

特定個人情報保護評価書(重点項目評価書)

評価書番号	評価書名
8	予防接種関係事務 重点項目評価書

個人のプライバシー等の権利利益の保護の宣言

甲府市は、予防接種関係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

予防接種関係事務では、運用・保守の一部を外部業者に委託しているため、業者選定の際に業者の情報保護管理体制を確認し、併せて秘密保持に関しても契約に含めることで万全を期している。また、内部による不正利用の防止のため、パスワードと生体による二要素認証を導入し、システムの操作者を限定している。

評価実施機関名

甲府市長

公表日

令和8年10月20日

項目一覧

I 基本情報
II 特定個人情報ファイルの概要
(別添1) 特定個人情報ファイル記録項目
III リスク対策
IV 開示請求、問合せ
V 評価実施手続
(別添2) 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	予防接種関係事務
②事務の内容	・予防接種法に基づき、予防接種手帳(予診票)の交付、予防接種の実施、予防接種の結果管理、実費の徴収、給付の支給を実施する。 ・特定個人情報ファイルは、行政手続きにおける特定の個人を識別するための番号の利用等に関する法律(以下「番号法」という)及び予防接種法に基づき、以下の事務において、収集を行う。 ①予防接種手帳(予診票の綴り:生後1か月児を対象)や助成券の交付 ②予防接種の結果入力 ③予防接種対象者への個別通知 ④実費の徴収 ⑤予防接種費用の償還払い及び助成 ⑥予防接種台帳の管理 ⑦予防接種実施依頼書の送付 ⑧予防接種実施報告書の送付 ⑨予防接種証明書の交付 ⑩健康被害救済の給付 ⑪窓口や郵送での書類の受入、サービス検索・電子申請機能での受領 ・予診情報・予防接種記録管理/請求支払システムを活用した情報連携に係る予防接種事務を行う。内容は以下のとおりである。 ①情報連携のため、予診情報・予防接種記録管理/請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録する。 ②住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 ③住民が予防接種時に、従来の紙の予診票に代えて、タブレットに搭載された医療機関用アプリ等においてマイナンバーカードを用いることにより、医療機関は住民が事前に入力した予診票情報、接種記録の取得/閲覧/入力が可能となる。 ④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	[10万人以上30万人未満] <選択肢> 1) 1,000人未満 3) 1万人以上10万人未満 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	健康管理システム(予防接種)
②システムの機能	帳票出力処理: ・予診票出力 各予防接種の対象者に対して、予診票を出力する。 ・未接種者一覧出力 予防接種対象者のうち、未接種であるものを抽出、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 [☐] 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 (予診情報・予防接種記録管理/請求支払システム)

システム2～5

システム2

①システムの名称	団体内統合宛名システム	
②システムの機能	・団体内統合宛名番号管理機能 団体内統合宛名番号の付番を行う。 団体内統合宛名番号と既存業務システムの宛名番号とを紐付けて管理する。 ・宛名情報管理機能 氏名・住所などの基本5情報を団体内統合宛名番号に紐付けて管理する。 ・中間サーバー連携機能 中間サーバーとのオンラインデータ連携、オフラインデータ連携用の媒体作成を行う。	
③他のシステムとの接続	☒ 情報提供ネットワークシステム ☐ 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	予診情報・予防接種記録管理／請求支払システム
②システムの機能	＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ ①予防接種関連データの登録機能 本市区町村は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市区町村で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・予防接種記録管理／請求支払システムに登録する。また、Public Medical Hubを経由して医療情報基盤・診療報酬審査支払機構（以下、「DX審査支払機構」という。）の医療保険者等向け中間サーバーと連動し、PMHキーを自動採番する。すでにPMHキーが採番済みの個人番号であれば、採番は行わずに既存のPMHキーを利用する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 予診情報・予防接種記録管理／請求支払システムは、マイナポータルからの予診情報・予防接種記録管理／請求支払システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予診情報・予防接種記録管理／請求支払システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナンバーカードの電子証明書のシリアル番号に紐づくPMH仮名識別子を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐づく接種記録・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、予診情報・予防接種記録管理／請求支払システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐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ンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリは、予診情報・予防接種記録管理／請求支払システムへ本人確認情報を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐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に提供する。また、医療機関が接種記録の入力画面から情報を入力することにより、予診情報・予防接種記録管理／請求支払システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐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 予診情報・予防接種記録管理／請求支払システムは接種記録等の情報を予防接種DBに連携し、予防接種DBにおいて予防接種の有効性・安全性等の調査・研究を行う。予診情報・予防接種記録管理／請求支払システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐付けて予診情報・予防接種記録管理／請求支払システムに連携する。

③他のシステムとの接続	☐ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☐ 宛名システム等 ☐ 税務システム ☐ その他（健康管理システム、マイナポータル、医療機関アプリ、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム、電子カルテ等、サービス検索・電子申請機能）
システム4	
①システムの名称	中間サーバ
②システムの機能	符号管理機能 符号管理機能は情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「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。 ・情報照会機能 情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会及び情報提供受領（照会した情報の受領）を行う。 ・情報提供機能 情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報（連携対象）の提供を行う。 ・既存システム接続機能 中間サーバと既存システム、宛名システム及び住民記録システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携する。 ・情報提供等記録管理機能 特定個人情報（連携対象）の照会、又は提供があった旨の情報提供等記録を作成し、管理する。 ・情報提供データベース管理機能 特定個人情報（連携対象）を副本として、保持・管理する。 ・データ送受信機能 中間サーバと情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会、情報提供、符号取得のための情報等について連携する。 ・セキュリティ管理機能 ・職員認証・権限管理機能 中間サーバを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報（連携対象）へのアクセス制御を行う。 ・システム管理機能 バッチ処理の状況管理、業務統計情報の集計、稼働状態の通知、保管切れ情報の削除を行う。
③他のシステムとの接続	☒ 情報提供ネットワークシステム ☐ 庁内連携システム ☐ 住民基本台帳ネットワークシステム ☐ 既存住民基本台帳システム ☒ 宛名システム等 ☐ 税務システム ☐ その他（ ）
システム5	
①システムの名称	サービス検索・電子申請機能
②システムの機能	・【住民向け機能】自らが受けることができるサービスをオンラインで検索及び申請ができる機能。 ・【地方公共団体向け機能】住民が電子申請を行った際の申請データ取得画面又は機能を地方公共団体に公開する機能。
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（e-Gov電子申請サービス）
システム6～10	
システム11～15	
システム16～20	

3. 特定個人情報ファイル名	
予防接種情報ファイル	
4. 個人番号の利用 ※	
法令上の根拠	・番号法第9条第1項及び別表14の項 ・行政手続きにおける特定の個人を識別するための番号の利用等に関する法律別表の主務省令で定める事務を定める命令第10条 ・番号法第19条第16号(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ワクチン接種記録システムを用いた情報提供・照会のみ) ・番号法第19条第6号(委託先への提供)
5. 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	番号法第19条第8号に基づく主務省令第2条の表 (情報提供の根拠): 25,26,153,154の項 (情報照会の根拠): 25,27,28,29,153の項
6. 評価実施機関における担当部署	
①部署	医務感染症課
②所属長の役職名	医務感染症課長
7. 他の評価実施機関	

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	
予防接種情報ファイル	
2. 基本情報	
①ファイルの種類 ※	[システム用ファイル] <選択肢> 1) システム用ファイル 2) その他の電子ファイル(表計算ファイル等)
②対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
③対象となる本人の範囲 ※	予防接種法施行令第1条の3に定められた対象者(接種を受ける時点で当市に住所を有する者)及び同令第6条の2に定められた記録を保有する者
その必要性	予防接種法に基づき、年齢、その他ワクチンの接種状況に基づき適切に予防接種を実施し、その記録を保持するため。
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 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る [☐] その他 (予防接種事務) ・予防接種記録情報
	・識別情報 個人番号: 対象者を正確に特定するために保有する。 その他識別情報: 当市において、個人を一意に識別するために独自の識別番号を保有する。(以降、宛番号と表記) ・連絡先等情報 予防接種手帳(予診表)等の送付先情報として保有する。 ・業務関係情報 予防接種の適切な実施及び予防接種記録を適正に管理するために保有する。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・識別情報(その他識別情報) PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5…予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。 ・業務関係情報(その他) 予防接種記録情報…(予防接種事務の適切な実施にあたり必要となる情報を管理し、)予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。
	その妥当性
全ての記録項目	別添1を参照。
⑤保有開始日	平成27年10月
⑥事務担当部署	医務感染症課

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、生活福祉課) ☐ 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 (他市区町村長) ☐ 民間事業者 (予防接種実施医療機関) ☐ 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、サービス検索・電子申請機能)
③使用目的 ※		本人確認、接種対象者を正確に把握するため。
④使用の主体	使用部署	医務感染症課
	使用者数	[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑤使用方法		1. 予防接種対象者の管理 以下の対象者について情報の登録(更新)を行う。 ・予防接種の対象となる者 2. 接種結果の管理 以下の対象者について接種結果の登録(更新)を行う。 ・予防接種を受けた者 3. 予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務 ・情報連携のため、本市区町村は、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ・登録後、予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対してオンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予診情報・予防接種記録管理／請求支払システムに伝送する。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予診情報・予防接種記録管理／請求支払システムで共有されることで予診情報・予防接種記録管理／請求支払システムからマイナポータルへの通知、マイナポータルや医療機関用アプリから予診情報・予防接種記録管理／請求支払システムの予診票情報及び接種記録の取得/閲覧/入力等といった情報連携が可能となる。
	情報の突合	・個人を正確に特定するために個人番号を利用して正確性を担保する。
⑥使用開始日		平成28年1月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	委託する <選択肢> 1) 委託する 2) 委託しない (1) 件	
委託事項1	システムの運用・保守	
①委託内容	健康管理システム(予防接種)の運用・保守	
②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	
③委託先名	株式会社電算	
再委託	④再委託の有無 ※	再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	契約書上に明記されており、協力事業者申請書を提出し承認する。
	⑥再委託事項	健康管理システム(予防接種)の運用・保守
委託事項2～5		
委託事項2	予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱	
①委託内容	予診情報・予防接種記録管理／請求支払システムの利用・情報連携業務及び運用保守業務	
②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	
③委託先名		
再委託	④再委託の有無 ※	再委託する <選択肢> 1) 再委託する 2) 再委託しない
	⑤再委託の許諾方法	書面又は電磁的方法による承諾
	⑥再委託事項	<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・予診情報・予防接種記録管理／請求支払システムの運用保守 ・PMHキーの採番及びPMHキーを介した医療機関用アプリ・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。
委託事項6～10		
委託事項11～15		
委託事項16～20		

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	[☐] 提供を行っている (2) 件 [] 移転を行っている () 件 [] 行っていない
提供先1	都道府県知事及び市区町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表:25,153,154の項
②提供先における用途	予防接種法及び新型インフルエンザ等対策特別措置法による予防接種の実施に関する情報であって主務省令で定めるもの
③提供する情報	予防接種事業関係情報であって主務省令で定めるもの
④提供する情報の対象となる本人の数	[10万人以上100万人未満] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤提供する情報の対象となる本人の範囲	「2.基本情報③対象者となる本人の範囲」と同じ
⑥提供方法	[☐] 情報提供ネットワークシステム [] 電子メール [] フラッシュメモリ [] その他 () [] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	情報提供ネットワークシステムを通じて特定個人情報の提供依頼の都度
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
①法令上の根拠	
②移転先における用途	
③移転する情報	
④移転する情報の対象となる本人の数	[] <選択肢> 1) 1万人未満 2) 1万人以上10万人未満 3) 10万人以上100万人未満 4) 100万人以上1,000万人未満 5) 1,000万人以上
⑤移転する情報の対象となる本人の範囲	
⑥移転方法	[] 庁内連携システム [] 電子メール [] フラッシュメモリ [] その他 () [] 専用線 [] 電子記録媒体(フラッシュメモリを除く。) [] 紙
⑦時期・頻度	
移転先2～5	
移転先6～10	
移転先11～15	
移転先16～20	

6. 特定個人情報の保管・消去

保管場所 ※

- ・当市では課税データを磁気ディスクで調整しており、以下に示した条件を満たしているサーバ内にデータとして保管している。
- ・建物及びサーバー室の入口でチェックを行い、サーバーの操作を許可された人だけが入場できる場所にサーバーを設置している。
- ・不正アクセス行為の禁止等に関する法律にいうアクセス制御機能としては、ユーザIDによる識別とパスワードによる認証、さらに認証したユーザに対する認可機能によって、そのユーザがシステム上で利用できることを制限することで、認証(ログイン)、認可(処理権限の付与)、監査(ログ運用)を行っている。

- ・クラウドサービスの利用において、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等の契約をし厳重に管理します。
- ・特定個人情報は、クラウドサービスを利用したデータベース内に保存されます。

- ・システム内のデータは、セキュリティゲートにて入退館管理をしている建物のうち、さらに厳格な入退室管理を行っている区画に設置したサーバ内に保管している。
- ・外部記憶媒体は、施錠できるキャビネットに保管している。
- ・サービス検索・電子申請機能に関しては、常時施錠されたオペレーションルームにて個人番号付電子申請データを管理しており、入退室には指紋認証等の厳重な入退室管理を実施している。
- ・事業者に関しては、事前に本番アクセスの申請を許可された者のみ個人番号付電子申請データベースへのアクセスを可能としている。
- ・サービス検索・電子申請機能は、「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」及び「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」等を遵守の上、日本国内で個人番号付電子申請データを保管している。
- ・e-Gov電子申請サービスに関しては、個人番号付電子申請データに事業者がアクセスできないようにアクセス制御を実施している。
- ・e-Gov電子申請サービスは、「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」及び「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」等を遵守の上、日本国内で個人番号付電子申請データを保管している。

＜ガバメントクラウドにおける措置＞

- ・サーバー等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。
- ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。
- ・日本国内でのデータ保管を条件としていること。
- ・特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存される。

＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞

予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。なお、以下のとおりセキュリティ対策を講じている。

- ・サーバ設置場所等への入退室記録管理、施錠管理
- ・論理的に区分された当市区町村の領域にデータを保管する。
- ・当該領域のデータは、暗号化処理をする。
- ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。
- ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。
- ・日本国内にデータセンターが存在するクラウドサービスを利用している。

＜中間サーバー・プラットフォームにおける措置＞

①中間サーバー・プラットフォームは政府情報システムのためのセキュリティ評価制度(ISMAP)に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。

なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。

- ・ISO/IEC27017、ISO/IEC27018 の認証を受けている。

- ・日本国内でデータを保管している。

②特定個人情報は、クラウドサービス事業者が保有・管理する環境に構築する中間サーバーのデータベース内に保存され、バックアップもデータベース上に保存される。

7. 備考

(別添1) 特定個人情報ファイル記録項目

予防接種情報ファイル

- ※1 個人番号は、宛名番号と紐づけて共通管理システムの情報から参照する。
※2 予防接種結果は種類毎に存在します。

項目名

- 1 対象者
- 2 対象者宛名番号
- 3 対象者個人番号(※1)
- 4 対象者情報
- 5 氏名
- 6 住所
- 7 電話番号
- 8 生年月日
- 9 性別
- 10 続柄
- 11 課税非課税区分
- 12 予防接種結果(※2)
- 13 受付番号
- 14 医療機関
- 15 支払月
- 16 フォロー登録
- 17 実施日
- 18 ロット番号
- 19 接種量
- 20 接種方式
- 21 接種場所
- 22 接種医師
- 23 ワクチン名称
- 24 ワクチンメーカー
- 25 有効日
- 26 予診医療機関
- 27 予診医師
- 28 発行履歴
- 29 発行年度
- 30 検診種類
- 31 発行理由
- 32 発行日
- 33 処理区分
- 34 更新日
- 35 更新時刻
- 36 更新者職員番号

<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加の記録項目>

(1)対象者情報

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

(2)ユーザー情報

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

(3)予診票情報

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

(4)予防接種記録情報

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

Ⅲ リスク対策 ※(7. ②を除く。)

1. 特定個人情報ファイル名		
予防接種情報ファイル		
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）		
リスク： 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	＜運用における措置＞ ・予診票の再発行等、窓口に対象者が来られた際には、本人確認書類等の確認を実施し、対象者以外の情報を入手しないよう事務マニュアルを作成し遵守している。 ・その他、特定個人情報の取り扱いに関しては当市セキュリティポリシーに準ずる。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療機関の受付窓口で本人確認の後、医療機関用アプリ等又は顔認証端末でマイナンバーカードを利用した認証により本人の情報のみが対象者として連携される。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、マイナンバーカードを利用した認証により、本人以外からの情報の入力を防止する。 ・既存事務において本人確認を行った個人番号を既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムに連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。 ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予診情報・予防接種記録管理／請求支払システムへは、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステムの的に制御している。 ・医療機関から医療機関用アプリを介して入力される際は、定められたインターフェース仕様に沿って決められたデータ項目のみが連携されるようシステム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。 ＜サービス検索・電子申請機能における措置＞ 【対象者以外の情報の入手を防止するための措置の内容】 ・マニュアルやWeb上で個人番号の提出が必要な者の要件を明示・周知し、対象以外の情報の入手を防止する。 ・申請時に個人番号付電子申請データに電子証明書を付与することで、本人以外のなりすましを防止する。 【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】 ・住民がサービス検索・電子申請機能の画面の誘導に従いサービスを検索し申請フォームを選択して必要情報を入力することとなるが、画面での誘導を簡潔に行うことで、異なる手続に係る申請や不要な情報を送信してしまうリスクを防止する。	
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

リスク: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:

- ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予診情報・予防接種記録管理／請求支払システムへは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目(PMHキーと個人番号)のみが返却されるようシステムの的に制御している。
- ・予診情報・予防接種記録管理／請求支払システムのデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。
- ・紐付け誤り防止機能により、誤った情報が紐付けられるリスクを低減する。

リスク:入手した特定個人情報が不正確であるリスク

リスクに対する措置の内容:

- ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。
- ・個人番号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。
- ・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:入手の際に特定個人情報が漏えい・紛失するリスク

リスクに対する措置の内容:

- ・予診情報・予防接種記録管理／請求支払システムとDX審査支払機構の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。
- ・健康管理システムは、予診情報・予防接種記録管理／請求支払システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。

＜サービス検索・電子申請機能における措置＞

【不適切な方法で入手が行われるリスクへの措置】

- ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、のちに署名検証も行われるため、本人からの情報のみが送信される。
- ・サービス検索・電子申請機能の画面の誘導において住民に何の手続きを探し電子申請を行いたいのか理解してもらいながら操作をしていただき、たどり着いた申請フォームが何のサービスにつながるものかを明示することで、住民に過剰な負担をかけることなく電子申請を実施いただけるよう措置を講じている。

【入手した特定個人情報が不正確であるリスクへの措置】

- ・住民がサービス検索・電子申請機能から個人番号付電子申請データを送信するためには、個人番号カードの署名用電子証明書による電子署名を付すこととなり、電子署名付与済の個人番号付電子申請データを受領した地方公共団体は署名検証(有効性確認、改ざん検知等)を実施することとなる。これにより、本人確認を実施する。

【入手した特定個人情報が漏えい・紛失するリスクへの措置】

- ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えいが起こらないようにしており、さらに通信自体も暗号化している。

3. 特定個人情報の使用		
リスク1: 目的を超えた紐付け、事務に必要なない情報との紐付けが行われるリスク		
リスクに対する措置の内容	<健康管理システム(予防接種)(宛名管理機能)における措置> 宛名管理システムにおいては、個人番号関連業務以外は個人番号にアクセスできないよう、個人番号を宛名情報(5情報)とは物理的に分けて管理しており、番号利用事務(システム)以外では、アクセスできないようにしている。 <健康管理システム(予防接種)における措置> ・番号利用業務以外の部門(条例に規定されていない業務も含む)における照会では、操作権限により、個人番号が参照できないような仕組みが構築されている。(個人番号を物理的に表示しない)また、健康管理システム(予防接種)に対して、不要なアクセスができないよう、適切なアクセス制御対策を実施している。 ・健康管理システム(予防接種)においては、システム操作に関する操作履歴の記録を適切な方法で実施している。 <健康管理システム(予防接種)の運用における措置> ・健康管理システム(予防接種)の稼動するLANでは、外部からの侵入ができないようファイアウォールによる適切なアクセス制御を実施している。 <予診情報・予防接種記録管理/請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・予診情報・予防接種記録管理/請求支払システムにアクセスする本市区町村の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予診情報・予防接種記録管理/請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予診情報・予防接種記録管理/請求支払システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 権限のない者(元職員、アクセス権限のない職員等)によって不正に使用されるリスク		
ユーザ認証の管理	[行っている]	<選択肢> 1) 行っている 2) 行っていない
具体的な管理方法	<健康管理システム(予防接種)における措置> ・ユーザIDによる識別とパスワードによる認証を実施しており、認証後は利用機能の認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、不正利用が行えない対策を実施している。 ・システムの利用できる端末をシステムで管理することにより、不要な端末からの利用ができないような制限を実施している。 <健康管理システム(予防接種)の運用における措置> ・不正アクセス行為を防ぐ措置として、外部からの侵入を防ぐためのファイアウォールの設置とウィルス対策ソフトの導入を行っている。 <予診情報・予防接種記録管理/請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市区町村は、予診情報・予防接種記録管理/請求支払システムのアクセス権限を管理する管理者を定める。 ・予診情報・予防接種記録管理/請求支払システムのログインはユーザID・パスワードで行う。 ・予診情報・予防接種記録管理/請求支払システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予診情報・予防接種記録管理/請求支払システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム(各業務システム)から予診情報・予防接種記録管理/請求支払システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。 <サービス検索・電子申請機能における措置> ・サービス検索・電子申請機能を LGWAN接続端末上で利用する必要がある職員を特定し、個人ごとのユーザIDを割り当てるとともに、IDとパスワードによる認証を行う。 ・なりすましによる不正を防止する観点から共用 IDの利用を禁止する。	

その他の措置の内容	＜サービス検索・電子申請機能における措置＞ 【アクセス権限の発効・失効の管理】 ・サービス検索・電子申請機能のアクセス権限の発効・失効については、以下の管理を行う。 ①発効の管理 ・アクセス権限が必要となった場合、ユーザーID管理者が事務に必要な情報にアクセスできるユーザーIDを発効する。 ・ユーザーID管理者が各事務に必要なアクセス権限の管理表を作成する。 ・アクセス権限の付与を必要最低限とする。 ②失効の管理 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、当該ユーザーIDを失効させる。 【アクセス権限の管理】 定期的にユーザーID一覧をシステムより出力し、アクセス権限の管理表と突合を行い、アクセス権限の確認及び不正利用の有無をユーザーID管理者が確認を行う。また、不要となったユーザーIDやアクセス権限を速やかに変更又は削除する。 【特定個人情報の使用の記録】 ・サービス検索・電子申請機能へのアクセスログ、システムへのアクセスログ、操作ログの記録を行い、操作者個人を特定できるようにする。 ・アクセスログ及び操作ログは、改ざんを防止するため、不正プロセス検知ソフトウェアにより、不正なログの書き込み等を防止する。 ・定期的に操作ログをチェックし、不正とみられる操作があった場合、操作内容を確認する。
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

リスク: 従業者が事務外で使用するリスク

リスクに対する措置の内容:

＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞

- ・本市区町村は、特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、事務外の使用を防止している。
- ・委託業務については、委託先との契約により、委託業者が従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。本市区町村は、当該教育の実施について履行確認を行う。再委託先においても同様の取扱とする。
- ・本市区町村は、操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、事務外での使用を防止する。

リスク: 特定個人情報ファイルが不正に複製されるリスク

リスクに対する措置の内容:

＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞

- ・既存システム(各業務システム)から特定個人情報を抽出したCSVファイルを予診情報・予防接種記録管理／請求支払システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。
- ・本市区町村の既存システム(各業務システム)から予診情報・予防接種記録管理／請求支払システムへの特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線(LGWAN又はその他の閉域網回線)を利用した接続のみが認められる。
- ・予診情報・予防接種記録管理／請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。
- ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。

＜サービス検索・電子申請機能における措置＞

【従業者が事務外で使用するリスクへの措置】

- ・サービス検索・電子申請機能へのアクセスできる端末を制限する。
- ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定されたUSBメモリ等のみを使用する。
- ・外部記憶媒体内のデータは暗号化する。

【特定個人情報ファイルが不正に複製されるリスクへの措置】

- ・サービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータについて、改ざんや業務目的以外の複製を禁止するルールを定め、ルールに従って業務を行う。
- ・アクセス権限を付与された最小限の職員等だけが、個人番号付電子申請等のデータについて、LGWAN接続端末への保存や外部記憶媒体への書き出し等ができるようにシステムの的に制御する。
- ・外部記憶媒体にサービス検索・電子申請機能から取得した個人番号付電子申請データ等のデータを複製する場合、使用管理簿に記載し、事前に責任者の承認を得たうえで複製する。なお、外部記憶媒体は限定されたUSBメモリ等のみを使用する。
- ・外部記憶媒体内のデータは暗号化する。

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
リスク： 委託先における不正な使用等のリスク		
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	[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	個人情報の秘密の保持義務、管理に関する重要項目等の報告、適正管理、持ち出しの制限、複製もしくは複写の制限 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 山梨県国保連合会及び国保中央会は特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項	
再委託先による特定個人情報ファイルの適切な取扱いの担保	[十分に行っている] <選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない 4) 再委託していない	
具体的な方法	情報セキュリティ事故防止を目的とし、委託事業者が再委託先に「秘密情報管理実施要領」を遵守させている。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・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、点検結果について山梨県国保連合会及び本市区町村に年1回報告を行う。	
その他の措置の内容	<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。	
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置		

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[] 提供・移転しない
リスク：不正な提供・移転が行われるリスク		
特定個人情報の提供・移転に関するルール	[定めていない]	<選択肢> 1) 定めている 2) 定めていない
ルールの内容及びルール遵守の確認方法		
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。)におけるその他のリスク及びそのリスクに対する措置		

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では、個人番号利用事務(システム)からの接続には認証を必須とし、個人番号利用事務(システム)以外のアクセスはできない対策を実施している。 ・団体内統合宛名システムでは、ユーザIDによる認証と認可機能により、そのユーザがシステム上で利用可能な機能を制限することで、個人番号関連業務関係者以外はアクセスできないよう対策を実施している。		
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている		
リスク2: 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では、個人番号利用事務(システム)からの接続には認証を必須とし、個人番号利用事務(システム)以外のアクセスはできない対策を実施している。 ・団体内統合宛名システムでは、ユーザIDによる認証と認可機能により、そのユーザのシステム上で利用可能な機能を制限することで、不正利用が行えない対策を実施している。		
リスクへの対策は十分か	[十分である] <選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている		
情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置			
<中間サーバー・プラットフォームにおける措置> ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク(総合行政ネットワーク等)を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理(アクセス制御)しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。			

7. 特定個人情報の保管・消去

リスク： 特定個人情報の漏えい・滅失・毀損リスク

①事故発生時手順の策定・周知	[十分に行っている]	<選択肢> 1) 特に力を入れて行っている 2) 十分に行っている 3) 十分に行っていない
②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		
その他の措置の内容	<サービス検索・電子申請機能における措置> 【物理的対策】 ・LGWAN接続端末については、業務時間内のセキュリティワイヤー等による固定、操作場所への入退室管理、業務時間外の施錠できるキャビネット等への保管、などの物理的対策を講じている。 ・外部記憶媒体については、限定された USBメモリ等以外の利用不可、施錠できるキャビネット等への保管、使用管理簿による管理、などの安全管理措置を講じている。 ・e-Gov電子申請サービスは、日本国内でデータを保管し、「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」及び「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」等を遵守することで、特定個人情報の漏えい・滅失・毀損リスクを防止している。 【技術的対策】 ・LGWAN接続端末へのウイルス検出ソフトウェア等の導入により、ウイルス定義ファイルの定期的な更新及びウイルスチェックを行い、マルウェア検出を行う。 ・サービス検索・電子申請機能と地方公共団体との間は、専用線であるLGWAN回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。 ・サービス検索・電子申請機能と e-Gov電子申請サービスは、専用線であるGSS G-Net回線を用いた通信を行うことで、外部からの盗聴、漏えい等が起こらないようにしており、さらに通信自体も暗号化している。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

特定個人情報の保管・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

<ガバメントクラウドにおける措置>

【物理的対策】

- ・ガバメントクラウドについては政府情報システムのセキュリティ制度 (ISMAP) のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可されたものだけがアクセスできるよう適切な入退室管理策を行っている。
- ・事前に許可されていない装置等に関しては、外部に持出できないこととしている。

【技術的対策】

- ・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。
- ・地方公共団体が委託したアプリケーション開発事業者等は、ガバメントクラウド事業者が提供するマネージドサービスにより、ネットワークアクセシビリティ、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。
- ・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。
- ・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。
- ・地方公共団体が委託したアプリケーション開発事業者等は、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。
- ・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。
- ・地方公共団体やアプリケーション開発事業者等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。
- ・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。

【物理的対策】

<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。

【技術的対策】

<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。

リスク: 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:

<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置>

- ・本特定個人情報ファイルの個人情報は、住基及び住民登録外者の異動情報を取得し、内部番号を基に最新の情報に反映されるため、古い情報のまま保管され続けるリスクは存在しない。

リスク: 特定個人情報が消去されずいつまでも存在するリスク

リスクに対する措置の内容:

<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置>

- ・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。

<サービス検索・電子申請機能における措置>

【特定個人情報が古い情報のまま保管され続けるリスクへの措置】

- ・LGWAN接続端末は、基本的には、個人番号付電子申請データの一時保管として使用するが、一時保管中に再申請や申請情報の訂正が発生した場合には古い情報で審査等を行わないよう、履歴管理を行う。

【特定個人情報が消去されずいつまでも存在するリスクへの措置】

- ・LGWAN接続端末については、業務終了後の不要な個人番号付電子申請データ等の消去について徹底し、必要に応じて管理者が確認する。
- ・外部記憶媒体については、定期的に内部のチェックを行い不要なデータの確認を行い、廃棄する場合は管理者の承認を得て行う手順を定めている。
- ・サービス検索・電子申請機能に保存された個人番号付電子申請データは、申請から5営業日後に自動的に論理削除され、申請から60日後に自動的に物理削除される。
- ・e-Gov電子申請サービスに保存された個人番号付電子申請データは、サービス検索・電子申請機能にデータ取得後、7日後に自動的に削除される。

8. 監査	
実施の有無	☐ 自己点検 ☐ 内部監査 ☐ 外部監査
9. 従業員に対する教育・啓発	
従業員に対する教育・啓発	☐ 十分に行っている ☐ 十分に力を入れて行っている ☐ 十分に力を入れていない
具体的な方法	・毎年、情報セキュリティに関する教育及び研修を実施する。 ・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。 ・委託業者に対しては、業務委託契約書に個人情報保護に関する秘密保持条項を明記し、契約を締結している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 本市区町村は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、適切な指導を行う。
10. 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データの取扱いについて委託を受けるアプリケーション開発事業者等が責任を有する。 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業の場合は、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アプリケーション開発事業者等が対応するものとする。 ＜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リテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 本市区町村は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、適切な指導を行う。	

IV 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	甲府市 保健衛生部生活衛生室医務感染症課 400-0858 山梨県甲府市相生2-17-1 問い合わせ先電話番号 055-237-2587
②請求方法	甲府市個人情報の保護に関する法律(令和4年条例第35号)の規定に基づき、開示・訂正・利用停止請求を受け付ける。
③法令による特別の手続	
④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	甲府市 保健衛生部生活衛生室医務感染症課 400-0858 山梨県甲府市相生2-17-1 問い合わせ先電話番号 055-237-2587
②対応方法	特定個人情報ファイルの取扱いに関する苦情は、口頭又は文書により受け付ける。

V 評価実施手続

1. 基礎項目評価	
①実施日	令和3年6月1日
②しきい値判断結果	[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] <選択肢> 1) 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 2) 基礎項目評価の実施が義務付けられる(任意に重点項目評価を実施) 3) 特定個人情報保護評価の実施が義務付けられない(任意に重点項目評価を実施)
2. 国民・住民等からの意見の聴取【任意】	
①方法	
②実施日・期間	
③主な意見の内容	
3. 第三者点検【任意】	
①実施日	
②方法	
③結果	

(別添2)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6年11月8日	I 1 ②事務の内容	・新型コロナウイルス感染症対策に係る予防接種事務 ①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の登録を行う。 ②予防接種の実施後に接種記録等を登録、管理し、他区市町村へ接種記録の照会・提供を行う。 ③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。		事後	
令和6年11月8日	I 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4	- ワクチン接種記録システム(VRS) ・ワクチン接種記録システムへの接種対象者・接種券発行登録 ・接種記録の管理 ・転出/死亡時等のフラグ設定 ・他市区町村への接種記録の照会・提供 ・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 ・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 ・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	
令和6年11月8日	II 3. 特定個人情報の入手・使用②	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	

令和6年11月8日	Ⅱ 3. 特定個人情報の入手・使用⑤	3. 新型コロナウイルス感染症対策に係る予防接種事務 ・当市への転入者について、転出元市区町村へ接種記録を照会するとともに、接種券の発行のために特定個人情報を使用する。 ・当市からの転出者について、転出先市区町村へ当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。 ・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。 情報の突合 ・新型コロナウイルス感染症対策に係る予防接種事務 当市からの転出者について、当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、当市区町村の接種記録と突合する。		事後	
令和6年11月8日	Ⅱ 4. 特定個人情報ファイルの取扱いの委託 委託事項2	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)(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	

令和6年11月8日	II 5. 特定個人情報ファイルの提供・移転(委託に伴うものを除く。) 提供先2	市区町村長 番号法 第19条第16号 新型コロナウイルス感染症対策に係る予防接種事務 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) 「2.基本情報③対象者となる本人の範囲」と同じ 当市への転入者について、転出元市区町村へ接種記録の照会を行う必要性が生じた都度		事後	
令和6年11月8日	II 6. 特定個人情報の保管・消去	＜ワクチン接種記録システムにおける追加措置＞ ワクチン接種記録システムは、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、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。	・クラウドサービスの利用において、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等の契約をし厳重に管理します。 ・特定個人情報は、クラウドサービスを利用したデータベース内に保存されます。 ＜ガバメントクラウドにおける措置＞ ・サーバー等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ・特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存される。	事前	

令和6年11月8日	Ⅱ 7. 備考	<ワクチン接種記録システムにおける追加措置> ・自機関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を用いて消去することができる。 ・自機関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ため、消去することができない。		事後	
令和6年11月8日	(別添1)ファイル記録項目	<新型コロナウイルス感染症対策に係る予防接種に関する記録項目> ・個人番号 ・宛名番号 ・自治体コード ・接種券番号 ・属性情報(氏名、生年月日、性別) ・接種状況(実施/未実施) ・接種回 ・接種日 ・ワクチンメーカー ・ロット番号 ・ワクチン種類(※) ・製品名(※) ・旅券関係情報(旧姓・別姓・別名、ローマ字氏名、国籍、旅券番号)(※) ・証明書ID(※) ・証明書発行年月日(※) ※ 新型コロナウイルス感染症予防接種証明書の交付に必要な場合のみ		事後	

令和6年11月8日	Ⅲ 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。） 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	＜ワクチン接種記録システムにおける追加措置＞ ・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。 ・ワクチン接種記録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。 ・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	
令和6年11月8日	Ⅲ 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 具体的な管理方法	＜ワクチン接種記録システムにおける追加措置＞ ・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に接続できるが、個人番号にはアクセスできないように制御している。		事後	

令和6年11月8日	Ⅲ 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	＜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住民基本台帳システムや予防接種台帳システムから特定個人情報を抽出したCSVファイルをワクチン接種記録システムへ登録する際には、以下のようになっている。 ・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。 ②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。 ・当市区町村の転入者について、転出元市区町村へ接種記録を照会する場合のみ入手し、使用する。 ・当市区町村からの転出者について、当市区町村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。 ③ワクチン接種記録システムから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6年11月8日	Ⅲ リスク対策 4.特定個人情報ファイルの取扱いの委託 その他の措置内容	〈新型コロナウイルス感染症対策に係る予防接種事務における追加措置〉 当市区町村、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	
------------------	---	--	--	-----------	--

令和6年11月8日	Ⅲ リスク対策 5.特定個人情報の提供・移転 その他の措置内容 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	<ワクチン接種記録システムにおける追加措置> ワクチン接種記録システムでは、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「情報提供等の記録」を入手し、記録の確認をすることができる。 <ワクチン接種記録システムにおける追加措置> ・転出元市区町村への個人番号の提供 当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ため、転出元市区町村へ個人番号を提供するが、 その際は、 ①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を用いて提供する。 ②個人番号と共に転出元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信したとして 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。 ・特定個人情報の提供は、限定された端末(LG-WAN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、必要最小限に限定している。具体的には、当市区町村への転入者について、 転出元市区町村での接種記録を入手するために、転出元市区町村へ個人番号と共に転出元の市区町村コードを提供する 場面に限定している。		事後	
------------------	---	--	--	-----------	--

令和6年11月8日	Ⅲ リスク対策 7.特定個人情報の保管・消去 その他の措置内容	・監視カメラを設置してサーバ設置場所への入退者を特定し、管理している。 ・サーバ設置場所、端末設置場所、記録媒体の保管場所を施錠管理している。 ・ウィルス対策ソフトの定期的パターン更新をしている。 ・不正アクセス防止策として、ファイアウォール、IDP/IPSを導入している。 ＜ワクチン接種記録システムにおける措置＞ 【物理的対策】、【技術的対策】について記載。	＜ガバメントクラウドにおける措置＞ 【物理的対策】及び【技術的対策】を追記 ＜ワクチン接種記録システムにおける措置＞ 【物理的対策】及び【技術的対策】を削除	事前	
令和6年11月8日	Ⅲ リスク対策 9.従事者に対する教育・啓発 その他の措置内容	＜新型コロナウイルス感染症対策に係る予防接種事務における追加措置＞ 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6年11月8日	Ⅲ リスク対策 10.その他のリスク対策	<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> 内閣官房情報通信技術(IT)総合戦略室から发出された「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。	<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データの取扱いについて委託を受けるアプリケーション開発事業者等が責任を有する。 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業の場合は、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アプリケーション開発事業者等が対応するものとする。	事前	
令和6年11月8日	IV V 開示請求、問合せ・評価実施手続 1.特定個人情報の開示・訂正・利用停止請求①	甲府市 福祉保健部保健衛生室医務感染症課 400-0858 山梨県甲府市相生2-17-1 問い合わせ先電話番号 055-237-2587	甲府市 保健衛生部生活衛生室医務感染症課 400-0858 山梨県甲府市相生2-17-1 問い合わせ先電話番号 055-237-2587	事後	
令和6年11月8日	IV V 開示請求、問合せ・評価実施手続 2.特定個人情報ファイルの取扱いに関する問合せ①	甲府市 福祉保健部保健衛生室医務感染症課 400-0858 山梨県甲府市相生2-17-1 問い合わせ先電話番号 055-237-2587	甲府市 保健衛生部生活衛生室医務感染症課 400-0858 山梨県甲府市相生2-17-1 問い合わせ先電話番号 055-237-2587	事後	
令和7年11月18日	I 1 特定個人情報ファイルを取り扱う事務		・予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務の内容 追記	事前	
令和7年11月18日	I 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		予診情報・予防接種記録管理／請求支払システム 追加	事前	
令和7年11月18日	II 2. 基本情報		<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> 追加	事前	
令和7年11月18日	II 3. 特定個人情報の入手・使用		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務 追加	事前	

令和7年11月18日	Ⅱ 4. 特定個人情報ファイルの取扱いの委託		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務 追加	事前	
令和7年11月18日	Ⅱ 6. 特定個人情報の保管・消去		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務 中間サーバー・プラットフォームにおける措置 追加	事前	
令和7年11月18日	(別添1)ファイル記録項目		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加の記録項目 追加	事前	
令和7年11月18日	Ⅲ 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。）		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置 追加	事前	
令和7年11月18日	Ⅲ リスク対策 3. 特定個人情報の使用		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置 追加	事前	
令和7年11月18日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置 追加	事前	
令和7年11月18日	Ⅲ リスク対策 6. 情報共有ネットワークシステムとの接続		中間サーバー・プラットフォームにおける措置 追加	事前	
令和7年11月18日	Ⅲ リスク対策 7. 特定個人情報の保管・消去 その他の措置内容		中間サーバー・プラットフォームにおける措置 追加	事前	
令和7年11月18日	Ⅲ リスク対策 9. 従事者に対する教育・啓発		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置 追加	事前	
令和7年11月18日	Ⅲ リスク対策 10. その他のリスク対策		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務 中間サーバー・プラットフォームにおける措置 追加	事前	
令和8年10月20日	Ⅰ 1 特定個人情報ファイルを取り扱う事務		サービス検索・電子申請機能に係る項目を追加	事前	

令和8年10月20日	I 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		DX審査支払機構、サービス検索・電子申請機能に係る項目を追加	事前	
令和8年10月20日	II 3. 特定個人情報の入手・使用		DX審査支払機構、サービス検索・電子申請機能に係る項目を追加	事前	
令和8年10月20日	II 6.特定個人情報の保管・消去		サービス検索・電子申請機能に係る項目を追加	事前	
令和8年10月20日	III 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。）		紐付け誤り防止機能、サービス検索・電子申請機能に係る項目を追加	事前	
令和8年10月20日	III リスク対策 3. 特定個人情報の使用		サービス検索・電子申請機能に係る項目を追加	事前	
令和8年10月20日	III リスク対策 7.特定個人情報の保管・消去 その他の措置内容		サービス検索・電子申請機能に係る項目を追加	事前	