	
予防接種事務ファイル	
2. 基本情報	
①ファイルの種類 ※	システム用ファイル <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	10万人以上100万人未満 <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	予防接種券の発行履歴がある者及び予防接種歴のある者
その必要性	予防接種対象者の管理、予防接種状況の管理を正確に行うため
④記録される項目	50項目以上100項目未満 <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 (予防接種記録情報)
その妥当性	・個人番号、その他識別情報:対象者を正確に特定するために保有 ・5情報、連絡先:正確な本人特定のため、予防接種等に記入された情報と突合するために保有、また、予防接種の接種勧奨に使用するため保有 ・その他住民票関係情報:予防接種費用の実費徴収の免除決定にあたり、世帯状況を確認するために保有 ・地方税関係情報:予防接種の実費に係る負担の有無を決定するために保有 ・予防接種記録情報:接種記録の管理を行うために記録 <予予請求システムを活用した情報連携に係る予防接種事務> ・その他識別情報(内部番号):PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5:予予請求システムが、外部と情報連携するために必要となる。 ・その他(予防接種記録情報):予予請求システムが、外部と情報連携するために必要となる。
全ての記録項目	別添2を参照。
⑤保有開始日	平成28年1月1日 <予予請求システムを活用した情報連携に係る予防接種事務に係る情報> 令和10年4月1日以降で本市が同事務を開始可能な日
⑥事務担当部署	福祉局あかし保健所保健予防課 / こども局子育て支援室こども健康課

3. 特定個人情報の入手・使用	
①入手元 ※	[☐] 本人又は本人の代理人 [☐] 評価実施機関内の他部署 (市民課) [☐] 行政機関・独立行政法人等 () [☐] 地方公共団体・地方独立行政法人 (市町村) [☐] 民間事業者 (医療機関) [☐] その他 (DX審査支払機構)
②入手方法	[☐] 紙 [☐] 電子記録媒体(フラッシュメモリを除く。) [☐] フラッシュメモリ [☐] 電子メール [☐] 専用線 [☐] 庁内連携システム [☐] 情報提供ネットワークシステム [☐] その他 (Public Medical Hub、医療機関用アプリ等、マイナポータル)
③入手の時期・頻度	・本人や医療機関から予防接種実施の報告がある都度 ・本人から予防接種費用の実費に係る免除申請がある都度 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ ・予予請求システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・国が予予請求システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本市が個人情報を入手し、予予請求システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等または医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予予請求システムにおいて個人番号と結びついて特定個人情報となる。
④入手に係る妥当性	・共通基盤システムより入手する住民情報・住民登録外情報は、接種対象者であることの確認を行うため入手する。 ・共通基盤システム(もしくは情報提供ネットワークを利用して他市町村)より入手する世帯情報及び地方税関係情報については、本人から実費免除の申請を受けた都度、税額を確認する必要があるため入手する。 ・医療機関や本人等から入手する接種記録については、予防接種法施行令第6条の2に基づき記録・保存する必要があるため入手する。 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ (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。 (個人情報として入手し、予予請求システムにおいて個人番号と結び付き特定個人情報となる情報) ・本市が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入手し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証(本人確認)の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。
⑤本人への明示	・共通基盤システムより取得する情報については、本人に利用目的を明示し、同意を得た上で入手している。 ・情報提供ネットワークを利用して他市町村から地方税関係情報を確認する必要がある場合については、書面にて同意を得た上で入手している。 ・医療機関や本人等から入手の場合、本人等が記入する予診票にも、本市へ接種記録が提出されることを明記し、署名を得ている。 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ ・マイナポータル等では、本人等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 ※		対象者の資格管理、接種記録の管理・保管、予防接種費用の実費の徴収に係る事務を行うため	
	変更の妥当性	－	
⑦使用の主体	使用部署 ※	福祉局あかし保健所保健予防課 ／ こども局子育て支援室こども健康課	
	使用者数	[50人以上100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住民票関係情報、本人等の申請内容等を健康かるてV8に登録し、登録された情報を基に予防接種の対象者を確認する。 ②健康かるてV8に接種記録を登録し、接種記録の管理及び保管を行う。 ③本人等の申請、住民票関係情報、地方税関係情報等の健康かるてV8に登録された情報を基に、予防接種費用の実費に係る免除対象者の確認及び確認結果の通知を行う。 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ ①情報連携のため、本市は、予予請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ②登録後、予予請求システムは、Public Medical Hubに対してオンライン資格確認等システムと予予請求システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予予請求システムに応答する。 ③PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予予請求システムで共有されることで予予請求システムからマイナポータルへの通知、マイナポータルや医療機関用アプリ等から予予請求システムの予診票情報及び接種記録の取得・閲覧・入力等といった情報連携が可能となる。	
	情報の突合 ※	・最新宛名コードにより住民票関係情報を突合し、対象者の資格を確認する。（使用方法①に該当） ・整理番号により住民票関係情報と対象者情報を確認する。（使用方法②に該当） ・個人番号により本人等の申請内容、住民関係情報、地方税関係情報を突合し、実費に係る免除対象者の確認を行う。（使用方法③に該当）	
	情報の統計分析 ※	特定の個人を判別するような情報の統計や分析は行わない。	
	権利利益に影響を与え得る決定 ※	－	
⑨使用開始日		平成28年1月1日 ＜予予請求システムを活用した情報連携に係る予防接種事務に係る情報＞ 令和10年4月1日以降で本市が同事務を開始可能な日	

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 (5) 件
委託事項1		健康管理システム構築・運用業務委託 ※導入完了後は保守・運用業務を委託する予定
①委託内容		健康管理標準準拠システム(健康かるてV8)導入業務
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 ※	全市民及び過去に市民であった者のうち予防接種歴のある者
	その妥当性	システムの運用保守・改修等の作業対象がファイル全体に及ぶため、上記範囲を委託する必要がある。
③委託先における取扱者数		[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [○] その他 (本市事務室等において、専用回線上の端末を用いて閲覧)
⑤委託先名の確認方法		明石市情報公開条例(平成14年条例第5号)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 大阪支社
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		番号連携サーバ等維持管理業務
①委託内容		団体内統合宛名システム(番号連携サーバ)の維持・運用管理 団体内統合宛名システム端末、中間サーバ端末等の維持管理
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 ※	予防接種券の発行履歴がある者及び予防接種歴のある者
	その妥当性	システムの運用保守・改修等の作業対象がファイル全体に及ぶため、上記範囲を委託する必要がある。
③委託先における取扱者数		[10人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [○] その他 (本市事務室等において、専用回線上の端末を用いて閲覧)
⑤委託先名の確認方法		明石市情報公開条例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		富士通Japan株式会社
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3		磁気テープ等保管集配業務委託	
①委託内容		システムをバックアップした磁気テープ等の集配及び保管業務	
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全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	予防接種の発行履歴がある者及び予防接種歴のある者	
	その妥当性	バックアップの対象がファイル全体に及ぶため、上記範囲を委託する必要がある。	
③委託先における取扱者数		[10人未満]	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [☒] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()	
⑤委託先名の確認方法		明石市情報公開条例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NXワンビシアークाइブズ	
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4		明石市共通管理系システム構築・運用業務委託	
①委託内容		共通基盤システム及び共通管理系システムの保守・運用業務	
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全体]	<選択肢> 1) 特定個人情報ファイルの全体 2) 特定個人情報ファイルの一部	
	対象となる本人の数	[10万人以上100万人未満]	<選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
	対象となる本人の範囲 ※	予防接種券の発行履歴がある者及び予防接種歴のある者	
	その妥当性	システムの運用保守・改修等の作業対象がファイル全体に及ぶため、上記範囲を委託する必要がある。	
③委託先における取扱者数		[10人以上50人未満]	<選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
④委託先への特定個人情報ファイルの提供方法		[] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [☒] その他 (本市事務室等において、専用回線上の端末を用いて閲覧)	
⑤委託先名の確認方法		明石市情報公開条例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		富士通グループ明石市共通管理系システム構築・運用業務共同事業体	

再委託	⑦再委託の有無 ※	☐ 再委託する ☐ 再委託しない
	⑧再委託の許諾方法	・委託先から再委託承諾申請書の提出があり、本市が再委託承諾書により承諾した場合に限る。 ・再委託先から従業者名簿及び再委託先の従業者から個人情報の取扱いに関する誓約書を提出させる。
	⑨再委託事項	共通基盤システム等の保守・運用業務における作業担当として、技術支援作業を行う。
委託事項5		予予請求システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱いに係る業務委託 ※本件については、記載の内容に則り、令和10年4月1日以降で本市が同事務を開始可能な日から実施予定
①委託内容		予予請求システムの利用・情報連携業務及び運用保守業務
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 ☐ 特定個人情報ファイルの全体
	対象となる本人の数	☐ 10万人以上100万人未満 ☐ 1万人未満 ☐ 1万人以上10万人未満 ☐ 10万人以上100万人未満 ☐ 100万人以上1,000万人未満 ☐ 1,000万人以上
	対象となる本人の範囲 ※	全市民及び過去に市民であった者のうち予防接種歴のある者
	その妥当性	予予請求システムは公益社団法人国民健康保険中央会（以下、国保中央会という。）が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。 ただし、予予請求システムに格納された特定個人情報は、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、兵庫県国民健康保険団体連合会（以下、兵庫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 ☐ 10人未満 ☐ 50人以上100人未満 ☐ 500人以上1,000人未満 ☐ 10人以上50人未満 ☐ 100人以上500人未満 ☐ 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また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		兵庫県国保連合会
再委託	⑦再委託の有無 ※	☐ 再委託する ☐ 再委託しない
	⑧再委託の許諾方法	書面または電磁的方法による承諾
	⑨再委託事項	・予予請求システムの運用保守 ・PMHキーの採番及びPMHキーを介した医療機関用アプリ等・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。

5. 特定個人情報の提供・移転（委託に伴うものを除く。）

提供・移転の有無	[☐] 提供を行っている（ 件）[☐] 移転を行っている（ 件） [☐] 行っていない
提供先1	都道府県知事又は市町村長
①法令上の根拠	番号法第19条第8号及び番号法第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条項番25、26
②提供先における用途	予防接種法(昭和23年法律第68号)による予防接種の実施、給付の支給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	予防接種に関する記録
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	本市が予防接種法に基づき実施する予防接種を受けた者
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	特定個人情報の提供依頼がある都度
提供先2	市町村長
①法令上の根拠	番号法第19条第8号及び番号法第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条項番153
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24年法律第31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	予防接種に関する記録
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	本市が新型インフルエンザ等対策特別措置法に基づき実施する予防接種を受けた者
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	特定個人情報の提供依頼がある都度

6. 特定個人情報の保管・消去

①保管場所 ※		＜健康からてV8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、クラウド事業者は政府情報システムのためのセキュリティ評価制度（以下「ISMAP」と記載。）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。 ＜団体内統合宛名システム、共通基盤システムにおける措置＞ ・団体内統合宛名システムサーバーは庁舎の管理区域内に、その他のサーバは入館管理が厳重な庁舎外のデータセンターに設置しており、サーバー室への入室についても、厳重に管理されている。なお、本市においては、当該サーバーへアクセス権限を有する端末のみ使用している。 ・特定個人情報は、サーバー室に設置されたサーバーのデータベース内に保存されている。 ＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、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。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームは、ISMAPのリストに登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 ＜紙、電子記録媒体における措置＞ ・帳票等の保管については、職員以外の者が入室できない書庫等にて保管する。 ・電子記録媒体の保管については、課内鍵付きの保管庫において保管する。 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ 予予請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、ISMAPのリストに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	＜選択肢＞ <table><tr><td>1) 1年未満</td><td>2) 1年</td><td>3) 2年</td></tr><tr><td>4) 3年</td><td>5) 4年</td><td>6) 5年</td></tr><tr><td>7) 6年以上10年未満</td><td>8) 10年以上20年未満</td><td>9) 20年以上</td></tr><tr><td>10) 定められていない</td><td></td><td></td></tr></table>	1) 1年未満	2) 1年	3) 2年	4) 3年	5) 4年	6) 5年	7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上	10) 定められていない		
1) 1年未満	2) 1年	3) 2年												
4) 3年	5) 4年	6) 5年												
7) 6年以上10年未満	8) 10年以上20年未満	9) 20年以上												
10) 定められていない														
	その妥当性	予防接種法施行規則第4条において、接種記録については予防接種を受けた者が死亡した日の翌日から5年を経過するまで保存しなければならないと規定されているため。												

③消去方法	＜健康かるてV8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。 ＜団体内統合宛名システム、共通基盤システムにおける措置＞ ・接種履歴データについては永年保存するため、誤りがない限り、消去は行わない。 ・消去は、各事務システムと連動しているため、通常、保守・運用を行う事業者が消去することはない。 ・機器更改等の際は、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去し、消去した記録を保存する。 ＜紙媒体における措置＞ ・帳票等の破棄は、焼却・熔解処理を行い破棄する。 ・破棄の記録については、明石市文書管理規程に基づき保存する。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST800-88、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。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、ISMAPに準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ ・本市の領域に保管されたデータのみ、予予請求システムを用いて消去することができる。 ・本市の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日（作成日）を起点として3年が経過した時点で、自動的に削除される。
7. 備考	—

(別添2) 特定個人情報ファイル記録項目

(各種予防接種の接種実績情報)

1.市区町村コード、2.宛名番号、3.接種種類コード、4.回数、5.予防接種対象者番号、6.予防接種管理番号、7.履歴番号、8.最新フラグ、9.接種券番号、10.実施区分、11.接種区分、12.予防接種記録ID、13.予防接種管理ID、14.実施日、15.接種同意フラグ、16.法定区分、17.実施機関コード、18.実施機関名、19.会場コード、20.会場名、21.医師名、22.ロット番号、23.接種量、24.接種部位、25.その他(接種部位)、26.GTINコード、27.ワクチンメーカー、28.ワクチン一般名、29.ワクチン通称、30.ワクチン販売名、31.有効期限、32.特別の事情、33.特別の事情(医師補記)、34.登録日、35.登録支所、36.接種方法、37.その他(接種方法)、38.要注意接種フラグ、39.要注意接種情報、40.接種記録修正情報コード、41.間違い接種フラグ、42.間違い接種種別、43.間違い接種の理由、44.接種結果最終更新日、45.疾病名、46.予防接種を行えなかった理由、47.例外接種フラグ、48.例外接種-種別、49.登録ステータス、50.記録修正・削除の理由区分、51.記録修正・削除の理由、52.接種時年齢、53.接種時月齢、54.接種時週齢、55.海外接種フラグ、56.生活保護区分、57.非課税世帯区分、58.中国残留邦人区分、59.障がい者区分、60.その他免除区分、61.高齢者定期接種判定区分、62.備考、63.修正日、64.減免対象区分の修正理由、65.接種対象者区分の修正理由

(罹患情報)

1.市区町村コード、2.宛名番号、3.接種種類コード、4.履歴番号、5.最新フラグ、6.把握日、7.登録日、8.登録支所、9.削除フラグ

(健康被害救済制度情報)

1.市区町村コード、2.履歴番号、3.該当者_宛名番号、4.最新フラグ、5.請求日、6.給付の種類、7.請求者_宛名番号、8.接種種類コード、9.回数、10.現住所、11.現住所方書、12.請求者氏名、13.本人との続柄、14.認定区分、15.決定日、16.認定結果、17.登録日、18.登録支所、19.削除フラグ

(予診票発行情報)

1.市区町村コード、2.宛名番号、3.接種種類コード、4.回数、5.予防接種管理ID、6.予防接種対象者番号、7.予防接種管理番号、8.履歴番号、9.最新フラグ、10.発行日、11.発行場所、12.接種券番号、13.登録日、14.登録支所、15.削除フラグ

(他市町村・医療機関等への接種依頼情報)

1.市区町村コード、2.宛名番号、3.接種種類コード、4.回数、5.履歴番号、6.最新フラグ、7.受付日、8.依頼先、9.依頼理由、10.保護者_宛名番号、11.保護者_氏名、12.登録日、13.登録支所、14.削除フラグ、15.削除フラグ、16.操作者ID、17.操作年月日、18.操作時刻、19.削除フラグ、20.操作者ID、21.操作年月日、22.操作時刻、23.ワクチンメーカー、24.ワクチン一般名、25.ワクチン通称、26.ワクチン販売名、27.有効期限、28.特別の事情、29.特別の事情(医師補記)、30.登録日、31.登録支所、32.接種方法、33.その他(接種方法)、34.要注意接種フラグ、35.要注意接種情報、36.接種記録修正情報コード、37.間違い接種フラグ、38.間違い接種種別、39.間違い接種の理由、40.接種結果最終更新日、41.疾病名、42.予防接種を行えなかった理由、43.例外接種フラグ、44.例外接種-種別、45.登録ステータス、46.記録修正・削除の理由区分、47.記録修正・削除の理由、48.接種時年齢、49.接種時月齢、50.接種時週齢、51.海外接種フラグ、52.生活保護区分、53.非課税世帯区分、54.中国残留邦人区分、55.障がい者区分、56.その他免除区分、57.高齢者定期接種判定区分、58.備考、59.修正日、60.減免対象区分の修正理由、61.接種対象者区分の修正理由、62.削除フラグ

(予予システム連携情報)

1.市区町村コード、2.宛名番号、3.履歴番号、4.最新フラグ、5.変更区分、6.保護者氏名、7.不開示フラグ、8.予防接種対象者番号、9.生活保護区分、10.非課税区分、11.中国残留邦人区分、12.障がい者区分、13.その他免除区分、14.高齢者定期接種判定区分、15.長期療養区分、16.通知対象外区分、17.海外接種区分、18.その他区分、19.登録日、20.登録支所、21.削除フラグ

※上記すべてについて、個人番号、5情報(氏名・氏名の振り仮名・住所・性別・生年月日)、住民となった日、住民でなくなった日等は、システム内部で宛名番号と紐づいて保持

< 予予請求支払システムにおける記録項目 >

(対象者情報)

1.個人番号、2.PMHキー、3.PMH仮名識別子、4.5情報(氏名・氏名の振り仮名・生年月日・性別・住所)、5.保護者氏名、6.自治体コード、7.自治体業務ID、8.連携ファイル名、9.連携日時、10.連携処理ステータス/エラー内容、11.制御フラグ(リカバリー/不開示/閲覧停止)、12.変更区分、13.消除の異動日、14.その他管理番号・ID等(予防接種対象者番号)、15.その他区分等(接種対象者区分/減免区分)

(ユーザー情報)

1.機関マスタID、2.機関ユーザーID、3.メールアドレス、4.ユーザー氏名、5.ユーザー区分、6.ユーザー権限ID、7.個人番号閲覧可能フラグ、8.ユーザー削除フラグ

(予診票情報)

1.項目ID、2.管理ID、3.更新日時、4.回答ID、5.回答内容、6.回答処理ステータス、7.回答日時、8.接種不可フラグ、9.予防接種設定ID、10.予防接種管理ID、11.組み合わせ番号、12.強制失効日、13.勧奨情報(ルールID、勧奨日)

(予防接種記録情報)

1.予防接種記録ID、2.予防接種管理ID、3.接種日、4.接種同意フラグ、5.医療機関コード、6.医師名、7.実施場所、8.実施区分、9.接種区分、10.GTINコード、11.ワクチンメーカー名、12.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)、13.ロット番号、14.接種量、15.接種部位、16.接種方法、17.ワクチン有効期限、18.要注意接種フラグ、19.特別の事情、20.海外接種フラグ、21.更新日時、22.最新/削除フラグ、23.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	
予防接種事務ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	医療機関等から提出された予防接種結果を健康からてV8へ取り込む際に、住民基本台帳システムから取得した住民情報と予診票（接種券）に記載された宛名コード・氏名・住所・生年月日等とマッチングを行い登録するため、対象者以外の情報が登録されることはない。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・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）から予予請求システムに連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。
必要な情報以外を入手することを防止するための措置の内容	健康からてV8の画面および帳票には、個人番号は表示しない仕組みとし、不要な閲覧が行われないようにする。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予請求システムへは、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステムの的に制御している。 ・医療機関から医療機関用アプリ等を介して入力される際は、定められたインターフェース仕様に沿って決められたデータ項目のみが連携されるようシステムの的に制御している。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、定められたデータ項目のみのみが入力されるようシステムの的に制御している。 ・生年月日等をチェックすることで紐付け誤りを防止する機能（以下、「紐付け誤り防止機能」という。）により、誤った情報が紐付けられるリスクを低減する。
その他の措置の内容	—
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2： 不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	＜窓口・郵送での入手＞ 接種券等の申請については定型の様式を利用し、窓口においては本人又は代理人の本人確認を実施する。郵送においては、本市を宛名とするもののみを受け付ける。 ＜システムを通じた入手＞ システムを通じた入手については、システムを利用する必要がある職員を特定し、ユーザーID、パスワード及び静脈による二要素認証を実施する。また、利用機能の認可機能により、当該職員がシステム上で参照できる情報を制限することで不適切な方法で入手が行えない対策を実施している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予請求システムへは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステムの的に制御している。 ・予予請求システムのデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。
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 that 不正確であるリスク		
入手の際の本人確認の措置の内容	接種券等の申請の際には、身分証明書等の提示により本人確認を行い、身分証明書等の提示がない場合は、2点以上の本人確認書類の提示により、本人確認を行う。代理人による申請の場合、代理人自身について身分証明書等による本人確認を行うとともに、住民票上世帯外の者については、代理権者であることを示す委任状等の提出を必要とする。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムが提供した個人番号は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	・マイナンバー(個人番号)カードの提示を求め確認を行う。 ・マイナンバー(個人番号)カードの提示による確認が困難な場合は、共通宛名システムまたは住民基本台帳ネットワークシステムを利用し確認を行う。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムが提供した個人番号は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	特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、入力等を行った者以外の者が確認する等、複数人により行うこととしている。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 入手の際に特定個人情報 that 漏えい・紛失するリスク		
リスクに対する措置の内容	＜健康からてV8における措置＞ 個人番号、5情報等の宛名情報の入手については、厳重に入館・入退室管理が行われているデータセンター内のサーバー間通信に限定することにより、情報漏えい・紛失等を防止している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムとDX審査支払機構の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 ・健康管理システムは、予予請求システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置		
・端末の画面が来庁者の目に触れないように設置する。 ・受領した予診票等が他者の目に触れないようにする。 ・マイナンバーが記載された書類は、鍵のかかる書庫にて保管している。		

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク		
宛名システム等における措置の内容	・情報連携に必要な情報との紐付けは不可能としている。 ・団体内統合宛名システムへは、権限のない者の接続を認めていない。	
事務で使用するその他のシステムにおける措置の内容	健康かるてV8は、事務に関係のない情報との紐付けはできない。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予予請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予予請求システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。	
その他の措置の内容	—	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 3) 課題が残されている 2) 十分である
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、パスワード及び静脈による二要素認証を行っているため、権限のない者は利用できない。 ・認証後は、ユーザ毎に利用可能な機能を制限しているため、権限のない機能は利用できない。 ・パスワードは定期的に変更している。なお、一定期間変更がなかった場合は、ログイン時にパスワード変更画面に遷移するよう設定している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市は、予予請求システムのアクセス権限を管理する管理者を定める。 ・予予請求システムのログインはユーザID・パスワードで行う。 ・予予請求システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予予請求システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム(各業務システム)から予予請求システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。	
アクセス権限の発効・失効の管理	[行っている]	＜選択肢＞ 1) 行っている 2) 行っていない
具体的な管理方法	人事異動や権限変更があった場合は、新しく権限を付与する者および権限を失効させる者について、書面で管理者が決裁し、健康かるてV8に内容を反映している。また、権限内容について定期的に確認している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システム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	・端末操作資格者のアクセス可能機能の権限一覧表を作成している。 ・業務上アクセスが不要となった機能については、アクセス権限の変更または削除している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・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	・端末から検索、更新した際のアクセスログを記録、一定期間保存している。 ・処理日時、端末情報、部署情報、操作者情報、処理事由を記録している。 ・バックアップされたアクセスログは、7年間保存している。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、システム上の操作のログを取得し、操作ログを定期的に確認する。	
その他の措置の内容		—	
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク3: 従業者が事務外で使用するリスク			
リスクに対する措置の内容		・アクセスログを取得しており、不正利用された場合にアクセスログを追跡できる仕組みとなっている。 ・職員に対して、情報セキュリティ研修を行っている。 ・委託業者(再委託業者を含む。)に従業者に対するセキュリティ教育を義務付ける。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、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		・端末は、原則、外部媒体を使用することができない仕組みとなっている。ただし、許可された専用の外部媒体のみ、使用することができる。 ・システムのバックアップデータ等は厳重に管理されており、権限のある者のみがアクセスできる。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・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ファイルを予予請求システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・本市の既存システム(各業務システム)から予予請求システムへの特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線(LGWAN又はその他の閉域網回線)を利用した接続のみが認められる。 ・予予請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。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
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			
・ログイン後一定時間操作がない場合、自動でログオフされる仕組みとなっている。 ・スクリーンセーバ等を利用して、長時間にわたり業務画面を表示させない。 ・端末のディスプレイを来庁者から見えない位置に配置する。			

☐ 委託しない

情報保護管理体制の確認	＜システム運用・保守委託について＞ ・委託業者を選定する際、委託先の情報保護管理体制として、プライバシーマーク等の公共機関の認定・認証を取得していることを選定基準としている。 ・委託業者の選定及び契約締結の決裁を行うなかで、委託業者の社会的信用と能力を確認している。 ・委託業者の業者登録内容が有効か適時確認している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 本市は、予予請求システムの利用・情報連携業務及び運用保守業務における特定個人情報の取扱いを兵庫県国保連合会に委託し、兵庫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。
--------------------	---

具体的な制限方法	＜システム運用・保守委託について＞ ・委託業者から実施体制及び名簿を提出させ、閲覧者・更新者を必要最小限としている。 ・委託業者（作業者）に個人情報保護に係る誓約書を提出させている。 ・誓約書の提出があった者に対して必要な業務と期間のみシステム操作の権限を与えている。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・本市がアクセス権限の管理状況を確認できる。 ・本市は、アクセス権限を付与する者を必要最小限に限定する。 ・本市は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本市は、アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再々委託先（PMHキー採番や運用保守）のみに付与される。
-----------------	---

具体的な方法	システム運用・保守委託について、アクセスログまたは作業記録を残している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムは特定個人情報の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。
--------	--

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	委託先から他者への提供は認めていない。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託先(再委託先及び再々委託先を含む。)から他者への提供は行わない。 ・本市は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)から他者への提供が行われていないことを確認できる。
--	--

委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	＜システム運用・保守について＞ ・業務委託に関しては、委託契約にて委託業務実施場所を本市事務所内に限定している。 ・委託契約の調査報告条項に基づき、必要があると認めるときは調査を行い、または報告を求める。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託先(再委託先及び再々委託先を含む。)には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・本市は委託契約に基づき、委託先(再委託先及び再々委託先を含む。)から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。
--	---

特定個人情報の消去ルール		[定めている]	＜選択肢＞ 1) 定めている	2) 定めていない
ルール内容及び ルール遵守の確認方法		＜システム運用・保守委託について＞ ・業務委託に関しては、委託契約にて委託業務実施場所を本市事務所に限定している。 ・保有する必要がなくなったときは、確実かつ速やかに廃棄し、又は消去するよう規定している。 ・委託契約の調査報告条項に基づき、必要があると認めるときは調査を行い、または報告を求める。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託契約終了後は予予請求システムに保管していた全ての特定個人情報を国保中央会が消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、本市は消去について国保中央会から報告を受けることができ、それにより消去状況について確認が可能となる。		
	委託契約書中の特定個人情報ファイルの取扱いに関する規定	[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		特定個人情報を含む個人情報のすべてのデータに対して以下のことを契約書上に明記している。 ・委託業務の遂行上知り得た内容を他に漏らし、または他の目的に使用しないこと。契約が終了し、または解除された後においても同様とする。 ・委託業務以外のために仕様書、資料及び成果物に記録されたデータ等を使用しないこと。 ・本市の指示がある場合を除き、契約による事務に関して知ることのできた個人情報を契約の目的以外に利用し、又は本市の承諾なしに第三者に提供しないこと。 ・委託業務の実施上知ることのできた個人情報について、個人情報の漏えい、滅失及びき損の防止その他の個人情報の適正な管理のために必要な措置を講じること。 ・本市から引き渡された個人情報が記録された資料等を本市の承諾なしに複写又は複製しないこと。 ・委託業務が完了したときは、関連資料等を直ちに返還し、又は引き渡すこと。 ・契約に違反する事態が生じ、又は生じる恐れのあることを知ったときは、速やかに本市に報告し、指示に従うこと。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 兵庫県国保連合会及び国保中央会は特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業員の明確化 ・従業員に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項		
	再委託先による特定個人情報ファイルの適切な取扱いの確保	[十分に行っている]	＜選択肢＞ 1) 特に力を入れて行っている 3) 十分に行っていない	2) 十分に行っている 4) 再委託していない
具体的な方法		許可のない再委託は認めていない。許可した場合でも通常の委託と同様の措置を適用している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・再々委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・国保中央会が、再々委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、再々委託の相手方によるセルフチェックを基本とし、必要に応じて国保中央会が訪問確認を行う。 ・点検後に改善事項がある場合は、国保中央会が改善指示及び改善状況のモニタリングを行う。 ・国保中央会は、点検結果について兵庫県国保連合会及び本市に年1回報告を行う。		
	その他の措置の内容	＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業員に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。		

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 3) 課題が残されている	2) 十分である
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	[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	<庁内のデータ連携で提供・移転する場合における措置> ・共通宛名システム等庁内システムとのデータ連携については、システム上で自動化されている。 ・端末機で情報を利用した場合は、操作履歴（ログ）を記録している。		
特定個人情報の提供・移転に関するルール	[定めている]	<選択肢> 1) 定めている	2) 定めていない
ルール内容及びルール遵守の確認方法	<庁内のデータ連携で提供・移転する場合における措置> ・情報の提供・移転を行う場合、利用部署からデータ利用申請を提出させ、データ利用に関し法的根拠等があるかを確認し、承認を得ればデータ利用ができる。		
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 3) 課題が残されている	2) 十分である
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	<庁内のデータ連携で提供・移転する場合における措置> ・データ利用が承認されていない部署への情報の提供・移転はされないことがシステム上で担保される。 ・各システムへのアクセスは、権限のある者のみに限定している。		
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 3) 課題が残されている	2) 十分である
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	<庁内のデータ連携で提供・移転する場合における措置> ・データ利用が承認されていない部署への情報の提供・移転はされないことがシステム上で担保される。		
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 3) 課題が残されている	2) 十分である
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	<団体内統合宛名システムにおける措置> ・番号法の規定に基づき、各業務と統合宛名番号の紐付けを行い、認められる範囲内においてのみ特定個人情報の照会を行う。 <中間サーバー・ソフトウェアにおける措置> ①情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、提供許可証の発行と照会内容の照会許可照会リスト(※2)との照会を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 ②中間サーバーの職員認証・権限管理機能(※3)では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※1) 情報提供ネットワークシステムを使用した特定個人情報の照会及び照会した情報の受領を行う機能。 (※2) 番号法の規定による情報提供ネットワークシステムを使用した特定個人情報の提供に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 (※3) 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である
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	<団体内統合宛名システムにおける措置> ・団体内統合宛名システムは中間サーバーとの間での通信及び特定個人情報の入手のみを実施できるよう設計されているため、安全性が担保されている。 <中間サーバー・ソフトウェアにおける措置> ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 <中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。		
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 3) 課題が残されている	2) 十分である
リスク3: 入手した特定個人情報ที่ไม่正確であるリスク			
リスクに対する措置の内容	<団体内統合宛名システムにおける措置> ・照会対象者の個人番号に基づき、正確に符号の紐付けが行われるため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 <中間サーバー・ソフトウェアにおける措置> ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 3) 課題が残されている	2) 十分である

リスク4: 入手の際に特定個人情報漏えい・紛失するリスク		
リスクに対する措置の内容	＜団体内統合宛名システムにおける措置＞ ・団体内統合宛名システムは、庁内ネットワーク及びLGWANのみに接続されたシステムであるため、操作ミス等による外部への情報の提供漏えいのリスクに対応している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している(※)。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に結果情報を情報照会機能において自動で削除することにより、特定個人情報漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク5: 不正な提供が行われるリスク		
リスクに対する措置の内容	＜団体内統合宛名システムにおける措置＞ ・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に規定された事務以外の事務においては、団体内統合宛名システムに接続することができないため、不正な提供が行われるリスクに対応している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能(※)により、情報提供ネットワークシステムにおける照会許可照合リストを情報提供ネットワークシステムから入手し、中間サーバーにも格納して、情報提供機能により、照会許可照合リストに基づき情報連携が認められた特定個人情報の提供の要求であるかチェックを実施している。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから提供許可証と情報照会者へたどり着くための経路情報を受領し、照会内容に対応した情報を自動で生成して送付することで、特定個人情報不正に提供されるリスクに対応している。 ③機微情報については自動応答を行わないように自動応答不可フラグを設定し、特定個人情報の提供を行う際に、送信内容を改めて確認し、提供を行うことで、センシティブな特定個人情報不正に提供されるリスクに対応している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。 ＜中間サーバーの運用における措置＞ ①情報提供ネットワークシステムを利用する場合は、どの特定個人情報をどの職員がいつどのような目的で提供したのかがすべて記録される。(提供記録は7年分保管する。) ②取得したログは定期的に確認を行う。 ③番号法または条例上認められる提供以外行わないようにする。 ④他機関からの提供が認められなかった場合についても記録を残す。	
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	＜団体内統合宛名システムにおける措置＞ ・団体内統合宛名システムは中間サーバーとの間での通信及び特定個人情報の提供のみを実施するよう設計されているため、不適切な方法で提供されるリスクに対応している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能(※)により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※)暗号化・復号機能と、鍵情報及び照会許可照合リストを管理する機能。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク7： 誤った情報を提供してしまうリスク、誤った相手に提供してしまうリスク		
リスクに対する措置の内容	＜団体内統合宛名システムの運用における措置＞ ・中間サーバーへの連携は適切な頻度で更新し、その正確性を担保することでリスクに対応する。 ・また、団体内統合宛名システムは中間サーバーとの間での通信及び個人情報の提供のみを実施するよう設計されているため、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。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 (※)特定個人情報を副本として保存・管理する機能。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		
＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォーム事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。		

7. 特定個人情報の保管・消去		
リスク1: 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1) 特に力を入れて遵守している 2) 十分に遵守している 3) 十分に遵守していない 4) 政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1) 特に力を入れて整備している 2) 十分に整備している 3) 十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1) 特に力を入れて周知している 2) 十分に周知している 3) 十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
	具体的な対策の内容	<本市における措置> ・電子計算機、データを含んだ記録媒体の盗難を防ぐために、施錠ができる場所等に保管し、セキュリティチェーンを利用して施錠をしている。 ・停電(落雷等)によるデータの消失を防ぐために、電子計算機に無停電電源装置等を付設している。 ・火災によるデータ消失を防ぐために、施設内に消火設備を完備している。 ・厳重に入館・入室管理されたデータセンターにサーバーを設置している。 ・システムのバックアップデータは媒体に格納し、遠隔地に保管している。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては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。 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームは、ISMAPのリストに登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 <予請求システムを活用した情報連携に係る予防接種事務における追加措置> 予請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、ISMAPのリストに登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスの利用

⑥技術的対策	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
具体的な対策の内容	<本市における措置> ・ネットワークを通じて悪意の第三者が侵入しないよう、ファイアウォールを設置している。 ・コンピュータウイルス対策ソフトウェアを導入している。 ・OSには随時パッチ適用を実施している。 <ガバメントクラウドにおける措置> ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年8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及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報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。 <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは、ISMAPのリストに登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 ・本市の端末と予予請求システムとの通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> 予予請求システムは、特定個人情報の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、ISMAPのリスト登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・予予請求システムは論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、予予請求システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予予請求システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。
⑦バックアップ	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない
⑧事故発生時手順の策定・周知	[十分にやっている] <選択肢> 1) 特に力を入れてやっている 2) 十分にやっている 3) 十分にやっていない

⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
	その内容	—	
	再発防止策の内容	—	
⑩死者の個人番号		[保管している]	<選択肢> 1) 保管している 2) 保管していない
	具体的な保管方法	死者の個人番号も現存者の個人番号と同様に管理している。	
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: 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		<団体内統合宛名システム、共通基盤システムにおける措置> ・住登者については、住民基本台帳法第14条第1項(住民基本台帳の正確な記録を確保するための措置)の規定に基づき調査等を実施する住民基本台帳と連携することから、正確な情報であることが担保されている。 <健康かるてV8における措置> ・住基システムより、随時住登者を連携することにより、正確な情報を管理する。 ・住登外者については、住登者と同様に正確な記録を確保できるよう業務所管課で住民基本台帳ネットワークシステムの情報を確認するなど、正確な情報を管理する。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本特定個人情報ファイルの個人情報は、住基及び住登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	<電子媒体における措置> ・健康かるてV8の運用期間中においては、原則消去は行わない。 ・健康かるてV8や関連機器の入替時においては、新規の電子記録媒体にデータを移行後、電子記録媒体を裁断等の物理的破壊により記録内容が判読することができないよう完全に消去する。 <紙媒体における措置> ・予診票等の紙媒体によるものについては、明石市文書管理規程に基づき保管し、予防接種法において定められている期間(予防接種法施行令第4条)経過後、焼却・溶解により破棄する。 <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・消去が必要となった情報は内部手続を経て消去し、その記録を残す。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。	
その他の措置の内容		—	
リスクへの対策は十分か		[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置			
—			

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> ・年に1回担当部署内において、評価書の記載内容通りの運用がなされていることについて、自己点検を行い、運用状況を確認する。 <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、定期的に自己点検を実施することとしている。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、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> ・「明石市情報セキュリティ基本方針」及び「明石市特定個人情報等取扱基準」に基づき、年に1回、複数の所管課を対象として監査を行っている。 <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。 <中間サーバー・プラットフォームにおける措置> ①運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ②ISMAPのリストに登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、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> ・番号利用事務職員に対し、番号法に基づく、特定個人情報保護に関する研修を年1回実施している。 ・全ての職員に対し、個人情報保護に関する研修を行っている。 ・委託業者に対しては、契約内容に個人情報保護に関する教育の実施を義務付け、業務契約において、個人情報保護の規定を設けている。 ・違反行為を行った者に対しては、都度指導の上、違反行為の程度によっては懲戒の対象となりうる。 <予防接種事務における措置> ・新たに配属された職員（非常勤職員、臨時職員等を含む。）に対しては、任用時及び随時、必要な知識の習得のため研修を実施するとともに、研修資料を保存する。 ・予防接種事務関係職員に対し、随時研修・指導を行い、職員のセキュリティ意識の向上及びセキュリティ対策の重要性の周知徹底を図る。 <中間サーバー・プラットフォームにおける措置> ①IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資料を作成し、中間サーバー・プラットフォームの運用に携わる職員及び事業者に対し、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、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

＜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また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。

＜中間サーバー・プラットフォームにおける措置＞

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

＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞

- ・本市は、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	明石市政策局市民相談室行政情報センター 〒673-8686 明石市中崎1丁目5番1号 TEL078-918-5003
②請求方法	個人情報の保護に関する法律(平成15年法律第57号)第77条に基づき、必要事項を記載した開示請求書を提出する。
特記事項	—
③手数料等	[無 料] ＜選択肢＞ 1) 有料 2) 無料 (手数料額、納付方法: 手数料は無料。写しの交付を希望する場合は、別途コピー代が必要。)
④個人情報ファイル簿の公表	[行っていない] ＜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	—
公表場所	—
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	明石市福祉局あかし保健所保健予防課 〒674-0068 明石市大久保町ゆりのき通1丁目4番地の7 TEL078-918-5668 明石市こども局子育て支援室こども健康課 〒673-0891 明石市大明石町1丁目6番1号 TEL078-918-5656
②対応方法	問い合わせの受付時に受付票を起票し、対応について記録を残す。

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和8年8月1日
②しきい値判断結果	[基礎項目評価及び全項目評価の実施が義務付けられる] <選択肢> 1) 基礎項目評価及び全項目評価の実施が義務付けられる 2) 基礎項目評価及び重点項目評価の実施が義務付けられる(任意に全項目評価を実施) 3) 基礎項目評価の実施が義務付けられる(任意に全項目評価を実施) 4) 特定個人情報保護評価の実施が義務付けられない(任意に全項目評価を実施)
2. 国民・住民等からの意見の聴取	
①方法	市民意見の提出手続きを定める要綱に基づき、パブリック・コメントによる意見聴取を実施する。パブリック・コメントの実施に際しては、市報「広報あかし」に記事を掲載するとともに、保健予防課、こども健康課、行政情報センター、各市民センター及び市ホームページにて全文を閲覧できるようにする。
②実施日・期間	令和8年9月1日から10月1日までの31日間
③期間を短縮する特段の理由	—
④主な意見の内容	
⑤評価書への反映	
3. 第三者点検	
①実施日	
②方法	明石市個人情報保護審議会に諮る。
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8月18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7 ②システムの機能	①ワクチン接種記録システム(VRS)への接種対象者・接種券発行登録機能 ②接種記録の管理機能 ③転出/死亡時等のフラグ設定機能 ④他市区町村への接種記録の照会・提供機能 ⑤新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会機能	①ワクチン接種記録システム(VRS)への接種対象者・接種券発行登録機能 ②接種記録の管理機能 ③転出/死亡時等のフラグ設定機能 ④他市区町村への接種記録の照会・提供機能 ⑤新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会機能 ⑥新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施 ⑦新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	I 基本情報 5. 個人番号の利用 法令上の根拠	※前略 ＜新型コロナウイルスのみに係る内容＞ 番号法第19条第15号(ワクチン接種記録システム(VRS)を用いた情報提供・照会のみ) 番号法第19条第5号(ワクチン接種記録システム(VRS)内のデータを管理する委託事業者への提供)	※前略 ＜新型コロナウイルスのみに係る内容＞ 番号法第19条第16号(ワクチン接種記録システム(VRS)を用いた情報提供・照会のみ) 番号法第19条第6号(ワクチン接種記録システム(VRS)内のデータを管理する委託事業者への提供)	事後	
令和4年8月18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 ②法令上の根拠	＜情報提供の根拠＞ 番号法第19条第8号及び別表第二の16の2、16の3、115の2の項 番号法別表第二の主務省令で定める事務を定める命令(平成26年内閣府・総務省例第7号)第12条の2、第12条の2の2、第59条の2 ＜情報照会の根拠＞ 番号法第19条第8号及び別表第二の16の2、17、18、19、115の2の項 番号法別表第二の主務省令で定める事務を定める命令第12条の2、第12条の3、第13条、第13条の2、第59条の2 (新型コロナウイルスに関する情報については、令和4年6月開始)	＜情報提供の根拠＞ 番号法第19条第8号及び別表第二の16の2、16の3、115の2の項 番号法別表第二の主務省令で定める事務を定める命令(平成26年内閣府・総務省例第7号)第12条の2、第12条の2の2、第59条の2 ＜情報照会の根拠＞ 番号法第19条第8号及び別表第二の16の2、17、18、19、115の2の項 番号法別表第二の主務省令で定める事務を定める命令第12条の2、第12条の3、第13条、第13条の2、第59条の2	事後	
令和4年8月18日	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	〔O〕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 〔O〕庁内連携システム 〔O〕情報提供ネットワークシステム 〔O〕その他(ワクチン接種記録システム(VRS))	〔O〕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 〔O〕庁内連携システム 〔O〕情報提供ネットワークシステム 〔O〕その他(ワクチン接種記録システム(VRS))(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム)	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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	※前略 ＜新型コロナウイルスのみに係る内容＞ ・転入時に転入前市区町村への接種記録の照会が必要になる都度(転入者本人から個人番号の提供の同意が得られた場合のみ) ・転出先市区町村から接種記録の照会を受ける都度 ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合であって接種記録の照会が必要になる都度	※前略 ＜新型コロナウイルスのみに係る内容＞ ・転入時に転入前市区町村への接種記録の照会が必要になる都度 ・他市区町村から接種記録の照会を受ける都度 ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合であって接種記録の照会が必要になる都度	事後	
令和4年8月18日	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入手にかかる妥当性	※前略 ＜新型コロナウイルスのみに係る内容＞ ・本市への転入者について、転入前市区町村へ接種記録を照会するために、転入者本人から個人番号の提供の同意が得られた場合のみ入手する。(番号法第19条第15号) ・本市からの転出者について、転出先市区町村での接種記録を提供するために、転出先市区町村から個人番号を入手する。(番号法第19条第15号) ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合のみ入手する。	※前略 ＜新型コロナウイルスのみに係る内容＞ ・本市への転入者について、転入前市区町村へ接種記録を照会し、提供を受ける場合のみ入手する。(番号法第19条第16号) ・本市からの転出者について、転出先市区町村での接種記録を提供するために、他市区町村から個人番号を入手する。(番号法第19条第16号) ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合のみ入手する。	事後	
令和4年8月18日	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	※前略 ＜新型コロナウイルスのみに係る内容＞ ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。	※前略 ＜新型コロナウイルスのみに係る内容＞ ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する ・電子交付アプリにより予防接種証明書の電子申請を受付け場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受け付ける場合においては、利用規約を表示し、同意を得てから入手する。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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	※前略 ＜新型コロナウイルスのみに係る内容＞ ④本市への転入者について、転入前市区町村へ接種記録を照会するために特定個人情報を使用する。 ⑤本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。 ⑥新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を使用する。	※前略 ＜新型コロナウイルスのみに係る内容＞ ④本市への転入者について、転入前市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 ⑤本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。 ⑥新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を使用する。	事後	

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8月18日	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 情報の突合	※前略 ＜新型コロナウイルスワクチンのみに係る内容＞ ・本市からの転出者について、本市での接種記録を転出先市区町村に提供するために、転出先市区町村から個人番号を入手し、本市の接種記録と突合する。（転出先市区町村にて、本人から個人番号の提供に関して同意が得られた場合のみ当処理を行う。）（使用方法⑤に該当）	※前略 ＜新型コロナウイルスワクチンのみに係る内容＞ ・本市からの転出者について、本市での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、本市の接種記録と突合する。（使用方法⑤に該当）	事後	
令和4年8月18日	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	[委託する] 4件	[委託する] 5件	事後	システム更新に伴う重要な変更
令和4年8月18日	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4	新設	明石市共通管理系システム構築・運用業務委託	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ①委託内容	新設	共通基盤システム及び共通管理系システムの保守・運用業務	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ②取扱いを委託する特定個人情報ファイルの範囲	新設	特定個人情報ファイルの全体	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数	新設	10万人以上100万人未満	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲	新設	予防接種券の発行履歴がある者及び予防接種歴のある者	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 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	新設	システムの運用保守・改修等の作業対象がファイル全体に及ぶため、上記範囲を委託する必要がある。	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ③委託先における取扱者数	新設	10人以上50人未満	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ④委託先への特定個人情報ファイルの提供方法	新設	[○]その他(本市事務室等において、専用回線上の端末を用いて閲覧)	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ⑤委託先名の確認方法	新設	明石市情報公開条例に基づく開示請求を行うことで確認ができる。	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ⑥委託先名	新設	富士通グループ明石市共通管理系システム構築・運用業務共同事業体	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ⑦再委託先の有無	新設	再委託する	事後	システム更新に伴う重要な変更

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8月18日	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4 ⑧再委託の許諾方法	新設	・委託先から再委託承諾申請書の提出があり、本市が再委託承諾書により承諾した場合に限る。 ・再委託先から従業者名簿及び再委託先の従業者から個人情報の取扱いに関する誓約書を提出させる。	事後	システム更新に伴う重要な変更
令和4年8月18日	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4 ⑨再委託事項	新設	共通基盤システム等の保守・運用業務における作業担当として、技術支援作業を行う。	事後	システム更新に伴う重要な変更
令和4年8月18日	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5	新設	委託事項4の記載を委託事項5に転記 ②取扱いを委託する特定個人情報ファイルの範囲 ③委託先における取扱者数 ⑤委託先名の確認方法 ⑥委託先名 ⑦再委託の有無 については、修正箇所については、下記のとおり	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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5 ①委託内容	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの管理等	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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5 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	ワクチン接種記録システム（VRS）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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5 ④委託先への特定個人情報ファイルの提供方法	LGWAN回線を用いた提供	LGWAN回線を用いた提供（VRS本体、コンビニ交付関連機能）、本人からの電子交付アプリを用いた提供（新型コロナウイルス感染症予防接種証明書電子交付機能）	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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	※前略 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得している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。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。 ※後略	※前略 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得している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。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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	※前略 ＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・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、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊または専用ソフト等を利用して完全に消去し、消去した記録を保存する。 ※後略	※前略 ＜中間サーバー・プラットフォームにおける措置＞ ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・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、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去し、消去した記録を保存する。 ※後略	事後	

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8月18日	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: 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	※前略 ＜新型コロナワクチンのみに係る措置＞ ①転入者本人からの個人番号の入手 本市への転入者について、転入前市区町村へ接種記録を照会するために、個人番号を入力する際は、接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ②転出先市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町村へ提供するため、転出先市区町村から個人番号を入力するが、その際は、転出先市区町村において、本人同意及び本人確認が行われた情報だけをワクチン接種記録システム(VRS)を通じて入手する。 ③新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入力するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。	※前略 ＜新型コロナワクチンのみに係る措置＞ ①転入者本人からの個人番号の入手 本市への転入者について、転入前市区町村へ接種記録を照会するために、本人から個人番号を入力する場合は、接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ②他市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町村へ提供するため、他市区町村から個人番号を入力するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム(VRS)を通じて入手する。 ③転出元市区町村からの接種記録の入手 本市への転入者について、転出元市区町村から接種記録を入力するが、その際は、本市において住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム(VRS)を通じて入手する。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日			④新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入力するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 交付申請には、個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。		
令和4年8月18日	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: 目的外の入手が行われるリスク 必要な情報以外を入力することを防止するための措置の内容	保健情報管理システムTIARAの画面および帳票には、個人番号は表示しない仕組みとし、不用意な閲覧が行われないようにする。	保健情報管理システムTIARAの画面および帳票には、個人番号は表示しない仕組みとし、不用意な閲覧が行われないようにする。 ＜ワクチン接種記録システム(VRS)における追加措置＞ (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 個人番号カードや旅券の読み取りにより必要な情報を入力し、申請者の自由入力を避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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: 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	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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アクセス制御している。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じることで、意図しない不適切な方法で特定個人情報送信されることを避ける。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報送信されることを避ける。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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: 入手した特定個人情報が入手の際の本人確認の措置の内容	接種券等の申請の際には、身分証明書等の提示により本人確認を行い、身分証明書等の提示がない場合は、2点以上の本人確認書類の提示により、本人確認を行う。代理人による申請の場合、代理人自身について身分証明書等による本人確認を行うとともに、住民票上世帯外の者については、代理権者であることを示す委任状等の提出を必要とする。	接種券等の申請の際には、身分証明書等の提示により本人確認を行い、身分証明書等の提示がない場合は、2点以上の本人確認書類の提示により、本人確認を行う。代理人による申請の場合、代理人自身について身分証明書等による本人確認を行うとともに、住民票上世帯外の者については、代理権者であることを示す委任状等の提出を必要とする。 ＜ワクチン接種記録システム(VRS)における追加措置＞ (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証で本人確認を行うため、本人からの情報のみが送信される。	事後	コンビニ交付に係る部分のみ「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4年8月18日	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: 入手した特定個人情報 that 不正確であるリスク 特定個人情報の正確性確保の措置の内容	特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、入力等を行った者以外の者が確認する等、複数人により行うこととしている。	特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、入力等を行った者以外の者が確認する等、複数人により行うこととしている。 ＜ワクチン接種記録システム(VRS)における追加措置＞ (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報(4情報・マイナンバー)に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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: 入手の際に特定個人情報 that 漏えい・紛失するリスク リスクに対する措置の内容	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリとVRS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。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはL2WAN回線を使用し、情報漏えいを防止する。また、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。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。	事後	コンビニ交付に係る部分のみ「事前」
令和4年8月18日	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 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	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ ① 特定個人情報を使用する場面を必要最小限に限定している。具体的には以下の3つの場面に限定している。 ・本市への転入者について、転入前市区町村へ接種記録を照会するために、転入者本人から個人番号の提供の同意が得られた場合のみ入手し、使用する。 ・本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 ② ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ ① 特定個人情報を使用する場面を必要最小限に限定している。具体的には以下の3つの場面に限定している。 ・本市への転入者について、転入前市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 ② ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	事後	
令和4年8月18日	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	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項(規約)」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・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 ・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 ・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	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項(規約)」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・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 ・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 ・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 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置	事後	コンビニ交付に係る部分のみ「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4年8月18日	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 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。） 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	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ ・本市への転入者について、転入前市区町村から接種記録を入手するため、転入前市区町村へ個人番号を提供するが、その際は、本人同意及び本人確認が行われた情報だけをワクチン接種記録システム（VRS）を用いて提供する。	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ ・本市への転入者について、転入前市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム（VRS）を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、転出元市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム（VRS）を用いて提供する。	事後	
令和4年8月18日	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 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。） 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	※前略 ＜ワクチン接種記録システム（VRS）における追加措置＞ ・本市への転入者について、転入前市区町村から接種記録を入手するため、転入前市区町村へ個人番号を提供するが、その際は、個人番号と共に転入前の市区町村コードを送信する。そのため、仮に誤った市区町村コードを個人番号と共に送付したとしても、電文を受ける市区町村では、該当者がいないため、誤った市区町村に対して個人番号が提供されない仕組みとなっている。	※前略 ＜ワクチン接種記録システム（VRS）における追加措置＞ ・本市への転入者について、転入前市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録は提供されない仕組みとなっている。	事後	
令和4年8月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 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	※前略 ＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ※後略	※前略 ＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ※後略	事後	
令和4年8月18日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク3：入手した特定個人情報が入り込むリスク リスクに対する措置の内容	※前略 ＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。	※前略 ＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、特定個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。	事後	
令和4年8月18日	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：特定個人情報の漏えい・滅失・毀損リスク ⑥ 技術的対策 具体的な対策の内容	※前略 ＜ワクチン接種記録システム（VRS）における措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切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本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。	※前略 ＜ワクチン接種記録システム（VRS）における措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切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本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。	事前	コンビニ交付に係る部分のみ「事前」
令和4年8月18日		・LGWAN端末とワクチン接種記録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。	・LGWAN端末とワクチン接種記録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。 （新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRS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。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、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。		

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8月18日	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	※前略 ＜新型コロナワクチンのみに係る措置＞ 内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	※前略 ＜新型コロナワクチンのみに係る措置＞ デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	事後	
令和4年8月18日	IVその他のリスク対策 1. 監査 ②監査 具体的なチェック方法	※前略 ＜新型コロナワクチンのみに係る措置＞ 内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	※前略 ＜新型コロナワクチンのみに係る措置＞ デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	事後	
令和4年8月18日	IVその他のリスク対策 2. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	※前略 ＜新型コロナワクチンのみに係る措置＞ 内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な指導をする。	※前略 ＜新型コロナワクチンのみに係る措置＞ デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な指導をする。	事後	
令和4年8月18日	IVその他のリスク対策 3. その他のリスク対策	※前略 ＜新型コロナワクチンのみに係る措置＞ 内閣官房情報通信技術(IT)総合戦略室から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、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。	※前略 ＜新型コロナワクチンのみに係る措置＞ デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、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。	事後	
令和4年8月18日	VI評価実施手続 1. 基礎項目評価 ①実施日	令和3年8月11日	令和4年5月24日	事後	
令和4年8月18日	VI評価実施手続 2. 国民・住民等からの意見の聴取 ①方法	市民意見の提出手続きを定める要綱に基づき、パブリック・コメントによる意見聴取を実施する。パブリック・コメントの実施に際しては、市報「広報あかし」に記事を掲載するとともに、保健予防課、こども健康課、各市民センター、行政情報センター及び市ホームページにて全文を閲覧できるようにする。	市民意見の提出手続きを定める要綱に基づき、パブリック・コメントによる意見聴取を実施する。パブリック・コメントの実施に際しては、市報「広報あかし」に記事を掲載するとともに、保健予防課、行政情報センター、あかし総合窓口、各市民センター・サービスコーナー及び市ホームページにて全文を閲覧できるようにする。	事後	
令和4年8月18日	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	令和3年9月1日から10月1日までの31日間	令和4年6月1日から6月30日までの30日間	事後	
令和4年8月18日	VI評価実施手続 2. 国民・住民等からの意見の聴取 ④主な意見の内容	1 業務委託に関すること ・委託先の確認方法や業務委託内容についての記載が不十分なのではないか。 ・再委託の承諾にあたって承諾書の交付があるなら、その旨追記してはどうか。 ・情報保護管理体制について、委託契約時・契約後においても確認する必要があるのではないかと。 ・再委託先への個人情報保護について、契約書に記載があるなら、その旨追記してはどうか。 2 特定個人情報の使用のリスクに関すること ・ユーザー認証の管理におけるパスワード変更について、その頻度やシステム設定等を追記してはどうか。 ・権限については、発行管理、失効管理に分けた方が分かりやすい。また、アクセス権限の見直し等を行っているのなら、その旨追記してはどうか。 3 監査に関すること ・実施部署や頻度について記載するのが望ましい。 ・再委託先を含む外部委託業者への監査も検討する必要があるのではないかと。	なし	事後	
令和4年8月18日	VI評価実施手続 2. 国民・住民等からの意見の聴取 ⑤評価書への反映	・業務委託について追記した。 ・不十分な部分、分かりにくい表現であった部分について修正した。 ・意見を参考にした上で、すでに記載している部分等については、修正した部分を除いて原案のままとする。	なし	事後	
令和4年8月18日	VI評価実施手続 3. 第三者点検 ①実施日	令和3年11月1日	令和4年7月8日	事後	
令和5年6月16日	I 基本情報 7. 評価実施機関における担当部署 ①部署	感染対策局あかし保健所保健予防課 / こども局子育て支援室こども健康課 / 感染対策局コロナワクチン対策室	福祉局あかし保健所保健予防課 / こども局子育て支援室こども健康課	事後	重要な変更にあたらないため。(組織改正による修正)

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5年6月16日	I 基本情報 7. 評価実施機関における担当部署 ②所属長の役職名	課長 / 課長 / 担当課長	課長 / 課長	事後	重要な変更にあたらなため。(組織改正による修正)
令和5年6月16日	II 特定個人情報ファイルの概要 2. 基本情報 ⑥事務担当部署	感染対策局あかし保健所保健予防課 / ことも局子育て支援室ことも健康課 / 感染対策局コロナワクチン対策室	福祉局あかし保健所保健予防課 / ことも局子育て支援室ことも健康課	事後	重要な変更にあたらなため。(組織改正による修正)
令和5年6月16日	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 ⑦使用の主体 使用部署	感染対策局あかし保健所保健予防課 / ことも局子育て支援室ことも健康課 / 感染対策局コロナワクチン対策室	福祉局あかし保健所保健予防課 / ことも局子育て支援室ことも健康課	事後	重要な変更にあたらなため。(組織改正による修正)
令和5年6月16日	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3 ⑥委託先名	株式会社ワンビシアークイブズ	株式会社NXワンビシアークイブズ	事後	
令和5年6月16日	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: 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 具体的な管理方法	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞権限のない者によって不正に使用されないよう、以下の対策を講じている。 ・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LGWAN端末による操作に限り可能になるように制御している。 ・LGWAN端末は、限定された者しかログインできる権限を保持しない。 ・ワクチン接種記録システム(VRS)におけるログイン認証は、ユーザID・パスワードにて行う。 ・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国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。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞権限のない者によって不正に使用されないよう、以下の対策を講じている。 ・ワクチン接種記録システム(VRS)における特定個人情報へのアクセスは、LGWAN端末による操作に限り可能になるように制御している。 ・LGWAN端末は、限定された者しかログインできる権限を保持しない。 ・ワクチン接種記録システム(VRS)におけるログイン認証は、ユーザID・パスワードにて行う。 ・ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、本市が指定する管理者が認めた者に限定して発行される。	事後	重要な変更にあたらなため。(VRS管理機能の実施に係る修正)
令和5年6月16日	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: 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 アクセス権限の発効・失効の管理 具体的な管理方法	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国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。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ワクチン接種記録システム(VRS)へのログイン用のユーザIDに付与されるアクセス権限は、本市が指定する管理者が必要最小限の権限で発効する。 本市が指定する管理者は、定期的又は異動・退職等のイベントが発生したタイミングで、権限を有していた職員の異動・退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。やむを得ず、複数の職員が共有するID(以下「共用ID」という。)を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動・退職等のイベントが発生したタイミングで確認し、当該事由が生じた際には速やかに把握している内容を更新する。	事後	重要な変更にあたらなため。(VRS管理機能の実施に係る修正)
令和5年6月16日	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: 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 アクセス権限の管理 具体的な管理方法	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、国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。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ワクチン接種記録システム(VRS)へのログイン用のユーザIDは、本市が指定する管理者が必要最小限の権限で発効する。 本市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザIDやアクセス権限を速やかに変更又は削除する。	事後	重要な変更にあたらなため。(VRS管理機能の実施に係る修正)
令和5年6月16日	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: 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 特定個人情報の使用の記録 具体的な管理方法	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞システム上の操作のログを取得しており、操作ログを確認できる。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞システム上の操作のログを取得しており、操作ログを確認できる。ログは定期的に及び必要に応じ随時に確認する。	事後	重要な変更にあたらなため。(VRS管理機能の実施に係る修正)
令和5年6月16日	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 ②請求方法	明石市個人情報保護条例第17条に基づき、必要事項を記載した開示請求書を提出する。	個人情報の保護に関する法律(平成15年法律第57号)第77条に基づき、必要事項を記載した開示請求書を提出する。	事後	
令和5年6月16日	V 開示請求、問合せ 2. 特定個人情報ファイルの取扱いに関する問合せ	明石市感染対策局あかし保健所保健予防課 千674-0068 明石市大久保町ゆりのき通1丁目4番地の7 ℡078-918-5668 明石市ことも局子育て支援室ことも健康課 千673-0891 明石市大明石町1丁目6番1号 ℡078-918-5656 明石市感染対策局コロナワクチン対策室 千674-0068 明石市大久保町ゆりのき通1丁目4番地の7 ℡078-918-5674	明石市福祉局あかし保健所保健予防課 千674-0068 明石市大久保町ゆりのき通1丁目4番地の7 ℡078-918-5668 明石市ことも局子育て支援室ことも健康課 千673-0891 明石市大明石町1丁目6番1号 ℡078-918-5656	事後	重要な変更にあたらなため。(組織改正による修正)

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8月9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7 ②システムの機能	①ワクチン接種記録システム(VRS)への接種対象者・接種券発行登録機能 ②接種記録の管理機能 ③転出/死亡時等のフラグ設定機能 ④他市区町村への接種記録の照会・提供機能 ⑤新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会機能 ⑥新型コロナウイルス感染症予防接種証明書の電子申請受付・電子交付の実施 ⑦新型コロナウイルス感染症予防接種証明書のコンビニ交付の実施	①ワクチン接種記録システム(VRS)への接種対象者・接種券発行登録機能 ②接種記録の管理機能 ③転出/死亡時等のフラグ設定機能 ④他市区町村への接種記録の照会・提供機能 ⑤新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会機能	事後	
令和6年8月9日	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に関する法律(平成25年法律第27号)(以下「番号法」という。)第9条第1項及び別表第一の10、93の2の項 番号法別表第一の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第5号)第10条、第67条の2 ※後略	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に関する法律(平成25年法律第27号)(以下「番号法」という。)第9条第1項及び別表の項番14、126 番号法別表の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第5号)第10条、第67条の2 ※後略	事後	軽微な修正(法改正に伴うもの)
令和6年8月9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 ②法令上の根拠	<情報提供の根拠> 番号法第19条第8号及び別表第二の16の2、16の3、115の2の項 番号法別表第二の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第7号)第12条の2、第12条の2の2、第59条の2 <情報照会の根拠> 番号法第19条第8号及び別表第二の16の2、17、18、19、115の2の項 番号法別表第二の主務省令で定める事務を定める命令第12条の2、第12条の3、第13条、第13条の2、第59条の2	<情報提供の根拠> 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(令和6年デジタル庁・総務省令第9号)第2条項番25、26、153 <情報照会の根拠> 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条項番25、27、28、29、153	事後	軽微な修正(法改正に伴うもの)
令和6年8月9日	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	[○]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(ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能を含む。)、コンビニエンスストア等のキオスク端末及び証明書交付センターシステム)	[○]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(ワクチン接種記録システム(VRS))	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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	※前略 <新型コロナワクチンのみに係る内容> ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する ・電子交付アプリにより予防接種証明書の電子申請を受け付ける場合及びコンビニエンスストア等のキオスク端末から予防接種証明書の申請を受け付ける場合においては、利用規約を表示し、同意を得てから入手する。	※前略 <新型コロナワクチンのみに係る内容> ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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5 ①委託内容	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの管理等	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理等	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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5 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	ワクチン接種記録システム(VRS)(新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	ワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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5 ④委託先への特定個人情報ファイルの提供方法	※前略 [○]その他(LGWAN回線を用いた提供(VRS本体、コンビニ交付関連機能)、本人からの電子交付アプリを用いた提供(新型コロナウイルス感染症予防接種証明書電子交付機能))	※前略 [○]その他(LGWAN回線を用いた提供)	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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 ①法令上の根拠	番号法第19条第8号及び別表第二の16の2、16の3の項	番号法第19条第8号及び番号法第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条項番25、26	事後	軽微な修正(法改正に伴うもの)
令和6年8月9日	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 ①法令上の根拠	番号法第19条第8号及び別表第二の115の2の項	番号法第19条第8号及び番号法第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条項番153	事後	軽微な修正(法改正に伴うもの)
令和6年8月9日	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	市区町村コード及び転入者の個人番号(本人からの同意が得られた場合のみ)	市区町村コード及び転入者の個人番号	事後	

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8月9日	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	※前略 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリ及び同アプリの利用端末には、申請情報を記録しないこととしている。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。	※前略 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	Ⅲ 特定個人情報ファイルの取扱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: 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	※前略 ＜新型コロナワクチンのみに係る措置＞ ① 転入者本人からの個人番号の入手 本市への転入者について、転入前市区町村へ接種記録を照会するために、個人番号を入力する際は、接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ② 転出先市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町村へ提供するため、転出先市区町村から個人番号を入力するが、その際は、転出先市区町村において、本人同意及び本人確認が行われた情報だけをワクチン接種記録システム（VRS）を通じて入手する。 ③ 新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入力するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。	※前略 ＜新型コロナワクチンのみに係る措置＞ ① 転入者本人からの個人番号の入手 本市への転入者について、転入前市区町村へ接種記録を照会するために、本人から個人番号を入力する場合は、接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ② 他市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、他市区町村から個人番号を入力するが、その際は、他市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム（VRS）を通じて入手する。 ③ 転出元市区町村からの接種記録の入手 本市への転入者について、転出元市区町村から接種記録を入手するが、その際は、本市において住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム（VRS）を通じて入手する。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日		④ 新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入力するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 交付申請には、個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。	④ 新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入力するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。		
令和6年8月9日	Ⅲ 特定個人情報ファイルの取扱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: 目的外の入手が行われるリスク 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	保健情報管理システムTIARAの画面および帳票には、個人番号は表示しない仕組みとし、不意な閲覧が行われないようにする。 ＜ワクチン接種記録システム（VRS）における追加措置＞ (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 個人番号カードや旅券の読み取りにより必要な情報を入手し、申請者の自由入力避けることで、交付申請者が不要な情報を送信してしまうリスクを防止する。	保健情報管理システムTIARAの画面および帳票には、個人番号は表示しない仕組みとし、不意な閲覧が行われないようにする。	事後	電子交付及びコンビニ交付終了に伴う修正

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8月9日	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: 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	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 当該機能では、専用アプリからのみ交付申請を可能とする。アプリの改ざん防止措置を講じること、意図しない不適切な方法で特定個人情報送信されることを避ける。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) 証明書交付センターにおいてキオスク端末の操作画面を制御し、コンビニ交付に対応する市町村に対してのみキオスク端末から交付申請を可能とすることで、意図しない不適切な方法で特定個人情報が送信されることを避ける。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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: 入手した特定個人情報が入力の本人確認の措置の内容	接種券等の申請の際には、身分証明書等の提示により本人確認を行い、身分証明書等の提示がない場合は、2点以上の本人確認書類の提示により、本人確認を行う。代理人による申請の場合、代理人自身について身分証明書等による本人確認を行うとともに、住民票上世帯外の者については、代理権者であることを示す委任状等の提出を必要とする。 ＜ワクチン接種記録システム(VRS)における追加措置＞ (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証で本人確認を行うため、本人からの情報のみが送信される。	接種券等の申請の際には、身分証明書等の提示により本人確認を行い、身分証明書等の提示がない場合は、2点以上の本人確認書類の提示により、本人確認を行う。代理人による申請の場合、代理人自身について身分証明書等による本人確認を行うとともに、住民票上世帯外の者については、代理権者であることを示す委任状等の提出を必要とする。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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: 入手した特定個人情報が入力の本人確認の措置の内容	特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、入力等を行った者以外の者が確認する等、複数人により行うこととしている。 ＜ワクチン接種記録システム(VRS)における追加措置＞ (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) ・券面入力補助APを活用し、個人番号カード内の記憶領域に格納された個人番号を申請情報として自動的に入力することにより、不正確な個人番号の入力を抑止する措置を講じている。 ・券面事項入力補助APから取得する情報(4情報・マイナンバー)に付されている署名について、VRS又は証明書交付センターシステムにおいて真正性の検証を行い、送信情報の真正性を確認する措置を講じている。	特定個人情報の入力、削除及び訂正を行う際は、整合性を確保するために、入力等を行った者以外の者が確認する等、複数人により行うこととしている。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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: 入手の際に特定個人情報が入力の紛失するリスク リスクに対する措置の内容	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。 (新型コロナウイルス感染症予防接種証明書電子交付機能) 電子交付アプリとVRS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。 (新型コロナウイルス感染症予防接種証明書コンビニ交付) キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。また、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。さらに、キオスク端末の画面表示や音声案内により、マイナンバーカード及び証明書の取り忘れ防止対策を実施する。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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: 入手の際に特定個人情報が入力の紛失するリスク 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。) その他のリスク及びそのリスクに対する措置	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手した特定個人情報については、限定された端末を利用して国から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	※前略 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手した特定個人情報については、限定された端末を利用して本市が指定する管理者から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	事後	

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8月9日	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	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム（VRS）（新型コロナウイルス感染症予防接種証明書電子交付機能及びコンビニ交付関連機能を含む。）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・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 ・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 ・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 ・新型コロナウイルス感染症予防接種証明書電子交付機能において、申請者本人から特定個人情報の提供を受ける際の入手に係る保護措置	※前略 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項（規約）」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム（VRS）に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・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 ・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 ・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	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日	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 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。） 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 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	＜ワクチン接種記録システム（VRS）における追加措置＞ ・特定個人情報の提供は、限定された端末（LGWAN端末）だけができるように制御している。 ・特定個人情報を提供する場面に必要最低限にしている。具体的には本市への転入者について、転入前市区町村での接種記録を入手するために、転入前市区町村への個人番号と共に転入前市区町村コードを提供する場面に限定している。	＜ワクチン接種記録システム（VRS）における追加措置＞ ・特定個人情報の提供は、限定された端末（LGWAN端末）だけができるように制御している。 ・特定個人情報を提供する場面に必要最低限にしている。具体的には本市への転入者について、転入前市区町村での接種記録を入手するために、他市区町村へ個人番号を提供する場面に限定している。	事後	
令和6年8月9日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク5 不正な提供が行われるリスク	＜団体内統合宛名システムにおける措置＞ ・番号法別表第二に規定された事務以外の事務においては、団体内統合宛名システムに接続することができないため、不正な提供が行われるリスクに対応している。 ※後略	＜団体内統合宛名システムにおける措置＞ ・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に規定された事務以外の事務においては、団体内統合宛名システムに接続することができないため、不正な提供が行われるリスクに対応している。 ※後略	事後	軽微な修正（法改正に伴うもの）
令和6年8月9日	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：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	※前略 ＜ワクチン接種記録システム（VRS）における措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切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本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。 ・LGWAN端末とワクチン接種記録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。 （新型コロナウイルス感染症予防接種証明書電子交付機能） ・電子交付アプリには、申請情報を記録しないこととしている。 ・電子交付アプリとVRS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。 （新型コロナウイルス感染症予防接種証明書コンビニ交付） ・証明書交付センターシステム及びキオスク端末には、申請情報・証明書データを記録しないこととしている。 ・キオスク端末と証明書交付センターシステム間の通信については専用回線、証明書交付センターシステムとVRS間の通信についてはLGWAN回線を使用し、情報漏えいを防止する。 また、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。	※前略 ＜ワクチン接種記録システム（VRS）における措置＞ ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切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本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。 ・LGWAN端末とワクチン接種記録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。	事後	電子交付及びコンビニ交付終了に伴う修正
令和6年8月9日		・LGWAN端末とワクチン接種記録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。	・LGWAN端末とワクチン接種記録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。		

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9月26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	予防接種法(昭和23年6月30日法律第68号)及び新型コロナウイルス等対策特別措置法(平成24年5月11日法律第31号)に基づき、市内に居住する者に対し予防接種を実施するとともに、接種歴等の情報管理・報告や給付の支給に対する事務等を行う。特定個人情報ファイルを取り扱う事務については、接種歴等の照会等に関する事務のみである。 <新型コロナワクチンのみに係る内容> ワクチン接種記録システム(VRS)へ予防接種対象者及び発行した接種券を登録し、予防接種の実施後に接種記録等を登録・管理、他市区町村へ接種記録の照会・提供を行う。また、予防接種の実施後に、接種者からの申請に基づき、新型コロナウイルス感染症予防接種証明書の交付を行う。	予防接種法(昭和23年6月30日法律第68号)及び新型コロナウイルス等対策特別措置法(平成24年5月11日法律第31号)に基づき、市内に居住する者に対し予防接種を実施するとともに、接種歴等の情報管理・報告や給付の支給に対する事務等を行う。特定個人情報ファイルを取り扱う事務については、接種歴等の照会等に関する事務のみである。 (別添1)事務の内容のVRSIに関する記載削除	事前	VRSの機能停止に伴う修正
令和6年9月26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7 ①システムの名称	ワクチン接種記録システム(VRS)	削除	事前	VRSの機能停止に伴う修正
令和6年9月26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7 ②システムの機能	①ワクチン接種記録システム(VRS)への接種対象者・接種券発行登録機能 ②接種記録の管理機能 ③転出/死亡時等のフラグ設定機能 ④他市区町村への接種記録の照会・提供機能 ⑤新型コロナウイルス感染症予防接種証明書の交付に係る接種記録の照会機能	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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に関する法律(平成25年法律第27号)(以下「番号法」という。)第9条第1項及び別表の項番14、126 番号法別表の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第5号)第10条、第67条の2 <新型コロナワクチンのみに係る内容> 番号法第19条第16号(ワクチン接種記録システム(VRS)を用いた情報提供・照会のみ) 番号法第19条第6号(ワクチン接種記録システム(VRS)内のデータを管理する委託事業者への提供)	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に関する法律(平成25年法律第27号)(以下「番号法」という。)第9条第1項及び別表の項番14、126 番号法別表の主務省令で定める事務を定める命令(平成26年内閣府・総務省令第5号)第10条、第67条の2	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	【○】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(ワクチン接種記録システム(VRS))	【○】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()	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	・本人や医療機関から予防接種実施の報告がある都度 ・本人から予防接種費用の実費に係る免除申請がある都度 <新型コロナワクチンのみに係る内容> ・転入時に転入前市区町村への接種記録の照会が必要になる都度 ・他市区町村から接種記録の照会を受ける都度 ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合であって接種記録の照会が必要になる都度	・本人や医療機関から予防接種実施の報告がある都度 ・本人から予防接種費用の実費に係る免除申請がある都度	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	・共通基盤システムより入手する住民情報・住民登録外情報は、接種対象者であることの確認を行うため入手する。 ・共通基盤システム(もしくは情報提供ネットワークを利用して他市区町村)より入手する世帯情報及び地方税関係情報については、本人から実費免除の申請を受けた都度、税額を確認する必要があるため入手する。 ・医療機関や本人等から入手する接種記録については、予防接種法施行令第6条の2に基づき記録・保存する必要があるため入手する。 <新型コロナワクチンのみに係る内容> ・本市への転入者について、転入前市区町村へ接種記録を照会し、提供を受ける場合のみ入手する。(番号法第19条第16号) ・本市からの転出者について、転出先市区町村での接種記録を提供するために、他市区町村から個人番号を入手する。(番号法第19条第16号) ・新型コロナウイルス感染症予防接種証明書の交付のため、接種者から交付申請があった場合のみ入手する。	・共通基盤システムより入手する住民情報・住民登録外情報は、接種対象者であることの確認を行うため入手する。 ・共通基盤システム(もしくは情報提供ネットワークを利用して他市区町村)より入手する世帯情報及び地方税関係情報については、本人から実費免除の申請を受けた都度、税額を確認する必要があるため入手する。 ・医療機関や本人等から入手する接種記録については、予防接種法施行令第6条の2に基づき記録・保存する必要があるため入手する。	事前	VRSの機能停止に伴う修正

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9月26日	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	・共通基盤システムより取得する情報については、本人に利用目的を明示し、同意を得た上で入手している。 ・情報提供ネットワークを利用して他市町村から地方税関係情報を確認する必要がある場合については、書面にて同意を得た上で入手している。 ・医療機関や本人等から入手の場合、本人等が記入する予診票にも、本市へ接種記録が提出されることを明記し、署名を得ている。 ＜新型コロナワクチンのみに係る内容＞ ・本市への転入者について接種者からの同意を得て入手する。 ・接種者からの接種証明書の交付申請に合わせて本人から入手する。	・共通基盤システムより取得する情報については、本人に利用目的を明示し、同意を得た上で入手している。 ・情報提供ネットワークを利用して他市町村から地方税関係情報を確認する必要がある場合については、書面にて同意を得た上で入手している。 ・医療機関や本人等から入手の場合、本人等が記入する予診票にも、本市へ接種記録が提出されることを明記し、署名を得ている。	事前	VRSの機能停止に伴う修正
令和6年9月26日	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住民票関係情報、本人等の申請内容等を保健情報管理システムTIARAに登録し、登録された情報を基に予防接種の対象者を確認する。 ②保健情報管理システムTIARAに接種記録を登録し、接種記録の管理及び保管を行う。 ③本人等の申請、住民票関係情報、地方税関係情報等の保健情報管理システムTIARAに登録された情報を基に、予防接種費用の実費に係る免除対象者の確認及び確認結果の通知を行う。 ＜新型コロナワクチンのみに係る内容＞ ④本市への転入者について、転入前市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 ⑤本市からの転出者について、転出先市区町村へ本市での接種記録を提供するために特定個人情報を使用する。 ⑥新型コロナウイルス感染症予防接種証明書の交付の際、接種記録を照会するために特定個人情報を使用する。	①住民票関係情報、本人等の申請内容等を保健情報管理システムTIARAに登録し、登録された情報を基に予防接種の対象者を確認する。 ②保健情報管理システムTIARAに接種記録を登録し、接種記録の管理及び保管を行う。 ③本人等の申請、住民票関係情報、地方税関係情報等の保健情報管理システムTIARAに登録された情報を基に、予防接種費用の実費に係る免除対象者の確認及び確認結果の通知を行う。	事前	VRSの機能停止に伴う修正
令和6年9月26日	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 情報の突合	・最新宛名コードにより住民票関係情報を突合し、対象者の資格を確認する。(使用方法①に該当) ・整理番号により住民票関係情報と対象者情報を確認する。(使用方法②に該当) ・個人番号により本人等の申請内容、住民関係情報、地方税関係情報を突合し、実費に係る免除対象者の確認を行う。(使用方法③に該当) ＜新型コロナワクチンのみに係る内容＞ ・本市からの転出者について、本市での接種記録を転出先市区町村に提供するために、他市区町村から個人番号を入手し、本市の接種記録と突合する。(使用方法⑤に該当)	・最新宛名コードにより住民票関係情報を突合し、対象者の資格を確認する。(使用方法①に該当) ・整理番号により住民票関係情報と対象者情報を確認する。(使用方法②に該当) ・個人番号により本人等の申請内容、住民関係情報、地方税関係情報を突合し、実費に係る免除対象者の確認を行う。(使用方法③に該当)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	[委託する] 5件	[委託する] 4件	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5	ワクチン接種記録システム(VRS)の管理等業務	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ①委託内容	新型コロナウイルス感染症対策に係る予防接種事務に関するワクチン接種記録システム(VRS)を用いた特定個人情報ファイルの管理等	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 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	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数	10万人以上100万人未満	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲	予防接種法等関連法令に定められる予防接種の対象者	削除	事前	VRSの機能停止に伴う修正

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9月26日	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5 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	ワクチン接種記録システム（VRS）を用いた特定個人情報ファイルの適切な管理等のために取り扱う必要がある。	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ③委託先における取扱者数	10人以上50人未満	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ④委託先への特定個人情報ファイルの提供方法	〔〇〕その他（LGWAN回線を用いた提供）	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ⑤委託先名の確認方法	下記「⑥委託者名」の項の記載より確認できる。	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ⑥委託先名	株式会社ミラボ	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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5 ⑦再委託先の有無	再委託しない	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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・移転の有無	〔〇〕提供を行っている 3件	〔〇〕提供を行っている 2件	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	市区町村長	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	番号法第19条第16号	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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提供先における用途	新型コロナウイルス感染症対策に係る予防接種事務	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	市区町村コード及び転入者の個人番号	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	10万人以上100万人未満	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	本市が予防接種法に基づき実施する予防接種をうけた者	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	〔〇〕その他（ワクチン接種管理システム（VRS）	削除	事前	VRSの機能停止に伴う修正

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9月26日	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	本市への転入者について、転入前市区町村への接種記録の照会を行う必要性が生じた都度	削除	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <ワクチン接種記録システム(VRS)における追加措置> ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお、以下のとおりのセキュリティ対策を講じている。 ・論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。 <紙、電子記録媒体における措置> (略)	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <紙、電子記録媒体における措置> (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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消去方法	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <紙媒体における措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <ワクチン接種記録システム(VRS)における追加措置> ・本市の領域に保管されたデータのみ、ワクチン接種記録システム(VRS)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。	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <紙媒体における措置> (略) <中間サーバー・プラットフォームにおける措置> (略)	事前	VRSの機能停止に伴う修正

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9月26日	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: 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	医療機関等から提出された予防接種結果を保健情報管理システムTIARAへ取り込む際に、住民基本台帳システム及び共通宛名システムから取得した住民情報と予診票(接種券)に記載された宛名コード・氏名・住所・生年月日等とマッチングを行い登録するため、対象者以外の情報が登録されることはない。 ＜新型コロナワクチンのみに係る措置＞ ①転入者本人からの個人番号の入手 本市への転入者について、転入前市区町村へ接種記録を照会するために、個人番号を入力する際は、接種券発行申請書兼接種記録確認同意書等により本人同意を取得し、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 ②転出先市区町村からの個人番号の入手 本市からの転出者について、本市での接種記録を転出先市区町村へ提供するため、転出先市区町村から個人番号を入力するが、その際は、転出先市区町村において、本人同意及び本人確認が行われた情報だけをワクチン接種記録システム(VRS)を通じて入手する。 ③新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入力するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。	医療機関等から提出された予防接種結果を保健情報管理システムTIARAへ取り込む際に、住民基本台帳システム及び共通宛名システムから取得した住民情報と予診票(接種券)に記載された宛名コード・氏名・住所・生年月日等とマッチングを行い登録するため、対象者以外の情報が登録されることはない。	事前	VRSの機能停止に伴う修正
令和6年9月26日		④新型コロナウイルス感染症予防接種証明書の交付申請者からの個人番号の入手 接種者について、新型コロナウイルス感染症予防接種証明書の交付のために個人番号を入力するのは、接種者から接種証明書の交付申請があった場合のみとし、さらに、番号法第16条に基づき、本人確認書類を確認することで、対象者以外の情報の入手を防止する。 (新型コロナウイルス感染症予防接種証明書電子交付機能、コンビニ交付) 交付申請には、個人番号カードのICチップ読み取り(券面事項入力補助AP)と暗証番号入力(券面事項入力補助APの暗証番号)による二要素認証を必須とすることで、対象者以外の情報の入手を防止する。			
令和6年9月26日	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: 不適切な方法で入手が行われるリスク リスクに対する措置の内容	＜窓口・郵送での入手＞ (略) ＜システムを通じた入手＞ (略) ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)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。	＜窓口・郵送での入手＞ (略) ＜システムを通じた入手＞ (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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: 入手の際に特定個人情報漏えい・紛失するリスク リスクに対する措置の内容	＜保健情報管理システムTIARAにおける措置＞ (略) ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手する特定個人情報については、情報漏えいを防止するために、暗号化された通信回線を使用する。	＜保健情報管理システムTIARAにおける措置＞ (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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: 入手の際に特定個人情報漏えい・紛失するリスク 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: 入手の際に特定個人情報漏えい・紛失するリスク リスクに対する措置	・端末の画面が来庁者の目に触れないように設置する。 ・受領した予診票等が他者の目に触れないようにする。 ・マイナンバーが記載された書類は、鍵のかかる書庫にて保管している。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 入手した特定個人情報については、限定された端末を利用して本市が指定する管理者から配布されたユーザIDを使用し、ログインした場合だけアクセスできるように制御している。	・端末の画面が来庁者の目に触れないように設置する。 ・受領した予診票等が他者の目に触れないようにする。 ・マイナンバーが記載された書類は、鍵のかかる書庫にて保管している。	事前	VRSの機能停止に伴う修正
令和6年9月26日	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: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	保健情報管理システムTIARAは、事務に関係のない情報との紐付けはできない。 ＜ワクチン接種記録システム(VRS)における追加措置＞ 接種会場等では、接種券番号の読取端末(タブレット端末)からインターネット経由でワクチン接種記録システム(VRS)に接続するが、個人番号にはアクセスできないように制御している。	保健情報管理システムTIARAは、事務に関係のない情報との紐付けはできない。	事前	VRSの機能停止に伴う修正

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9月26日	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: 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 具体的な管理方法	・ユーザーID、パスワード及び静脈による二要素認証を行っているため、権限のない者は利用できない。 ・認証後は、ユーザ毎に利用可能な機能を制限しているため、権限のない機能は利用できない。 ・パスワードは定期的に変更している。なお、一定期間変更がなかった場合は、ログイン時にパスワード変更画面に遷移するよう設定している。 ＜ワクチン接種記録システム（VRS）における追加措置＞ 権限のない者によって不正に使用されないよう、以下の対策を講じている。 ・ワクチン接種記録システム（VRS）における特定個人情報へのアクセスは、LGWAN端末による操作に限り可能になるように制御している。 ・LGWAN端末は、限定された者しかログインできる権限を保持しない。 ・ワクチン接種記録システム（VRS）におけるログイン認証は、ユーザID・パスワードにて行う。 ・ワクチン接種記録システム（VRS）へのログイン用のユーザIDは、本市が指定する管理者が認めた者に限定して発行される。	・ユーザーID、パスワード及び静脈による二要素認証を行っているため、権限のない者は利用できない。 ・認証後は、ユーザ毎に利用可能な機能を制限しているため、権限のない機能は利用できない。 ・パスワードは定期的に変更している。なお、一定期間変更がなかった場合は、ログイン時にパスワード変更画面に遷移するよう設定している。	事前	VRSの機能停止に伴う修正
令和6年9月26日	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: 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 アクセス権限の発効・失効の管理 具体的な管理方法	人事異動や権限変更があった場合は、新しく権限を付与する者および権限を失効させる者について、書面で管理者が決裁し、保健情報管理システムTIARAに内容を反映している。また、権限内容について定期的に確認している。 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）へのログイン用のユーザIDに付与されるアクセス権限は、本市が指定する管理者が必要最小限の権限で発効する。 本市が指定する管理者は、定期的又は異動・退職等のイベントが発生したタイミングで、権限を有していた職員の異動・退職等情報を確認し、当該事由が生じた際には速やかにアクセス権限を更新し、当該ユーザIDを失効させる。やむを得ず、複数の職員が共有するID（以下「共用ID」という。）を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、管理者が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動・退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。	人事異動や権限変更があった場合は、新しく権限を付与する者および権限を失効させる者について、書面で管理者が決裁し、保健情報管理システムTIARAに内容を反映している。また、権限内容について定期的に確認している。	事前	VRSの機能停止に伴う修正
令和6年9月26日	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: 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 アクセス権限の管理 具体的な管理方法	・端末操作資格者のアクセス可能機能の権限一覧表を作成している。 ・業務上アクセスが不要となった機能については、アクセス権限の変更または削除している。 ＜ワクチン接種記録システム（VRS）における追加措置＞ ワクチン接種記録システム（VRS）へのログイン用のユーザIDは、本市が指定する管理者が必要最小限の権限で発効する。 本市が指定する管理者は、定期的にユーザID及びアクセス権限の一覧をシステムにおいて確認し、アクセス権限及び不正利用の有無を確認する。また、不要となったユーザIDやアクセス権限を速やかに変更又は削除する。	・端末操作資格者のアクセス可能機能の権限一覧表を作成している。 ・業務上アクセスが不要となった機能については、アクセス権限の変更または削除している。	事前	VRSの機能停止に伴う修正
令和6年9月26日	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: 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 特定個人情報の使用の記録 具体的な管理方法	・端末から検索、更新した際のアクセスログを記録、一定期間保存している。 ・処理日時、端末情報、部署情報、操作者情報、処理事由を記録している。 ・バックアップされたアクセスログは、7年間保存している。 ＜ワクチン接種記録システム（VRS）における追加措置＞ システム上の操作のログを取得しており、操作ログを確認できる。ログは定期に及び必要に応じ随時に確認する。	・端末から検索、更新した際のアクセスログを記録、一定期間保存している。 ・処理日時、端末情報、部署情報、操作者情報、処理事由を記録している。 ・バックアップされたアクセスログは、7年間保存している。	事前	VRSの機能停止に伴う修正

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9月26日	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク4: 特定個人情報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	・端末は、原則、外部媒体を使用することができない仕組みとなっている。ただし、許可された専用の外部媒体のみ、使用することができる。 ・システムのバックアップデータ等は厳重に管理されており、権限のある者のみがアクセスできる。 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 住民基本台帳システムから特定個人情報を出したCSVファイルをワクチン接種記録システム(VRS)へ登録する際には、以下のようにしている。 ・作業を行う職員及び端末を必要最小限に限定する。 ・作業に用いる電子記録媒体については、不正な複製、持ち出し等を防止するために、許可された専用の外部記録媒体を使用する。また、媒体管理簿等に使用の記録を記載する等、利用履歴を残す。 ・作業に用いる電子記録媒体の取扱いについては、承認を行い、当該承認の記録を残す。 ・電子記録媒体に格納するデータについては、暗号化やパスワード設定を行う。 ・電子記録媒体による作業を終了したら、内部のデータを確実に消去する。管理簿に消去の記録を記載する等、消去履歴を残す。	・端末は、原則、外部媒体を使用することができない仕組みとなっている。ただし、許可された専用の外部媒体のみ、使用することができる。 ・システムのバックアップデータ等は厳重に管理されており、権限のある者のみがアクセスできる。	事前	VRSの機能停止に伴う修正
令和6年9月26日	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク4: 特定個人情報ファイルが不正に複製されるリスク 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	・ログイン後一定時間操作がない場合、自動でログオフされる仕組みとなっている。 ・スクリーンセーバ等を利用して、長時間にわたり業務画面を表示させない。 ・端末のディスプレイを来庁者から見えない位置に配置する。 ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ ①特定個人情報を使用する場面に必要最小限に限定している。具体的には以下の3つの場面に限定している。 ・本市への転入者について、転入前市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・本市からの転出者について、本市での接種記録を転出先市区町村へ提供するために、個人番号を入手し、使用する。 ・接種者について、新型コロナウイルス感染症予防接種証明書の交付申請があった場合に、接種記録を照会するために、個人番号を入手し、使用する。 ②ワクチン接種記録システム(VRS)からCSVファイルにてダウンロードする接種記録データには、個人番号が含まれない。	・ログイン後一定時間操作がない場合、自動でログオフされる仕組みとなっている。 ・スクリーンセーバ等を利用して、長時間にわたり業務画面を表示させない。 ・端末のディスプレイを来庁者から見えない位置に配置する。	事前	VRSの機能停止に伴う修正
令和6年9月26日	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	＜システム運用・保守委託について＞ (略) ＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 本市、国、当該システムの運用保守事業者の三者の関係を規定した「ワクチン接種記録システムの利用にあたっての確認事項(規約)」に同意することにより、当該確認事項に基づき、ワクチン接種記録システム(VRS)に係る特定個人情報の取扱いを当該システムの運用保守事業者に委託することとする。なお、次の内容については、当該確認事項に規定されている。 ・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 ・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 ・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	＜システム運用・保守委託について＞ (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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 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。) 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 具体的方法	＜庁内のデータ連携で提供・移転する場合における措置＞ ・共通宛名システム等庁内システムとのデータ連携については、システム上で自動化されている。 ・端末機で情報を利用した場合は、操作履歴(ログ)を記録している。 ＜ワクチン接種記録システム(VRS)における追加措置＞ ワクチン接種記録システム(VRS)では、他市区町村への提供の記録を取得しており、委託業者から「情報提供の記録」を入手し、記録の確認をすることができる。	＜庁内のデータ連携で提供・移転する場合における措置＞ ・共通宛名システム等庁内システムとのデータ連携については、システム上で自動化されている。 ・端末機で情報を利用した場合は、操作履歴(ログ)を記録している。	事前	VRSの機能停止に伴う修正

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9月26日	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 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。） 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	<庁内のデータ連携で提供・移転する場合における措置> (略) <新型コロナウイルス感染症対策に係る予防接種事務における追加措置> ・本市への転入者について、転入前市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、その際は、住民基本台帳等により照会対象者の個人番号であることを確認した情報を、ワクチン接種記録システム（VRS）を用いて提供する。 転出先市区町村へ接種記録を提供するが、その際は、転出元市区町村において、住民基本台帳等により照会対象者の個人番号であることを確認し、当該個人番号に対応する個人の接種記録のみをワクチン接種記録システム（VRS）を用いて提供する。	<庁内のデータ連携で提供・移転する場合における措置> (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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 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。） 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	<庁内のデータ連携で提供・移転する場合における措置> (略) <ワクチン接種記録システム（VRS）における追加措置> ・本市への転入者について、転入前市区町村から接種記録を入手するため、他市区町村へ個人番号を提供するが、電文を受ける市区町村で、該当者がいない場合は、個人番号は保管されず、これに対して接種記録は提供されない仕組みとなっている。	<庁内のデータ連携で提供・移転する場合における措置> (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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 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。） 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 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	<ワクチン接種記録システム（VRS）における追加措置> ・特定個人情報の提供は、限定された端末（LGWAN端末）だけができるように制御している。 ・特定個人情報を提供する場面を必要最低限にしている。具体的には本市への転入者について、転入前市区町村での接種記録を入手するために、他市区町村へ個人番号を提供する場面に限定している。	—	事前	VRSの機能停止に伴う修正
令和6年9月26日	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：特定個人情報の漏えい・滅失・毀損リスク ⑥物理的対策 具体的な対策の内容	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <ワクチン接種記録システム（VRS）における追加措置> ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切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満たしている。 ・サーバー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。	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	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：特定個人情報の漏えい・滅失・毀損リスク ⑥技術的対策 具体的な対策の内容	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <ワクチン接種記録システム（VRS）における措置> ワクチン接種記録システム（VRS）は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報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、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切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本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県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。 ・LGWAN端末とワクチン接種記録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。	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略)	事前	VRSの機能停止に伴う修正

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9月26日	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	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <新型コロナワクチンのみに係る措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	IVその他のリスク対策 1. 監査 ②監査 具体的なチェック方法	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <新型コロナワクチンのみに係る措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な監督をする。	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	IVその他のリスク対策 2. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	<本市における措置> (略) <予防接種事務における措置> (略) <中間サーバー・プラットフォームにおける措置> (略) <新型コロナワクチンのみに係る措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第9条(市区町村の責任)に則し、適切に職員等の当該システムの利用を管理し、必要な指導をする。	<本市における措置> (略) <予防接種事務における措置> (略) <中間サーバー・プラットフォームにおける措置> (略)	事前	VRSの機能停止に伴う修正
令和6年9月26日	IVその他のリスク対策 3. その他のリスク対策	<中間サーバー・プラットフォームにおける措置> (略) <新型コロナワクチンのみに係る措置> デジタル庁(旧内閣官房情報通信技術(IT)総合戦略室)から発出された「新型コロナウイルスワクチン接種記録システムの利用にあたっての確認事項」に同意のうえ、第7条(情報到達の責任分界点)、第8条(通信経路の責任分界点)、第9条(市区町村の責任)に則し、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。	<中間サーバー・プラットフォームにおける措置> (略)	事前	VRSの機能停止に伴う修正
令和7年7月16日	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	※前略 ・4情報、連絡先:正確な本人特定のため、予診票等に記入された情報と突合するために保有、また、予防接種の接種動向に使用するため保有 ※後略	※前略 ・5情報、連絡先:正確な本人特定のため、予診票等に記入された情報と突合するために保有、また、予防接種の接種動向に使用するため保有 ※後略	事後	
令和7年7月16日	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	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館、及びサーバー室への入室を行う際は、警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ・特定個人情報は、サーバー室に設置された中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 <紙、電子記録媒体における措置> (略)	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームは、政府情報管理システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 <紙、電子記録媒体における措置> (略)	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	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保存期間 その妥当性	予防接種法施行令第6条の2において、接種記録については5年間保存しなければならないと規定されている。しかし、二重接種等の誤りを防ぐためや、海外渡航時の証明で必要になるため、生涯必要となる。そのため、過去の接種記録を永年保存しておく必要がある。	予防接種法施行規則第3条において、接種記録については5年間保存しなければならないと規定されている。しかし、二重接種等の誤りを防ぐためや、海外渡航時の証明で必要になるため、生涯必要となる。そのため、過去の接種記録を永年保存しておく必要がある。	事後	

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7年7月16日	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	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ・特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・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、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊により完全に消去し、消去した記録を保存する。 <紙媒体における措置> (略)	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度(ISMAP)に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 <紙媒体における措置> (略)	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク4: 入手の際に特定個人情報が増えい・紛失するリスク リスクに対する措置の内容	<団体内統合宛名システムにおける措置> (略) <中間サーバー・ソフトウェアにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ・中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、漏えい・紛失のリスクに対応している。 ・中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはない。	<団体内統合宛名システムにおける措置> (略) <中間サーバー・ソフトウェアにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 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	<団体内統合宛名システムにおける措置> (略) <中間サーバー・ソフトウェアにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ・中間サーバーと既存システム、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。 ・中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ・中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	<団体内統合宛名システムにおける措置> (略) <中間サーバー・ソフトウェアにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォームの事業者及びクラウドサービス事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク3: 入手した特定個人情報が増えい・紛失するリスク リスクに対する措置の内容	※前略 <中間サーバー・ソフトウェアにおける措置> ①中間サーバーは、特定個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 ※後略	※前略 <中間サーバー・ソフトウェアにおける措置> ①中間サーバーは、個人情報保護委員会との協議を経て、内閣総理大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。 ※後略	事後	誤記の修正

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7年7月16日	Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	<中間サーバー・ソフトウェアにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ・中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ・中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ・中間サーバー・プラットフォームでは、特定個人情報情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ・特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	<中間サーバー・ソフトウェアにおける措置> (略) <中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォーム事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	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 ⑤物理的対策 具体的な対策の内容	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームをデータセンターに構築し、設置場所への入退室管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ・事前に申請し承認されていない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	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 ⑥技術的対策 具体的な対策の内容	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ・中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ・導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームではUTM(コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置)等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ④中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤中間サーバーのデータベースに保存される特定個人情報情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	Ⅳ その他のリスク対策 1. 監査 ②監査 具体的な内容	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ①運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ②政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更
令和7年7月16日	Ⅳ その他のリスク対策 3. その他のリスク対策	<中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームを活用することにより、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リテラン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。	<中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームを活用することにより、政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者による高レベルのセキュリティ管理(入退室管理等)、ITリテラン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。	事後	特定個人情報の漏えいその他の事態を発生させるリスクを相当程度変動させるものではないと考えられる変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	I 基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の内容	予防接種法(昭和23年6月30日法律第68号)及び新型コロナウイルス等対策特別措置法(平成24年5月11日法律第31号)に基づき、市内に居住する者に対し予防接種を実施するとともに、接種歴等の情報管理・報告や給付の支給に対する事務等を行う。特定個人情報ファイルを取り扱う事務については、接種歴等の照会等に関する事務のみである。	予防接種法(昭和23年6月30日法律第68号)及び新型コロナウイルス等対策特別措置法(平成24年5月11日法律第31号)に基づき、市内に居住する者に対し予防接種を実施するとともに、接種歴等の情報管理・報告や給付の支給に対する事務等を行う。 <予診情報・予防接種記録管理/請求支払システム(以下「予予請求システム」という。)を活用した情報連携に係る予防接種事務> ・本市は、情報連携のため、予予請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 ・住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 ・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	システム更新等に伴う重要な変更
	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム1 ①システムの名称	保健情報管理システムTIARA	健康かるてV8	事前	システム更新等に伴う重要な変更
	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム2 ②システムの機能	①本人確認 申告書等の受付などを行う際、窓口における本人確認のため、提示された個人番号カード等を基に住基ネットが保有する本人確認情報に照会を行い、確認結果を画面上に表示する機能。 ②本人確認情報検索 統合端末において入力された4情報(氏名、住所、性別、生年月日)の組み合わ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機能。 ③地方公共団体情報システム機構への情報照会 全国サーバに対して個人番号又は4情報の組み合わせをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する機能。	①本人確認 申告書等の受付などを行う際、窓口における本人確認のため、提示された個人番号カード等を基に住基ネットが保有する本人確認情報に照会を行い、確認結果を画面上に表示する機能。 ②本人確認情報検索 統合端末において入力された5情報(氏名、氏名の振り仮名、住所、性別、生年月日)の組み合わ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機能。 ③地方公共団体情報システム機構への情報照会 全国サーバに対して個人番号又は5情報の組み合わせをキーとした本人確認情報照会要求を行い、該当する個人の本人確認情報を受領する機能。	事後	法改正に伴う変更
	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3～6	システム3: 共通宛名システム システム4: 共通基盤システム (庁内連携システムと同義) システム5: 団体内統合宛名システム (宛名システム等と同義) システム6: 中間サーバー	システム3: 共通基盤システム (庁内連携システムと同義) システム4: 団体内統合宛名システム (宛名システム等と同義) システム5: 中間サーバー ※変更前のシステム3: 共通宛名システムを削除、それに伴い変更前のシステム4～6をシステム3～5へ転記。	事前	システム更新等に伴う重要な変更
	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 ①システムの名称	新設	予予請求システム	事前	システム更新等に伴う重要な変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム6 ②システムの機能	新設	①予防接種関連データの登録機能 本市は、健康管理システムからの情報連携又は予予請求システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予予請求システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予予請求システムは、本市で管理している個人番号、対象者情報、予診票情報及び接種記録を予予請求システムに登録する。また、Public Medical Hubを経由して医療情報基盤・診療報酬審査支払機構（以下、「DX審査支払機構」という。）の医療保険者等向け中間サーバーと連動し、PMHキーを自動採番する。すでにPMHキーが採番済みの個人番号であれば、採番は行わずに既存のPMHキーを利用する。	事前	システム更新等に伴う重要な変更
			③情報連携機能（マイナポータル） ・識別子の格納機能 予予請求システムは、マイナポータルからの予予請求システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予予請求システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナナンバーカードの電子証明書のシリアル番号に紐づくPMH仮名識別子を利用した照会を行う。予予請求システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐づく接種記録・通知をマイナポータルへ提供する。また、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、予予請求システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐づく予診票情報を登録する。		
			④情報連携機能（医療機関用アプリ等） ・本人確認情報の格納機能 予防接種対象者が、顔認証端末又はマイナ資格確認アプリを利用してマイナナンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリ等は、予予請求システムへ本人確認情報を利用した照会を行う。予予請求システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐づく予防接種対象者番号をキーに予診票情報を医療機関用アプリ等に提供する。また、医療機関が接種記録の入力画面から情報を入力することにより、予予請求システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐づく接種記録を登録する。 ⑤情報連携機能（履歴照会回答システム） ・識別子の格納機能 予予請求システムは接種記録等の情報を予防接種DBIに連携し、予防接種DBIにおいて予防接種の有効性・安全性等の調査・研究を行う。予予請求システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐付けて予予請求システムに連携する。		
	I 基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム システム6 ③他のシステムとの接続	新設	健康かるてV8、マイナポータル、医療機関用アプリ等、Public Medical Hub、履歴照会回答システム	事前	システム更新等に伴う重要な変更
	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に関する法律（平成25年法律第27号）（以下「番号法」という。）第9条第1項及び別表の項番14、126 番号法別表の主務省令で定める事務を定める命令（平成26年内閣府・総務省令第5号）第10条、第67条の2	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に関する法律（平成25年法律第27号）（以下「番号法」という。）第9条第1項及び別表の項番14、126 番号法別表の主務省令で定める事務を定める命令（平成26年内閣府・総務省令第5号）第10条、第67条の2 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ 明石市個人番号の利用に関する条例（平成27年12月28日条例第34号） ※令和9年9月頃条例改正予定	事前	システム更新等に伴う重要な変更
	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	※前略 ・業務関係情報 []国税関係情報 [○]地方税関係情報 []健康・医療関係情報 []医療保険関係情報 []児童福祉・子育て関係情報 []障害者福祉関係情報 []生活保護・社会福祉関係情報 []介護・高齢者福祉関係情報 []雇用・労働関係情報 []年金関係情報 []学校・教育関係情報 []災害関係情報 [○]その他（予防接種記録）	※前略 ・業務関係情報 []国税関係情報 [○]地方税関係情報 []健康・医療関係情報 []医療保険関係情報 []児童福祉・子育て関係情報 []障害者福祉関係情報 []生活保護・社会福祉関係情報 []介護・高齢者福祉関係情報 []雇用・労働関係情報 []年金関係情報 []学校・教育関係情報 []災害関係情報 [○]その他（予防接種記録情報）	事前	システム更新等に伴う重要な変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅱ 特定個人情報ファイルの概要 2. 基本情報 ④記録される項目 その妥当性	※前略 ・予防接種記録：接種記録の管理を行うために記録	※前略 ・予防接種記録情報：接種記録の管理を行うために記録 ＜予防請求システムを活用した情報連携に係る予防接種事務＞ ・その他識別情報（内部番号）：PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5：予防請求システムが、外部と情報連携するために必要となる。 ・その他（予防接種記録情報）：予防請求システムが、外部と情報連携するために必要となる。	事前	システム更新等に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 2. 基本情報 ⑤保有開始日	平成28年1月1日	平成28年1月1日 ＜予防請求システムを活用した情報連携に係る予防接種事務に係る情報＞ 令和10年4月1日以降で本市が同事務を開始可能な日	事前	システム更新等に伴う重要な変更
	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	〔○〕 本人又は本人の代理人 〔○〕 評価実施機関内の他部署（市民課） 〔 〕 行政機関・独立行政法人等（ ） 〔○〕 地方公共団体・地方独立行政法人（市町村） 〔 〕 民間事業者（ ） 〔 〕 その他（ ）	〔○〕 本人又は本人の代理人 〔○〕 評価実施機関内の他部署（市民課） 〔 〕 行政機関・独立行政法人等（ ） 〔○〕 地方公共団体・地方独立行政法人（市町村） 〔○〕 民間事業者（医療機関） 〔○〕 その他（DX審査支援機構）	事前	システム更新等に伴う重要な変更
	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	〔○〕 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（ ）	〔○〕 紙 〔 〕 電子記録媒体（フラッシュメモリを除く。） 〔 〕 フラッシュメモリ 〔 〕 電子メール 〔 〕 専用線 〔○〕 庁内連携システム 〔○〕 情報提供ネットワークシステム 〔○〕 その他（Public Medical Hub、医療機関用アプリ等、マイナポータル）	事前	システム更新等に伴う重要な変更
	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	※前略	※前略 ＜予防請求システムを活用した情報連携に係る予防接種事務＞ ・予防請求システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・国が予防請求システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本市が個人情報を入手し、予防請求システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等また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、予防請求システムにおいて個人番号と結びついて特定個人情報となる。	事前	システム更新等に伴う重要な変更
	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	※前略	※前略 ＜予防請求システムを活用した情報連携に係る予防接種事務＞ （PMHキー採番処理依頼時に入手される特定個人情報） ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 （個人情報として入手し、予防請求システムにおいて個人番号と結び付き特定個人情報となる情報） ・本市が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入手し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証（本人確認）の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。	事前	システム更新等に伴う重要な変更
	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	※前略	※前略 ＜予防請求システムを活用した情報連携に係る予防接種事務＞ ・マイナポータル等では、本人等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	システム更新等に伴う重要な変更

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住民票関係情報、本人等の申請内容等を保健情報管理システムTIARAに登録し、登録された情報を基に予防接種の対象者を確認する。 ②保健情報管理システムTIARAに接種記録を登録し、接種記録の管理及び保管を行う。 ③本人等の申請、住民票関係情報、地方税関係情報等の保健情報管理システムTIARAに登録された情報を基に、予防接種費用の実費に係る免除対象者の確認及び確認結果の通知を行う。	①住民票関係情報、本人等の申請内容等を健康からてV8に登録し、登録された情報を基に予防接種の対象者を確認する。 ②健康からてV8に接種記録を登録し、接種記録の管理及び保管を行う。 ③本人等の申請、住民票関係情報、地方税関係情報等の健康からてV8に登録された情報を基に、予防接種費用の実費に係る免除対象者の確認及び確認結果の通知を行う。 ＜予予請求システムを活用した情報連携に係る予防接種事務＞ ①情報連携のため、本市は、予予請求システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ②登録後、予予請求システムは、Public Medical Hubに対してオンライン資格確認等システムと予予請求システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予予請求システムに回答する。 ③PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予予請求システムで共有されることで予予請求システムからマイナポータルへの通知、マイナポータルや医療機関用アプリ等から予予請求システムの予診票情報及び接種記録の取得・閲覧・入力等といった情報連携が可能となる。	事前	システム更新に伴う重要な変更
	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 ⑨使用開始日	平成28年1月1日	平成28年1月1日 ＜予予請求システムを活用した情報連携に係る予防接種事務に係る情報＞ 令和10年4月1日以降で本市が同事務を開始可能な日	事前	システム更新に伴う重要な変更
	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	[委託する] 4件	[委託する] 5件	事前	システム更新に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1	保健システム構築・運用業務	健康管理システム構築・運用業務委託 ※導入完了後は保守・運用業務を委託する予定	事前	システム更新に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ①委託内容	・保健情報管理システムTIARAの保守・運用業務 ・法制度改正に伴う保健情報管理システムTIARAの改修	健康管理標準準拠システム（健康からてV8）導入業務	事前	システム更新に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲	予防接種券の発行履歴がある者及び予防接種歴のある者	全市民及び過去に市民であった者のうち予防接種歴のある者	事前	システム更新に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑥委託先名	富士通グループ明石市保健システム構築・運用業務共同事業体	株式会社両備システムズ 大阪支社	事前	システム更新に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 ⑦再委託の有無	[再委託する]	[再委託しない]	事前	システム更新に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 再委託 ⑧再委託の許諾方法	・委託先から再委託承諾申請書の提出があり、本市が再委託承諾書により承諾した場合に限る。 ・再委託先から従業者名簿及び再委託先の従業者から個人情報の取扱いに関する誓約書を提出させる。	削除	事前	システム更新に伴う重要な変更
	Ⅱ 特定個人情報ファイルの概要 4. 特定個人情報ファイルの取扱いの委託 委託事項1 再委託 ⑨再委託事項	保健情報管理システムTIARAの保守・運用業務における作業担当として、技術支援作業を行う。	削除	事前	システム更新に伴う重要な変更

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 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲	予防接種券の発行履歴がある者及び予防接種歴のある者	予防接種歴のある者	事後	誤記による変更
	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 ⑦再委託の有無	[再委託する]	[再委託しない]	事前	システム更新に伴う重要な変更
	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 ⑧再委託の許諾方法	・委託先から再委託承諾申請書の提出があり、本市が再委託承諾書により承諾した場合に限る。 ・再委託先から従業者名簿及び再委託先の従業者から個人情報の取扱いに関する誓約書を提出させる。	削除	事前	システム更新に伴う重要な変更
	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	団体内統合宛名システムの維持・運用管理における作業担当として、技術支援作業を行う。	削除	事前	システム更新に伴う重要な変更
	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6	新設	予予請求システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱いに係る業務委託 ※本件については、記載の内容に則り、令和10年4月1日以降で本市が同事務を開始可能な日から実施予定	事前	システム更新に伴う重要な変更
	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6 ①委託内容	新設	予予請求システムの利用・情報連携業務及び運用保守業務	事前	システム更新に伴う重要な変更
	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6 ②取扱いを委託する特定個人情報ファイルの範囲	新設	[特定個人情報ファイルの一部]	事前	システム更新に伴う重要な変更
	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6 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の数	新設	10万人以上100万人未満	事前	システム更新に伴う重要な変更
	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6 ②取扱いを委託する特定個人情報ファイルの範囲 対象となる本人の範囲	新設	全市民及び過去に市民であった者のうち予防接種歴のある者	事前	システム更新に伴う重要な変更
	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6 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	新設	予予請求システムは公益社団法人国民健康保険中央会（以下、国保中央会という。）が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。ただし、予予請求システムに格納された特定個人情報は、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、兵庫県国民健康保険団体連合会（以下、兵庫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	システム更新に伴う重要な変更
	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6 ③委託先における取扱者数	新設	10人以上50人未満	事前	システム更新に伴う重要な変更
	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6 ④委託先への特定個人情報ファイルの提供方法	新設	[]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 [O] その他（LGWANまたは閉域網回線を用いた提供）	事前	システム更新に伴う重要な変更

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6 ⑤委託先名の確認方法	新設	下記「⑥委託先名」の項の記載より確認できる。	事前	システム更新に伴う重要な変更
	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5 ⑥委託先名	新設	兵庫県国保連合会	事前	システム更新に伴う重要な変更
	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6 再委託 ⑦再委託の有無	新設	[再委託する]	事前	システム更新に伴う重要な変更
	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6 再委託 ⑧再委託の許諾方法	新設	書面または電磁的方法による承諾	事前	システム更新に伴う重要な変更
	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6 再委託 ⑨再委託事項	新設	・予予請求システムの運用保守 ・PMHキーの採番及びPMHキーを介した医療機関用アプリ等・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。	事前	システム更新に伴う重要な変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ① 保管場所	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> ・団体内統合宛名システムサーバーは庁舎の管理区域内に、その他のサーバーは入館管理が厳重な庁舎外のデータセンターに設置しており、サーバー室への入室についても、厳重に管理されている。なお、本市においては、当該サーバーへアクセス権限を有する端末のみ使用している。 ・特定個人情報、サーバー室に設置されたサーバーのデータベース内に保存されている。 ・バックアップデータを遠隔地に保管している。 (保健情報管理システムTIARA及び共通宛名システムのみの) <中間サーバー・プラットフォームにおける措置> ① 中間サーバー・プラットフォームは、政府情報管理システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。	<健康からてV8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、クラウド事業者は政府情報システムのためのセキュリティ評価制度(以下「ISMAP」と記載。)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。 <団体内統合宛名システム、共通基盤システムにおける措置> ・団体内統合宛名システムサーバーは庁舎の管理区域内に、その他のサーバーは入館管理が厳重な庁舎外のデータセンターに設置しており、サーバー室への入室についても、厳重に管理されている。なお、本市においては、当該サーバーへアクセス権限を有する端末のみ使用している。	事前	システム更新等に伴う重要な変更
		・日本国内でデータを保管している。② 特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 <紙、電子記録媒体における措置>・帳票等の保管については、職員以外の者が入室できない書庫等にて保管する。 ・電子記録媒体の保管については、課内鍵付きの保管庫において保管する。	・特定個人情報は、サーバー室に設置されたサーバーのデータベース内に保存されている。 <ガバメントクラウドにおける措置> ① サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、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。 <中間サーバー・プラットフォームにおける措置> ① 中間サーバー・プラットフォームは、ISMAPのリストに登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。		
			・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ② 特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。 <紙、電子記録媒体における措置>・帳票等の保管については、職員以外の者が入室できない書庫等にて保管する。 ・電子記録媒体の保管については、課内鍵付きの保管庫において保管する。 <予予請求システムを活用した情報連携に係る予防接種事務> 予予請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、ISMAPのリストに登録されたサービスが、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。		
	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 保存期間 その妥当性	予防接種法施行令第6条の2において、接種記録については5年間保存しなければならないと規定されている。しかし、二重接種等の誤りを防ぐためや、海外渡航時の証明で必要になるため、生涯必要となる。そのため、過去の接種記録を永年保存しておく必要がある。	予防接種法施行規則第4条において、接種記録については予防接種を受けた者が死亡した日の翌日から5年を経過するまで保存しなければならないと規定されているため。	事後	法改正に伴う変更

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅱ 特定個人情報ファイルの概要 6. 特定個人情報の保管・消去 ③消去方法	<保健情報管理システムTIARA、団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> ・接種履歴データについては永年保存するため、誤りがない限り、消去は行わない。 ・消去は、各事務システムと連動しているため、通常、保守・運用を行う事業者が消去することはない。 ・機器更改等の際は、保存された情報が読み出できないよう、物理的破壊または専用ソフト等を利用して完全に消去し、消去した記録を保存する。 <紙媒体における措置> ・帳票等の破棄は、焼却・熔解処理を行い破棄する。 ・破棄の記録については、明石市文書管理規程に基づき保存する。	<健康からてV8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	システム更新等に伴う重要な変更
		<中間サーバー・プラットフォームにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度 (ISMAP) に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出できないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。	<団体内統合宛名システム、共通基盤システムにおける措置> ・接種履歴データについては永年保存するため、誤りがない限り、消去は行わない。 ・消去は、各事務システムと連動しているため、通常、保守・運用を行う事業者が消去することはない。 ・機器更改等の際は、保存された情報が読み出できないよう、物理的破壊または専用ソフト等を利用して完全に消去し、消去した記録を保存する。 <紙媒体における措置> ・帳票等の破棄は、焼却・熔解処理を行い破棄する。 ・破棄の記録については、明石市文書管理規程に基づき保存する。 <ガバメントクラウドにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報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、NIST800-88、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。 <中間サーバー・プラットフォームにおける措置> ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、ISMAPに準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ③中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出できないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。		
			<予予請求システムを活用した情報連携に係る予防接種事務> ・本市の領域に保管されたデータのみ、予予請求システムを用いて消去することができる。 ・本市の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。		

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	医療機関等から提出された予防接種結果を保健情報管理システムTIARAへ取り込む際に、住民基本台帳システム及び共通宛名システムから取得した住民情報と予診票(接種券)に記載された宛名コード・氏名・住所・生年月日等とマッチングを行い登録するため、対象者以外の情報が登録されることはない。	医療機関等から提出された予防接種結果を健康かるてV8へ取り込む際に、住民基本台帳システムから取得した住民情報と予診票(接種券)に記載された宛名コード・氏名・住所・生年月日等とマッチングを行い登録するため、対象者以外の情報が登録されることはない。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・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、マイナンバーヘルログインし、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)から予予請求システムに連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。	事前	システム更新等に伴う重要な変更
	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: 目的外の入手が行われるリスク 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	保健情報管理システムTIARAの画面および帳票には、個人番号は表示しない仕組みとし、不用意な閲覧が行われないようにする。	健康かるてV8の画面および帳票には、個人番号は表示しない仕組みとし、不用意な閲覧が行われないようにする。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予請求システムへは、定められたインターフェース仕様に沿って決められたデータ項目(PMHキーと個人番号)のみが返却されるようシステムの制御している。 ・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の制御している。 ・本人が、マイナンバーヘルログインし、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の制御している。 ・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	システム更新等に伴う重要な変更
	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: 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	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予予請求システムへは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目(PMHキーと個人番号)のみが返却されるようシステムの制御している。 ・予予請求システムのデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。 ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。	事前	システム更新等に伴う重要な変更
	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: 入手した特定個人情報が入力の本人確認の措置の内容	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムが提供した個人番号は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	システム更新等に伴う重要な変更
	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: 入手した特定個人情報が入力の真正性確認の措置の内容	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムが提供した個人番号は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	システム更新等に伴う重要な変更
	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: 入手した特定個人情報が入力の真正性確認の措置の内容	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。	事前	システム更新等に伴う重要な変更

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4: 入手の際に特定個人情報が増え、紛失するリスク リスクに対する措置の内容	＜保健情報管理システムTIARAにおける措置＞ 個人番号、基本4情報等の宛名情報の入手については、厳重に入館・入退室管理が行われているデータセンター内のサーバー間通信に限定することにより、情報漏えい・紛失等を防止している。	＜健康からてV8における措置＞ 個人番号、5情報等の宛名情報の入手については、厳重に入館・入退室管理が行われているデータセンター内のサーバー間通信に限定することにより、情報漏えい・紛失等を防止している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムとDX審査支払機構の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 ・健康管理システムは、予予請求システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。	事前	システム更新等に伴う重要な変更
	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: 目的を超えた紐付け、事務に必要な情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	保健情報管理システムTIARAは、事務に関係のない情報との紐付けはできない。	健康からてV8は、事務に関係のない情報との紐付けはできない。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予予請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予予請求システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。	事前	システム更新等に伴う重要な変更
	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: 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 具体的な管理方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市は、予予請求システムのアクセス権限を管理する管理者を定める。 ・予予請求システムのログインはユーザID・パスワードで行う。 ・予予請求システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予予請求システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム(各業務システム)から予予請求システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。	事前	システム更新等に伴う重要な変更
	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: 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 アクセス権限の発効・失効の管理 具体的な管理方法	人事異動や権限変更があった場合は、新しく権限を付与する者および権限を失効させる者について、書面で管理者が決裁し、保健情報管理システムTIARAに内容を反映している。また、権限内容について定期的に確認している。	人事異動や権限変更があった場合は、新しく権限を付与する者および権限を失効させる者について、書面で管理者が決裁し、健康からてV8に内容を反映している。また、権限内容について定期的に確認している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システム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	システム更新等に伴う重要な変更
	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: 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 アクセス権限の管理 具体的な管理方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・共用IDは発行せず、必ず個人に対し、ユーザーIDを発行する。 ・管理者が定期的に管理表を確認し、必要に応じて見直しを行う。	事前	システム更新等に伴う重要な変更
	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: 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 特定個人情報の使用の記録 具体的な方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・本市は、システム上の操作のログを取得し、操作ログを定期的に確認する。	事前	システム更新等に伴う重要な変更

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: 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	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・本市は、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。	事前	システム更新等に伴う重要な変更
	Ⅲ特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク4: 特定個人情報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	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・既存システム(各業務システム)から特定個人情報を出出したCSVファイルを予予請求システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・本市の既存システム(各業務システム)から予予請求システムへの特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線(LGWAN又はその他の閉域網回線)を利用した接続のみが認められる。 ・予予請求システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。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	システム更新等に伴う重要な変更
	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	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 本市は、予予請求システムの利用・情報連携業務及び運用保守業務における特定個人情報の取扱いを兵庫県国保連合会に委託し、兵庫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	システム更新等に伴う重要な変更
	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 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	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・本市がアクセス権限の管理状況を確認できる。 ・本市は、アクセス権限を付与する者を必要最小限に限定する。 ・本市は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本市は、アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再々委託先(PMHキー採番や運用保守)のみに付与される。	事前	システム更新等に伴う重要な変更
	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 特定個人情報ファイルの取扱いの記録 具体的な方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予予請求システムは特定個人情報の取り扱いのログを保存し、本市は特定個人情報に係る操作のログを閲覧・出力できる。 ※再々委託先(PMHキー採番や運用保守)に係る特定個人情報の取扱いログに限られる。	事前	システム更新等に伴う重要な変更

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 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 特定個人情報の提供ルール 委託先から他者への提供に関するルール内容及びルール遵守の確認方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託先（再委託先及び再々委託先を含む。）から他者への提供は行わない。 ・本市は委託契約に基づき、委託先（再委託先及び再々委託先を含む。）から他者への提供が行われていないことを確認できる。	事前	システム更新等に伴う重要な変更
	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 特定個人情報の提供ルール 委託元から委託先間の提供に関するルール内容及びルール遵守の確認方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託先（再委託先及び再々委託先を含む。）には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・本市は委託契約に基づき、委託先（再委託先及び再々委託先を含む。）から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。	事前	システム更新等に伴う重要な変更
	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 特定個人情報の消去ルール ルール内容及びルール遵守の確認方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託契約終了後は予予請求システムに保管していた全ての特定個人情報を国保中央会が消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、本市は消去について国保中央会から報告を受けることができ、それにより消去状況について確認が可能となる。	事前	システム更新等に伴う重要な変更
	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 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	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ 兵庫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開覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業員の明確化 ・従業者に対する監督・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	システム更新等に伴う重要な変更
	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 再委託先による特定個人情報ファイルの取扱いの適切な取扱いの確保 具体的な方法	※前略	※前略 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・再々委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・国保中央会が、再々委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、再々委託の相手方によるセルフチェックを基本とし、必要に応じて国保中央会が訪問確認を行う。 ・点検後に改善事項がある場合は、国保中央会が改善指示及び改善状況のモニタリングを行う。 ・国保中央会は、点検結果について兵庫県国保連合会及び本市に年1回報告を行う。	事前	システム更新等に伴う重要な変更

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 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 その他の措置の内容	ー	＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。	事前	システム更新等に伴う重要な変更
	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：特定個人情報の漏えい・滅失・毀損リスク ⑤ 物理的対策 具体的な対策の内容	＜本市における措置＞ (略) ＜中間サーバー・プラットフォームにおける措置＞ ① 中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。	＜本市における措置＞ (略) ＜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。 ＜中間サーバー・プラットフォームにおける措置＞ ① 中間サーバー・プラットフォームは、ISMAPのリストに登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・ISO/IEC27017、ISO/IEC27018の認証を受けている。 ・日本国内でデータを保管している。 ＜予予請求システムを活用した情報連携に係る予防接種事務における追加措置＞	事前	システム更新等に伴う重要な変更
			予予請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、ISMAPのリストに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		

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: 特定個人情報の漏えい・滅失・毀損リスク ⑥ 技術的対策 具体的な対策の内容	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ①～③ (略) ④ 中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度 (ISMAP) に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤～⑧ (略)	<本市における措置> (略) <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8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及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。	事前	システム更新等に伴う重要な変更
			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。 <中間サーバー・プラットフォームにおける措置> ①～③ (略) ④ 中間サーバー・プラットフォームは、ISMAPのリストに登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤～⑧ (略) <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> 予予請求システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、ISMAPのリスト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定める技術的対策を満たしている。		
			主に以下の技術的対策を講じている。 ・予予請求システムは論理的に区分された本市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、予予請求システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予予請求システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。		
	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: 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	<団体内統合宛名システム、共通宛名システム、共通基盤システムにおける措置> ・住登者については、住民基本台帳法第14条第1項(住民基本台帳の正確な記録を確保するための措置)の規定に基づき調査等を実施する住民基本台帳と連携することから、正確な情報であることが担保されている。 ・住登外者については、住登者と同様に正確な記録を確保できるよう業務所管課で住民基本台帳ネットワークシステムの情報を確認するなど、正確な情報を管理する。 <保健情報管理システムTIARAにおける措置> ・共通基盤システムより、随時住登者・住登外者を連携することにより、正確な情報を管理する。	<団体内統合宛名システム、共通基盤システムにおける措置> ・住登者については、住民基本台帳法第14条第1項(住民基本台帳の正確な記録を確保するための措置)の規定に基づき調査等を実施する住民基本台帳と連携することから、正確な情報であることが担保されている。 <健康かるてV8における措置> ・住基システムより、随時住登者を連携することにより、正確な情報を管理する。 ・住登外者については、住登者と同様に正確な記録を確保できるよう業務所管課で住民基本台帳ネットワークシステムの情報を確認するなど、正確な情報を管理する。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本特定個人情報ファイルの個人情報は、住基及び住登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	システム更新等に伴う重要な変更

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 手順の内容	<電子媒体における措置> ・保健情報管理システムTIARAの運用期間中においては、原則消去は行わない。 ・保健情報管理システムTIARAや関連機器の入替時においては、新規の電子記録媒体にデータを移行後、電子記録媒体を裁断等の物理的破壊により記録内容が判読することができないよう完全に消去する。 <紙媒体における措置> ・予診票等の紙媒体によるものについては、明石市文書管理規程に基づき保管し、予防接種法において定められている期間(予防接種法施行令第6条の2)経過後、焼却・溶解により破棄する。	<電子媒体における措置> ・健康かるてV8の運用期間中においては、原則消去は行わない。 ・健康かるてV8や関連機器の入替時においては、新規の電子記録媒体にデータを移行後、電子記録媒体を裁断等の物理的破壊により記録内容が判読することができないよう完全に消去する。 <紙媒体における措置> ・予診票等の紙媒体によるものについては、明石市文書管理規程に基づき保管し、予防接種法において定められている期間(予防接種法施行規則第4条)経過後、焼却・溶解により破棄する。 <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・消去が必要となった情報は内部手続を経て消去し、その記録を残す。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日(作成日)を起点として3年が経過した時点で、自動的に削除される。	事前	システム更新等に伴う重要な変更 (紙媒体における措置については、法改正に伴う変更/事後)
	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	※前略	※前略 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、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	システム更新等に伴う重要な変更
	Ⅳ その他のリスク対策 1. 監査 ② 監査 具体的な内容	<本市における措置> (略) <中間サーバー・プラットフォームにおける措置> ①(略) ②政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	<本市における措置> (略) <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。 <中間サーバー・プラットフォームにおける措置> ①(略) ②ISMAPのリストに登録されたクラウドサービス事業者は、定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、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	システム更新等に伴う重要な変更
	Ⅳ その他のリスク対策 2. 従業者に対する教育・啓発 従業者に対する教育・啓発 具体的な方法	※前略	※前略 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、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	システム更新等に伴う重要な変更

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 3. その他のリスク対策	<中間サーバー・プラットフォームにおける措置> ①中間サーバー・プラットフォームを活用することにより、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。	<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また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。 <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォームを活用することにより、ISMAPに登録されたクラウドサービス事業者による高レベルのセキュリティ管理（入退室管理等）、ITリテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用・監視を実現する。 <予予請求システムを活用した情報連携に係る予防接種事務における追加措置>	事前	システム更新等に伴う重要な変更
			・本市は、情報セキュリティポリシーや特定個人情報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。		
	VI評価実施手続 1. 基礎項目評価 ①実施日	令和4年5月24日	令和8年8月1日	事後	誤記による変更
	VI評価実施手続 2. 国民・住民等からの意見の聴取 ①方法	市民意見の提出手続きを定める要綱に基づき、パブリック・コメントによる意見聴取を実施する。パブリック・コメントの実施に際しては、市報「広報あかし」に記事を掲載するとともに、保健予防課、行政情報センター、あかし総合窓口、各市民センター・サービスコーナー及び市ホームページにて全文を閲覧できるようにする。	市民意見の提出手続きを定める要綱に基づき、パブリック・コメントによる意見聴取を実施する。パブリック・コメントの実施に際しては、市報「広報あかし」に記事を掲載するとともに、保健予防課、こども健康課、行政情報センター、各市民センター及び市ホームページにて全文を閲覧できるようにする。	事前	システム更新等に伴う重要な変更
	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	令和4年6月1日から6月30日までの30日間	令和8年9月1日から10月1日までの31日間	事前	システム更新等に伴う重要な変更
	VI評価実施手続 2. 国民・住民等からの意見の聴取 ④主な意見の内容	なし	削除	事前	システム更新等に伴う重要な変更
	VI評価実施手続 2. 国民・住民等からの意見の聴取 ⑤評価書への反映	なし	削除	事前	システム更新等に伴う重要な変更
	VI評価実施手続 3. 第三者点検 ①実施日	令和4年7月8日	削除	事前	システム更新等に伴う重要な変更
	VI評価実施手続 3. 第三者点検 ③結果	特定個人情報保護評価指針の審査の観点に照らし、適合性及び妥当性ともに基準を満たしていると判断された。	削除	事前	システム更新等に伴う重要な変更