

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
2	予防接種に関する事務 全項目評価書(案)

個人のプライバシー等の権利利益の保護の宣言

豊橋市は、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、そ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

豊橋市長

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 ※	感染の恐れがある疾病の発生及びまん延を防止し、公衆衛生の向上及び健康の増進を図るため、予防接種法に基づく定期予防接種を実施し、免疫保有率の向上に努める。 また、新型インフルエンザ等感染症のまん延予防の緊急の必要性があるときには、臨時接種または新臨時接種を行う。 予防接種の実施にあたっては、対象者の抽出、接種データの登録・管理及び実費徴収の有無等に関する事務を行い、特定個人情報については、番号法別表14、126の規定により、以下の事務において取り扱う。 ○予防接種法第5条第1項又は第6条第1項若しくは第3項の予防接種の実施に関する事務 ○予防接種法第5条第1項又は第6条第1項の予防接種の実施の指示に関する事務 ○予防接種法第6条第3項の予防接種の実施に必要な協力に関する事務 ○予防接種法第15条第1項(健康被害の救済措置)の給付の支給の請求の受理、その請求に係る事実についての審査又はその請求に対する応答に関する事務 ○予防接種法第15条第1項の給付の支給を受ける権利に係る届出等の受理、その届出等に係る事実についての審査又はその届出等に対する応答に関する事務 ○予防接種法第28条の実費の徴収に関する事務 ○新型インフルエンザ等対策特別措置法(以下、新型インフル特措法という)第28条第1項の規定による指示に基づき行う予防接種に関する事務 ＜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＞ ・本市は、情報連携のため、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 ・住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 ・住民が予防接種時に、従来の紙の予診票に代えて、タブレット等に搭載された医療機関アプリにおいてマイナンバーカードを用いることにより、医療機関は住民が事前に入力した予診票情報、接種記録の取得/閲覧/入力が可能となる。 ・本市は、医療機関から入力された予診票情報、接種記録の取得及び住民への通知が可能となる。
③対象人数	〔 30万人以上 〕 ＜選択肢＞ 1) 1,000人未満 2) 1,000人以上1万人未満 3) 1万人以上10万人未満 4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム

システム1

①システムの名称	健康管理システム
②システムの機能	・対象者抽出機能: 予防接種対象者及び未接種者を抽出する。 ・予防接種入力機能: 個人の予防接種の情報を入力する。 ・予防接種情報取込: 予防接種のパンチデータを取り込む。 ・予防接種照会: 個人、ワクチンごと、全接種などの履歴を照会する。 ・予診票出力: 予診票やクーポン券を印刷する。
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 ☐ 市内連携システム ☐ 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 (生活保護システム、障害者福祉システム、国保年金システム、後期高齢システム、国保年金システムと後期高齢システムからの情報は、予防接種事務では使用しない)

システム2

3 / 37 ページ

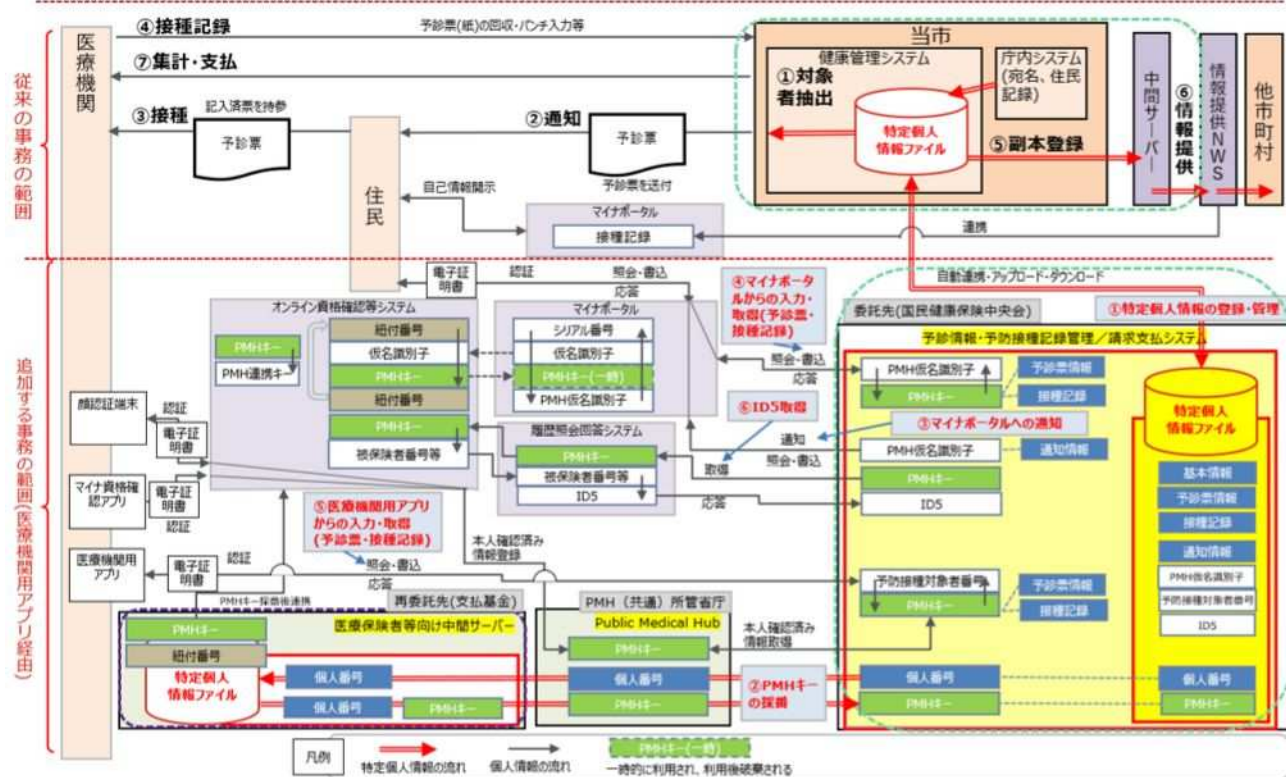
システム4	
①システムの名称	予診情報・予防接種記録管理／請求支払システム
②システムの機能	<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ①予防接種関連データの登録機能 本市は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種動向における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・予防接種記録管理／請求支払システムに登録する。また、Public Medical Hubを経由して社会保険診療報酬支払基金（以下、「支払基金」という。）の医療保険者等向け中間サーバーと連動し、PMHキーを自動採番する。すでにPMHキーが採番済みの個人番号であれば、採番は行わずに既存のPMHキーを利用する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 予診情報・予防接種記録管理／請求支払システムは、マイナポータルからの予診情報・予防接種記録管理／請求支払システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予診情報・予防接種記録管理／請求支払システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナ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（医療機関アプリ） ・本人確認情報の格納機能 予防接種対象者が、顔認証端末又はマイナ資格確認アプリを利用してマイナ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データベースに連携し、予防接種データベースにおいて予防接種の有効性・安全性等の調査・研究を行う。予診情報・予防接種記録管理／請求支払システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐づけて予診情報・予防接種記録管理／請求支払システムに連携する。
③他のシステムとの接続	[] 情報提供ネットワークシステム [] 庁内連携システム [] 住民基本台帳ネットワークシステム [] 既存住民基本台帳システム [] 宛名システム等 [] 税務システム [☒] その他 （健康管理システム、マイナポータル、医療機関アプリ、Public Medical Hub、 履歴調査回答システム、オンライン資格確認等システム）
システム6～10	
システム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. 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把握し、適正な管理・接種勧奨を行うため。 ・対象者の課税状況により、実費徴収の有無の判定を行うため。 ・健康被害が発生した場合に、給付の支給の請求や権利に係る事実についての審査又はその請求等に応答するため
②実現が期待されるメリット	・予防接種の対象者であることの確認及び接種履歴の管理により、未接種者勧奨が可能となり、接種率の向上につながる。 ・転出入時等における効率的な事務が可能となる。
5. 個人番号の利用 ※	
法令上の根拠	番号法第9条第1項 別表14、126 番号法第19条第6号(委託先への提供)
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[実施する] <選択肢> 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	番号法第19条第8号に基づく主務省令 番号法第19条第8号に基づく主務省令第2条の表における情報照会の根拠: 25、27、28、29、153 番号法第19条第8号に基づく主務省令第2条の表における情報提供の根拠: 25、26、153、154
7. 評価実施機関における担当部署	
①部署	健康部保健医療企画課
②所属長の役職名	保健医療企画課長
8. 他の評価実施機関	

(別添1) 事務の内容

予防接種事務の概要 全体図

従来の事務では、①～⑦の流れで健康管理システム・中間サーバに情報が登録・連携される。今回利便性の向上のため、予防接種における住民からの予診票入力及び接種記録の取得、医療機関からの予診票取得、接種記録の入力等のオンライン化を事務の範囲に追加する。追加する事務では、①②の流れで、情報が連携され、住民がマイナポータル経由、医療機関が医療機関用アプリ経由でオンライン化(③④⑤⑥)が実現できる。(緑色部が評価対象の事務、青色部については社会保険診療報酬支払基金(支払基金)がPIAを実施するため評価対象外)



(備考)

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

①特定個人情報の登録・管理

- ・本市は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診情報・予防接種記録管理／請求支払システムにおいて対象者の個人番号を含む対象者情報と予防接種管理情報の紐付け及び登録を行う。(LGWAN回線等経由)
- ・本市は予診情報・予防接種記録管理／請求支払システムから接種記録等、必要な情報を自動連携またはダウンロードし、健康管理システム等への取込を行う。
- ・予診情報・予防接種記録管理／請求支払システムへ登録された個人情報へのアクセスは適切に制御される。

②PMHキー採番

- ・予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対して個人番号を連携することで、オンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼する。
- ・Public Medical Hubは、医療保険者等向け中間サーバを経由しPMHキーを採番して予診情報・予防接種記録管理／請求支払システムに回答する。
- ・医療保険者等向け中間サーバは、PMHキーと個人番号を紐付けて、PMHキーと紐付番号をオンライン資格確認等システムへ連携する。
- ・オンライン資格確認等システムは、紐付番号をキーに仮名識別子とPMHキーを紐付けて、マイナポータルに連携する。
- ・マイナポータルは、新たにPMH用の仮名識別子(PMH仮名識別子)を生成し、シリアル番号、仮名識別子、PMHキーと紐付けて、予診情報・予防接種記録管理／請求支払システムに連携する。(連携後、マイナポータル上からPMHキーは削除される。)以降、③④⑤⑥が可能となる。

③マイナポータルへの通知

- ・予診情報・予防接種記録管理／請求支払システムからマイナポータル経由で住民向けの通知を行うため、本市は予診情報・予防接種

記録管理／請求支払システムを利用してマイナポータルに識別子(PMH仮名識別子)と通知情報を登録する。

④マイナポータルからの入力・取得(予診票・接種記録)

・住民は、マイナポータル経由で予診情報・予防接種記録管理／請求支払システムへの予診票の事前入力や、予診情報・予防接種記録管理／請求支払システムから接種記録や通知情報を閲覧/取得する。

⑤医療機関アプリからの入力・取得(予診票・接種記録)

・医療機関が医療機関アプリを利用し、接種時に住民からマイナンバーカードによる本人確認を経て、事前入力された予診票及び接種記録の閲覧/取得/入力を行う。

⑥ID5取得

・予防接種データベースへの接種記録等の連携時に個人を特定する識別子情報として、予診情報・予防接種記録管理／請求支払システムが履歴照会回答システム経由でID5を取得する。

Ⅱ 特定個人情報ファイルの概要

1. 特定個人情報ファイル名

予防接種情報ファイル

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 ※	予防接種法等関連法令に定められる予防接種の対象者	
	その必要性	予防接種の対象者を把握し、被接種者の接種情報を適正に管理するため
④記録される項目	[10項目以上50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予防接種事務> ・予防接種記録情報
	その妥当性	・個人番号及びその他識別情報：対象者を正確に特定するために保有 ・4情報、連絡先及びその他住民票関係情報： ①予診票を発送する際、正確な住所、連絡先が必要なため。 ②年齢要件によって異なる予防接種の接種可否の判断のため。 ③送付物が返戻された場合等の本人への連絡のため。 ④死亡転出等を把握し、接種対象者からの除外や送付物の抜き取り作業をするため。 ・業務関係情報：接種費用にかかる実費徴収の有無の判定及び接種情報を適正に管理するため <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・識別情報(その他識別情報) PMHキー、PMH仮名識別子、PMH連携キー、予防接種対象者番号、ID5…予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。 ・業務関係情報(その他) 予防接種記録情報…予防接種事務の適切な実施にあたり必要となる情報を管理し、予診情報・予防接種記録管理／請求支払システムが、外部と情報連携するために必要となる。
	全ての記録項目	別添2を参照。
⑤保有開始日	平成27年10月	
⑥事務担当部署	豊橋市保健所 保健医療企画課	

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、市民税課、障害福祉課、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 （ 他自治体 ） [☐] 民間事業者 （ 医療機関 ） [☐] その他 （ 支払基金 ）
②入手方法	[☐] 紙 [☐] 電子記録媒体（フラッシュメモリを除く。） [☐] フラッシュメモリ [☐] 電子メール [☐] 専用線 [☐] 庁内連携システム [☐] 情報提供ネットワークシステム [☐] その他 （ Public Medical Hub、医療機関アプリ、マイナポータル ）
③入手の時期・頻度	・住民基本情報は日次、税情報は月次、障害者データは年11回 ・転入者の予防接種記録や実費の徴収について照会が必要などき ・予防接種健康被害救済申請の都度 ・転入時に転出元市区町村への接種記録の照会が必要になる都度 ・他市区町村から転出者の本市での接種記録の照会を受ける都度 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ ・予診情報・予防接種記録管理／請求支払システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・本市が予診情報・予防接種記録管理／請求支払システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本市が個人情報を入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレット等に搭載された医療機関アプリ又は医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。
④入手に係る妥当性	・庁内連携システムを利用して入手する住民基本情報や障害者情報については、法令等に基づく接種対象者であることの確認、税情報については、接種費用にかかる実費徴収の有無の判定を行うものである。 ・予防接種記録については、接種対象者が接種時の年齢、月齢に応じたスケジュールにより接種することが求められており、市町村が適切な勧奨を行うにあたり、新たに転入してきた者の転入前の接種記録を把握することは必要である。 ・情報提供ネットワークを利用して入手する地方税情報については、本人等からの申請を受けた都度入手する必要がある、実費徴収の有無について確認を行うものである。（本人の同意を得られた場合のみ） ・予防接種健康被害救済請求にかかる情報の入手は、本人等からの申請によるものである。（個人番号は請求書により入手） ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ （PMHキー採番処理依頼時に入手される特定個人情報） ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 （その他：個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結び付き特定個人情報となる情報） 本市が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入手し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証（本人確認）の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレット等に搭載された医療機関アプリを用いた予診票の確認・接種記録がオンライン化す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、医療機関アプリ又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。

⑤本人への明示		・本人及び代理人から入手する情報は、書面にて利用目的を明示する。 ・住民基本情報の入手については、番号法及び予防接種施行規則により明示されている。 なお、H28年12月14日付け厚生労働省事務連絡において、「予防接種記録については、本人の同意なく、市町村が他の市町村に提供できることとされており、市町村間での情報連携にあたって、その都度本人の同意を取得することは必須であるとは考えていない」とされている。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・本人又は本人の代理人から入手する情報については、利用目的を明示した上で入手している。マイナポータル及び医療機関アプリ又は医療機関での顔認証端末では、本人又は本人の代理人が画面に表示された利用目的を確認して、本人確認することにより入手する。
⑥使用目的 ※		予防接種の実施にあたり、本人の資格確認(住所、年齢等)や、実費徴収の有無を適正かつ公平に決定する。 また、接種記録の保管・管理を行い、未接種者に対する接種勧奨を実施する。
	変更の妥当性	
⑦使用の主体	使用部署※	健康部保健医療企画課
	使用者数	[10人以上50人未満] <選択肢> 1) 10人未満 2) 10人以上50人未満 3) 50人以上100人未満 4) 100人以上500人未満 5) 500人以上1,000人未満 6) 1,000人以上
⑧使用方法 ※		①対象者の資格(住所、年齢)確認 本人等からの申請及び医療機関からの接種記録について、住民基本情報をもとに対象者であることを確認する。 ②接種記録の保管・管理 健康管理システムに医療機関や本人等からの接種情報を登録し、保管・管理を行う。 ③接種費用にかかる実費徴収の有無の確認 本人等の申請に基づき、地方税関係情報を確認し、実費徴収の有無を確認する。 ④未接種者への接種勧奨 接種記録をもとに、対象年齢の間に接種するよう勧奨ハガキを送る。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・情報連携のため、本市は、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ・登録後、予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対してオンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予診情報・予防接種記録管理／請求支払システムに応答する。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予診情報・予防接種記録管理／請求支払システムで共有されることで予診情報・予防接種記録管理／請求支払システムからマイナポータルへの通知、マイナポータルや医療機関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 ※	・窓口業務において、本人確認書類に個人番号カードが使われた際に個人番号で単件検索を行う ・住民記録システムからの個人番号の入手は宛名番号により突合する ・情報提供ネットワークシステムを経由する情報は、符号と団体内統合宛名で突合する
	情報の統計分析※	個人を特定する統計は行わない。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・特定の個人を判別するような情報の統計や分析は行わない。
	権利利益に影響を与え得る決定 ※	予防接種費用にかかる実費徴収の有無の決定
⑨使用開始日		平成28年1月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※	☐ 委託する ☐ 委託しない (2) 件	
委託事項1	健康管理システムの開発・運用保守及び制度改正に伴う改修業務	
①委託内容	健康管理システムの開発・運用支援・保守	
②取扱いを委託する特定個人情報ファイルの範囲	☐ 特定個人情報ファイルの全体	
対象となる本人の数	☐ 10万人以上100万人未満	
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	
その妥当性	システムの安定稼働のため、高度で専門的な知識を有する民間事業者に委託している。	
③委託先における取扱者数	☐ 10人未満	
④委託先への特定個人情報ファイルの提供方法	☐ 専用線 ☐ 電子メール ☐ 電子記録媒体(フラッシュメモリを除く。) ☐ フラッシュメモリ ☐ 紙 ☐ その他 (システムの直接操作)	
⑤委託先名の確認方法	豊橋市情報公開条例(平成8年豊橋市条例第2号)に基づく開示請求で確認できる。	
⑥委託先名	株式会社ヒミカ、株式会社両備システム	
再委託	⑦再委託の有無 ※	☐ 再委託する
	⑧再委託の許諾方法	特別な理由がある場合には、事前に書面による本市の承諾を得ることを条件に再委託を認めている。本市では再委託の必要性や業務内容、再委託先のセキュリティ管理体制を確認した上で許諾している。
	⑨再委託事項	運用支援業務
委託事項2～5		
委託事項2	予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱	
①委託内容	予診情報・予防接種記録管理／請求支払システムの利用・情報連携業務及び運用保守業務	
②取扱いを委託する特定個人情報ファイルの範囲	☐ 特定個人情報ファイルの一部	
対象となる本人の数	☐ 10万人以上100万人未満	
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	
その妥当性	予診情報・予防接種記録管理／請求支払システムは公益社団法人国民健康保険中央会(以下、国保中央会という。)が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。ただし、予診情報・予防接種記録管理／請求支払システムに格納された特定個人情報は、自動処理により再々委託先(これ以降の全ての委託を含む。以下、同じ。)に情報連携されるため、愛知県国民健康保険団体連合会(以下、愛知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 ☐ 50人以上100人未満 ☐ 100人以上500人未満 ☐ 500人以上1,000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又は閉域網回線を用いた提供 ）
⑤委託先名の確認方法		下記、「⑥委託先名」の項の記載より確認できる。
⑥委託先名		愛知県国保連合会
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	書面又は電磁的方法による承諾
	⑨再委託事項	<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・予診情報・予防接種記録管理／請求支払システムの運用保守 ・PMHキーの採番及びPMHキーを介した医療機関アプリ・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。

5. 特定個人情報の提供・移転(委託に伴うものを除く。)	
提供・移転の有無	[☐] 提供を行っている (4) 件 [☐] 移転を行っている () 件 [☐] 行っていない
提供先1	市町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表第25項
②提供先における用途	予防接種法による予防接種の実施に関する事務であって主務省令で定めるもの
③提供する情報	予防接種の実施に関する情報 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)
④提供する情報の対象となる本人の数	[1万人以上10万人未満] <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	予防接種法等関連法令に定められる予防接種の対象者
⑥提供方法	[☐] 情報提供ネットワークシステム [☐] 専用線 [☐] 電子メール [☐] 電子記録媒体(フラッシュメモリを除く。) [☐] フラッシュメモリ [☐] 紙 [☐] その他 ()
⑦時期・頻度	情報提供依頼があったとき 転入者について、転出元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
提供先2～5	
提供先2	都道府県知事
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表第26項
②提供先における用途	予防接種法による予防接種の実施に関する事務であって主務省令で定めるもの
③提供する情報	予防接種の実施に関する情報 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)
④提供する情報の対象となる本人の数	[1万人以上10万人未満] <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	予防接種法等関連法令に定められる予防接種の対象者
⑥提供方法	[☐] 情報提供ネットワークシステム [☐] 専用線 [☐] 電子メール [☐] 電子記録媒体(フラッシュメモリを除く。) [☐] フラッシュメモリ [☐] 紙 [☐] その他 ()
⑦時期・頻度	情報提供依頼があったとき 転入者について、転出元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

提供先3	都道府県知事または市町村長
①法令上の根拠	番号法第19条第8号に基づく主務省令第2条の表第153項
②提供先における用途	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって主務省令で定めるもの
③提供する情報	予防接種の実施に関する情報 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)
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	予防接種法等関連法令に定められる予防接種の対象者
⑥提供方法	[☒] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	情報提供依頼があったとき 転入者について、転出元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
提供先4	厚生労働大臣
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条の表第154項
②提供先における用途	新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務であって主務省令で定めるもの
③提供する情報	予防接種の実施に関する情報 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)
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	予防接種法等関連法令に定められる予防接種の対象者
⑥提供方法	[☒] 情報提供ネットワークシステム [] 専用線 [] 電子メール [] 電子記録媒体(フラッシュメモリを除く。) [] フラッシュメモリ [] 紙 [] その他 ()
⑦時期・頻度	情報提供依頼があったとき 転入者について、転出元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

6. 特定個人情報の保管・消去

①保管場所 ※	＜本市における措置＞ ・データセンターにて特定個人情報を保管しており、監視設備としてセキュリティゲートにて監視カメラを設置し、入退館管理を24時間有人監視している。 ・建物内のうち、さらにサーバー室の出入口を限定し、入退室管理を行っている部屋に設置されたサーバー内に保管している。 ＜中間サーバー・プラットフォームにおける措置＞ ・中間サーバー・プラットフォーム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。 ＜ガバメントクラウドにおける措置＞ ①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。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。なお、以下のとおりセキュリティ対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・論理的に区分された当市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	<table border="1"> <tr> <td data-bbox="359 1220 486 1355">期間</td><td data-bbox="486 1220 1492 1355"> ＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない </td></tr> <tr> <td data-bbox="359 1355 486 1433">その妥当性</td><td data-bbox="486 1355 1492 1433"> 予防接種法規則第3条で5年間保存しなければならないとされているが、予防接種は5年以上の接種期間中に同じワクチンを複数回接種するものもあり、残りの接種回数等、正確な接種状況の把握のため、5年経過後も保管する必要がある。 </td></tr> </table>	期間	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない	その妥当性	予防接種法規則第3条で5年間保存しなければならないとされているが、予防接種は5年以上の接種期間中に同じワクチンを複数回接種するものもあり、残りの接種回数等、正確な接種状況の把握のため、5年経過後も保管する必要がある。
期間	＜選択肢＞ 1) 1年未満 2) 1年 3) 2年 4) 3年 5) 4年 6) 5年 7) 6年以上10年未満 8) 10年以上20年未満 9) 20年以上 10) 定められていない				
その妥当性	予防接種法規則第3条で5年間保存しなければならないとされているが、予防接種は5年以上の接種期間中に同じワクチンを複数回接種するものもあり、残りの接種回数等、正確な接種状況の把握のため、5年経過後も保管する必要がある。				

③消去方法	＜本市における措置＞ 予防接種法で定められている5年を過ぎたデータについては、本市の判断において削除を行う。 ＜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する。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ ・本市の領域に保管されたデータのみ、予診情報・予防接種記録管理／請求支払システムを用いて消去することができる。 ・本市の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日（作成日）を起点として3年が経過した時点で、自動的に削除される。
7. 備考	

(別添2) 特定個人情報ファイル記録項目

<宛名>

・整理番号 ・カナ氏名 ・生年月日 ・性別 ・氏名 ・世帯番号 ・続柄 ・町名称 ・番地 ・枝番 ・郵便番号 ・住所 ・方書 ・電話番号
・行政区 ・小学校区分 ・中学校区分 ・課税区分 ・国籍 ・取消区分 ・住民となった日 ・住民でなくなった日 ・最新異動 ・最新異動年月日
・個人番号※システム内部で宛名情報と紐づいて保持

<予防接種>

・事業番号 ・期・回数区分 ・予防枝番 ・年度事業 ・予定連番 ・受診日 ・会場その他 ・受診種別 ・登録日 ・負担金区分
・接種医療機関番号 ・接種医療機関その他 ・接種区分 ・Lot番号 ・接種量 ・ツ反結果区分
・反応状態区分 ・長径 ・予診医医療機関番号 ・予診医番号 ・接種医医療機関番号 ・接種医番号 ・ワクチンメーカー名コード ・備考
・抗体検査判定結果 ・抗体検査番号 ・抗体検査方法 ・抗体価 ・抗体価単位
・抗体価単位その他

<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務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 ・勸奨情報(ルールID、勸奨日)

(4)予防接種記録情報

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

Ⅲ 特定個人情報ファイルの取扱いプロセスにおけるリスク対策 ※(7. リスク1⑨を除く。)

1. 特定個人情報ファイル名	
予防接種情報ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1： 目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・最新の住民情報を管理している既存住民基本台帳システムより情報の移転を受けており、窓口や電話では、身分証明書の提示や氏名＋生年月日などの2情報以上の聞き取りで検索を行い、対象者であることを確認している。 ・予防接種を委託している実施医療機関の受付において、身分証明書等の提示による本人確認を実施するよう、豊橋市予防接種実施要領等で定めている。 ・予防接種のパンチデータをシステムに取り込む際には、宛名番号またはカナ＋生年月日の2情報の組み合わせでマッチングを行い、対象者のみを取り込む。 ・個人番号の管理画面以外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。 ・その他、特定個人情報の取扱いに関しては、「豊橋市情報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、医療機関アプリ又は顔認証端末でマイナンバーカードを利用した認証により本人の情報のみが対象者として連携される。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、マイナンバーカードを利用した認証により、本人以外からの情報の入力を防止する。 ・既存事務において本人確認を行った個人番号を既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムに連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。
必要な情報以外を入手することを防止するための措置の内容	・移転を受ける情報は、予防接種対象者及び履歴を管理するのに必要な情報のみであり、不要な情報の入手が行われない仕組みが講じられている。 ・他システムへ情報連携するファイルについては、個人番号が含まれない形式とする。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・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。
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	目的を越えた入手が行われている恐れがないかなどを確認するため、システムを利用する必要がある職員に対して個人ごとにID・パスワードを設定し、アクセスログを取得することで、定期的に点検することを可能とする。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・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。

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に不正であるリスク		
入手の際の本人確認の措置の内容	・最新の住民情報を管理している既存住民基本台帳システムより情報の移転を受けており、窓口や電話では、身分証明書の提示や氏名＋生年月日などの2情報以上の聞き取りで検索を行い、対象者であることを確認している。 ・予防接種を委託している実施医療機関の受付において、身分証明書等の提示による本人確認を実施するよう、豊橋市予防接種実施要領等で定めている。 ・予防接種のパンチデータをシステムに取り込む際には、宛名番号またはカナ＋生年月日の2情報の組み合わせでマッチングを行っている。 <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> ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。	
個人番号の真正性確認の措置の内容	・既存住民基本台帳システムより情報の移転を受けており、真正性は担保されている。 ・窓口で個人番号カードの提示を求め、個人番号の真正性を確認する。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号をPublic Medical Hubから加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。	
特定個人情報の正確性確保の措置の内容	・特定個人情報の入力、修正、削除を行う際は、限られた担当者のみ行い、入力内容に誤りの無いよう十分注意して行う。 ・その他、特定個人情報の取り扱いに関しては、「豊橋市情報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> 個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容	・専用のネットワーク回線を利用することで、外部への漏えいリスクを低減している。 ・提出された予診票については、全件数を確認し、施錠された部屋に保管している。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・予診情報・予防接種記録管理／請求支払システムと支払基金の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 ・健康管理システムは、予診情報・予防接種記録管理／請求支払システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。)におけるその他のリスク及びそのリスクに対する措置		

3. 特定個人情報の使用			
リスク1: 目的を超えた紐付け、事務に必要なでない情報との紐付けが行われるリスク			
宛名システム等における措置の内容	個人番号利用業務以外または、個人番号を必要としない業務から予防接種情報の要求があった場合は、個人番号が含まれない情報のみを提供するようにアクセス制御を行っている。		
事務で使用するその他のシステムにおける措置の内容	他業務からアクセスされる、予防接種情報と特定個人情報を含むデータベースを切り離して管理している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予診情報・予防接種記録管理／請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関アプリや住民から予診情報・予防接種記録管理／請求支払システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。		
その他の措置の内容			
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 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	◎健康管理システム、電子申請機能のいずれかのシステムが入った端末にはすべて生体認証機能が付いており、権限を付与された職員のみが端末の起動を行うことができる。 ・健康管理システムを利用する必要がある職員、個人番号の照会を可能とする対象者、不可とする対象者を特定し、個人ごとにユーザー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っている。 ・ユーザーIDについては、正確性を維持する仕組みを構築し、適宜更新している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市は、予診情報・予防接種記録管理／請求支払システムのアクセス権限を管理する管理者を定める。 ・予診情報・予防接種記録管理／請求支払システムのログインはユーザー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ーIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予診情報・予防接種記録管理／請求支払システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム(各業務システム)から予診情報・予防接種記録管理／請求支払システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。		
アクセス権限の発効・失効の管理	[行っている]	＜選択肢＞ 1) 行っている	2) 行っていない
具体的な管理方法	・職員ごとに、所属長が業務に必要なアクセス権限を付与し、利用可能な機能を制限している。 ・健康管理システムへのユーザーIDごとのアクセス権限は、保健所(ほいっぷ内)にて管理を行い、登録／変更を行っている。その他の者は、アクセス権限の登録／変更を行うためのアクセス権限が与えられていない。 ・人事異動の場合等、権限が不要となった場合は、保健所(ほいっぷ内)職員が不要となったIDや権限を変更または削除し、アクセス権限の失効管理を適切に行っている。 ＜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＞ ・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ー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	・職員の業務に応じたアクセス権限が付与されるよう管理しており、健康管理システムへのユーザーIDごとのアクセス権限については、保健所(ほいっぷ内)職員が管理を行っている。 ・ユーザーIDやアクセス権限については、保健所(ほいっぷ内)が定期的に確認を実施し、不要となったIDや権限を変更または削除する。 <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> ・共用IDは発行せず、必ず個人に対し、ユーザーIDを発行する。 ・管理者が定期的に管理表を確認し、必要に応じて見直しを行う。	
特定個人情報の使用の記録	[記録を残している]	<選択肢> 1) 記録を残している 2) 記録を残していない
具体的な方法	・健康管理システムでは、操作者による認証から認証解除を行うまでの間、監査証跡の記録を行っている。(操作者がどの個人に対して照会・異動を行ったかまで記録している。) ・監査証跡として、使用した職員と使用した端末、日時、使用の目的と事務、照会した個人の特定等を記録している。 ・自動実行等による処理(副本データの作成や連携等)についても、同様に監査証跡の記録を行っている。 ・監査証跡は7年間保存し、連携失敗等のエラー発生時の原因調査・特定で必要になることもあるため、削除については本市の判断において行う。 ※7年の根拠: 電子計算機使用詐欺(刑法第246条の2)の罰則の公訴時効が7年と規定されているため。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・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	・他市区町村や行政機関において住民等の情報を事務外の目的で閲覧したり、漏えい事故を起こしたケースについての新聞記事等を職場で共有し注意喚起を行っている。 ・個人や他市区町村、関係機関からの問合せへの対応方法を共有し、注意喚起を行っている。 ・アクセスログを管理していることを周知し、事務外利用を抑制している。 ・新規任用者には個人情報の取扱いについての研修に参加させ、事務外利用の禁止を徹底している。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・本市は、特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、業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いとする。 ・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、業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	・事務端末には特定個人情報ファイルが複製されない仕組みとなっている。 ・システムのバックアップデータはデータセンター内のサーバ内に管理し、権限を持った者のみアクセスを許可している。 ・システム操作からデータが持出しできないよう制御している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・既存システム（各業務システム）から特定個人情報を抽出したCSVファイルを予診情報・予防接種記録管理／請求支払システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・本市の既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムへの特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線（LGWAN又はその他の閉域網回線）を利用した接続のみが認められる。 ・予診情報・予防接種記録管理／請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置		

4. 特定個人情報ファイルの取扱いの委託		[] 委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認	・委託先の社会的信用と能力を確認して選定する(業務実績、プライバシーマークの取得状況、ISMSの認証取得等)。また、委託業者が選定基準を引き続き満たしていることを適時確認する。 ・個人情報保護に関する規定や体制の整備、人的安全管理措置、技術的安全管理措置について確認する。 ・必要があると認められる際は委託先に対し報告を求め実地調査を行うことができる。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 本市は、予診情報・予防接種記録管理／請求支払システムの利用・情報連携業務及び運用保守業務における特定個人情報の取扱いを愛知県国保連合会に委託し、愛知県国保連合会は国保中央会に再委託することとする。 特定個人情報の適正な取扱いに関するガイドライン(行政機関等編)に基づき、国保中央会の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。	
特定個人情報ファイルの閲覧者・更新者の制限	[制限している]	＜選択肢＞ 1) 制限している 2) 制限していない
具体的な制限方法	・個人情報保護に関する誓約書を従事する者から委託業者に対して提出させ、受領報告書、受託者(法人格)の誓約書及び「個人情報保護管理者届及び委託業務場所届」を提出するよう指示している。 ・受領報告書により誓約書の提出が確認されたものに対してのみ、システム操作の権限を与えている。 ・再委託業者も委託業者と同様に個人情報保護に関する誓約書を従事する者から再委託先に提出させ、受領報告書及び再委託先(法人格)の誓約書を受託者に提出するよう指示している。 受託者に対して再委託先から受領した書類の写しを市に提出させている。 ＜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＞ ・本市がアクセス権限の管理状況を確認できる。 ・本市は、アクセス権限を付与する者を必要最小限に限定する。 ・本市は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本市は、アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再々委託先(PMHキー採番や運用保守)のみに付与される。	
特定個人情報ファイルの取扱いの記録	[記録を残している]	＜選択肢＞ 1) 記録を残している 2) 記録を残していない
具体的な方法	・委託側において利用するユーザーIDについては、職員と同等のログ監視を行っており、利用履歴の参照も職員と同等の確認を行うことができる。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムは特定個人情報の取り扱いのログを保存し、本市は特定個人情報に係る操作のログを閲覧・出力できる。 ※再々委託先(PMHキー採番や運用保守)に係る特定個人情報の取扱いログに限られる。	
特定個人情報の提供ルール	[定めている]	＜選択肢＞ 1) 定めている 2) 定めていない
委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	・本市の指示または書面による承諾がある場合を除き、業務に関して知りえた個人情報を契約の目的以外の目的のために提供してはいけなくと定めている。 ・必要があると認められる際は委託先に対し報告を求め実地調査を行うことができる。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・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	・委託業者は、本市より個人情報が記録された資料の提供を受ける場合は、本市にその個人情報の内容、媒体及び数量を記載した書類を提出する。 ・必要があると認められる際は委託先に対し報告を求め実地調査を行うことができる。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・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	・委託業者は、業務完了後直ちに本市へ個人情報を返還する。また、本市に必要がある場合は、業務完了時以外でも個人情報の返還を求められる。 ・委託業者は、本市へ返還する特定個人情報以外は業務完了後直ちに廃棄又は消去する。その際に、書面による報告を求めることとする。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・委託契約終了後は予診情報・予防接種記録管理／請求支払システムに保管していた全ての特定個人情報を国保中央会が消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、本市は消去について国保中央会から報告を受けることができ、それにより消去状況について確認が可能となる。
委託契約書中の特定個人情報ファイルの取扱いに関する規定		[定めている] <選択肢> 1) 定めている 2) 定めていない
	規定の内容	・委託業務を遂行する目的以外に使用しないこと ・特定個人情報の閲覧者、更新者を制限すること ・特定個人情報を第三者に提供しないこと ・利用するユーザIDを権限のない第三者に貸与しないこと ・利用するユーザIDを権限のない第三者に利用されないよう定期的にパスワードを変更すること ・個人情報の確認状況を随時委託先の視察、監査又は必要な報告を求めることができること ・個人情報の改ざん、盗用等の防止について措置を講じること ・個人情報の適切な管理(運搬方法、保管場所)のために必要な措置を講じること ・本市の書面による承諾がある場合を除き、個人情報資料の複写、複製しないこと ・個人情報の適正な取扱いについて、従事者に対し監督及び教育を行うこと <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> 愛知県国保連合会及び国保中央会は特定個人情報の適正な取扱いに関するガイドライン(行政機関等編)を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項

再委託先による特定個人情報ファイルの適切な取扱いの確保	[十分に行っている] ＜選択肢＞ 1) 特に力を入れて行っている 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	・原則再委託は禁止している。 ・再委託を認める場合は、委託業者と再委託業者の間で、個人情報の取り扱いについて定めた個人情報取扱特記事項を準用することとする。 ・再委託業者も委託業者と同様に個人情報保護に関する誓約書及び従事者から再委託業者に提出された誓約書の受領報告書を受託者に提出させている。 受託者に対して再委託先から受領した書類の写しを市に提出させている。 ＜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、点検結果について愛知県国保連合会及び本市に年1回報告を行う。
その他の措置の内容	＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[○] 提供・移転しない	
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＞ 団体内統合宛名システムの職員認証・権限管理機能により、職員の操作ログ、時刻等の内容が記録されるため、不適切な端末の操作や情報の入手を抑止する。 ＜団体内統合宛名システムの運用における措置＞ 団体内統合宛名システムの職員権限を、人事異動や権限変更が生じた際には早急に反映することで、権限のない職員の情報の入手を防止する。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能(※1)により、情報提供ネットワークシステムに情報照会を行う際には、情報提供許可証の発行と照会内容の照会許可照会リスト(※2)との照合を情報提供ネットワークシステムに求め、情報提供ネットワークシステムから情報提供許可証を受領してから情報照会を実施することになる。つまり、番号法上認められた情報連携以外の照会を拒否する機能を備えており、目的外提供やセキュリティリスクに対応している。 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) 番号法別表第2及び第19条第14号に基づき、事務手続きごとに情報照会者、情報提供者、照会・提供可能な特定個人情報をリスト化したもの。 (※3) 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報へのアクセス制御を行う機能。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	
リスク2: 安全が保たれない方法によって入手が行われるリスク			
リスクに対する措置の内容	＜団体内統合宛名システムのソフトウェアにおける措置＞ ・団体内統合宛名システムは自機関向けの中間サーバーとだけ、通信および特定個人情報の入手のみを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・ソフトウェアにおける措置＞ ・中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ ・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。		
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			
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。		
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている	

リスク4: 入手の際に特定個人情報が漏えい・紛失するリスク		
リスクに対する措置の内容	＜中間サーバー・ソフトウェアにおける措置＞ ・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(※)。 ・情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報漏えい・紛失するリスクを軽減している。 ・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＞ ・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できない。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク5: 不正な提供が行われるリスク		
リスクに対する措置の内容	＜本市における措置＞ ・健康管理システムと情報提供ネットワークシステムとは定められたネットワークを利用し、外部からの不正アクセスができない仕組みとする。(インターネットとは切り離されて管理されている) ＜中間サーバー・ソフトウェアにおける措置＞ ・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。 ・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情報提供許可証と情報照会者へたどり着くための経路情報を受領し、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。 ・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。 ・中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 (※) 情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。	
リスクへの対策は十分か	[十分である]	＜選択肢＞ 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク6: 不適切な方法で提供されるリスク		
リスクに対する措置の内容	＜本市における措置＞ ・健康管理システムと情報提供ネットワークシステムとは定められたネットワークを利用し、外部からの不正アクセスができない仕組みとする。(インターネットとは切り離されて管理されている) ＜中間サーバー・ソフトウェアにおける措置＞ ・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。 ・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会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＞ ・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。	
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	＜本市における措置＞ ・連携システムの十分な検証を実施し、正確に提供・移転が行われるようにする。 ・連携システムには、あらかじめ許可された提供・移転先のみ接続されており、誤った相手に情報の提供・移転が行われないことをシステム上で担保する。 ＜中間サーバー・ソフトウェアにおける措置＞ ・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。 ・情報提供データベース管理機能(※)により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ・情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 (※)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＞ ・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＞ ・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> ・データセンターにて特定個人情報を保管しており、監視設備としてセキュリティゲートにて監視カメラを設置し、入退館管理を24時間有人監視している。 ・建物内のうち、さらにサーバー室の出入口を限定し、入退室管理を行っている部屋に設置されたサーバー内に保管している。 <中間サーバー・プラットフォームにおける措置> ・中間サーバー・プラットフォーム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。 <ガバメントクラウドにおける措置> ①ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスの利用

⑥技術的対策	[十分にやっている] <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> ・コンピュータウイルス監視ソフトを使用し、サーバ・端末双方でウイルスチェックを実施する。また、新種の不正プログラムに対応するために、ウイルスパターンファイルは定期的に更新し、可能な限り最新のものを使用する。 <中間サーバー・プラットフォームの措置> ・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。 <ガバメントクラウドにおける措置> ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」(令和4年10月 デジタル庁。以下「利用基準」という。))に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者(利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。)は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウェアについて、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。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度(ISMAP)において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・予診情報・予防接種記録管理／請求支払システムは論理的に区分された当市の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、予診情報・予防接種記録管理／請求支払システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予診情報・予防接種記録管理／請求支払システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ・本市の端末と予診情報・予防接種記録管理／請求支払システムとの通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。

⑦バックアップ	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にしていない
⑧事故発生時手順の策定・周知	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか	[発生なし]	<選択肢> 1) 発生あり 2) 発生なし
その内容		
再発防止策の内容		
⑩死者の個人番号	[保管している]	<選択肢> 1) 保管している 2) 保管していない
具体的な保管方法	生存者の個人番号と同様の方法にて安全管理措置を実施する。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
リスク2: 特定個人情報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	・最新の住民情報を管理している既存住民基本台帳システムより情報の移転を受けており、日次処理で健康管理システムにも最新の特定個人情報が反映される仕組みを構築している。 ・本市に住所を有しない者の場合は、本人からの届出がされた後、速やかに情報の更新を行い、最新の状態を保つこととしている。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・本特定個人情報ファイルの個人情報は、住基及び住民登録外者の異動情報を取得し、内部番号を基に最新の情報に反映されるため、古い情報のまま保管され続けるリスクは存在しない。	
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている

リスク3: 特定個人情報が消去されずいつまでも存在するリスク		
消去手順	[定めている]	<選択肢> 1) 定めている 2) 定めていない
手順の内容	・特定個人情報の適正な取扱いに関するガイドラインに従い、情報提供NWSを使用した記録は7年間で削除する。 ・例外として、連携不備の懸念があった場合は、原因調査・特定のため、保管期間を延長する。 ・特定個人情報の削除時には、削除後データに過不足のないように、削除記録を残す。 ・磁気ディスクの廃棄時は、豊橋市特定個人情報等の取扱いに関する管理要綱に基づき、保護管理者の許可を得て、専用ソフトによるフォーマット、物理的粉碎等を行うことにより、復元不可能な方法により削除又は廃棄を行う。 また、磁気ディスク管理簿にその記録を残す。 <ガバメントクラウドにおける措置> データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・消去が必要となった情報は内部手続を経て消去し、その記録を残す。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日（作成日）を起点として3年が経過した時点で、自動的に削除される。	
その他の措置の内容		
リスクへの対策は十分か	[十分である]	<選択肢> 1) 特に力を入れている 2) 十分である 3) 課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置		

IV その他のリスク対策 ※

1. 監査		
①自己点検	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的なチェック方法	<本市における措置> ・定期的(年に1回以上)に、評価書の記載内容どおりの運用がなされていることを所属内において自己点検を実施し、運用状況を確認することとする。 <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。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 本市は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、必要な自己点検を行う。	
②監査	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的な内容	<本市における措置> ・内部監査 年に1回、組織内に置かれた監査担当により、以下の観点による自己監査を実施し、監査結果を踏まえて体制や規定を改善することとする。 ・評価書記載事項と運用実態のチェック ・個人情報保護に関する規定、体制整備 ・個人情報保護に関する人的安全管理措置 ・職員の役割責任の明確化、安全管理措置の周知 <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。 <ガバメントクラウドにおける措置> ガバメントクラウドについては政府情報システムのセキュリティ制度(ISMAP)のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 本市は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、必要な監査を行う。	
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発	[十分にしている]	<選択肢> 1) 特に力を入れて行っている 2) 十分にしている 3) 十分にっていない
具体的な方法	<本市における措置> ・所属内において、新任職員向けに情報セキュリティ及び個人情報保護に関する教育および研修を実施する。 ・他都市等で発生した情報セキュリティ事故などの記事を所属内で随時回覧等することにより、個人情報保護に関する職員の意識を高める。 ・職員は、本市情報セキュリティポリシーに基づき実施している情報セキュリティ研修に定期的に参加し、個人情報保護に関する意識を高め、個人情報の適切な取扱いを行う。 <中間サーバー・プラットフォームにおける措置> ・IPA(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。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 本市は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、適切な指導を行う。	

3. その他のリスク対策

＜中間サーバー・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リテラシの高い運用担当者によるセキュリティリスクの低減、及び技術力の高い運用担当者による均一的で安定したシステム運用、監視を実現する。

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

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

本市は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。

V 開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求

①請求先	豊橋市総務部行政課 じょうほうひろば 〒440-8501 豊橋市今橋町1番地 電話:0532-51-2037 FAX:0532-51-0789	
②請求方法	個人情報の保護に関する法律、豊橋市個人情報の保護に関する法律施行条例及び豊橋市個人情報の保護に関する法律施行細則に規定する方法による。	
	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: ただし、「写しの交付」の場合には規則に定める額を徴収する。)	
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	豊橋市保健所保健医療企画課 豊橋市中野町字中原100番地 電話0532-39-9109 FAX0532-38-0780
②対応方法	電話による問い合わせについては、 ①対象者の連絡先として登録のある電話番号からの電話であること ②①の電話番号へ折り返して対応するなど慎重な対応を心掛けている

VI 評価実施手続

1. 基礎項目評価	
①実施日	令和8年7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	豊橋市パブリックコメント手続要綱に基づき、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、広報紙に公表している旨の記事を掲載し、市ホームページ及び市内公共施設にて閲覧できるようにする。
②実施日・期間	令和6年7月22日(月)～令和6年8月21日(水)
③期間を短縮する特段の理由	—
④主な意見の内容	意見なし
⑤評価書への反映	
3. 第三者点検	
①実施日	2024/08/27
②方法	個人情報保護に関する学識経験者を委員に含む、豊橋市情報公開・個人情報保護審査会が第三者点検を実施した。
③結果	評価書の記載内容に問題はないと認められた。
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2年12月1日		重点項目評価書	全項目評価書	事後	特定個人情報番号88番(新型コロナウイルス等対策特措法
令和3年9月1日			新型コロナウイルス感染症対策に係る予防接種事務と予防接種の実施後に、接種者からの申請	事後	VRSの利用開始に伴う再評価
令和4年6月1日			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を追加	事後	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
令和6年4月1日			特別臨時接種終了に伴うVRS機能の変更を追加	事前	年度末の更新
令和6年4月1日	I-7評価実施機関における担当部署	I-7 ①健康政策課、感染症対策室	I-7 ①保健医療企画課 ②保健医療企画課長	事後	機構改革による課名変更
令和6年10月24日	I-②事務の内容	番号法別表第一・項番10又は93の2の規定	番号法別表14、126の規定	事後	法令改正に伴う変更
令和6年10月24日	I-②事務の内容		〇新型コロナウイルス特措法第46条第3項の規定により読み替えて適用する予防接種法第6条第1項	事後	法令改正に伴う変更
令和6年10月24日	I-②事務の内容		VRSへ予防接種対象者及び発行した接種券の登録を行うを削除	事後	自己点検
令和6年10月24日	I-5個人番号の利用	番号法第9条第1項 別表第一 項番10、93の2	番号法第9条第1項 別表14、126	事後	自己点検
令和6年10月24日	I-6情報提供ネットワークシステムによる情報連携	番号法第19条第8号及び別表第二 別表第二における情報照会の根拠:16の2、	番号法第19条第8号に基づく主務省令 番号法第19条第8号に基づく主務省令第2条の	事後	法令改正に伴う変更
令和6年10月24日	(別添1)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の内容の図を一部修正(×印の部分削除)	事後	自己点検
令和6年10月24日	II-4-委託事項2 ①委託内容	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)	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。)	事後	自己点検
令和6年10月24日	II-5-提供先		提供先1(①法令上の根拠を各項目に分けて表記(提供先2～4を追加)	事前	自己点検及び法令改正に伴う変更
令和6年10月24日	II-4-⑥委託先名		株式会社ヒミカ、株式会社両備システムを追加	事前	標準準拠システムへ移行するにあたり、事前に提出
令和6年10月24日	II-6-①保管場所 ③消去方法		<ガバメントクラウド>における措置>を追加	事前	システムをガバメントクラウドへ移行するにあたり、事前に提出
令和6年10月24日	(別添2)特定個人情報ファイル記録項目		<宛名> 小学校区分・中学校区分を追加	事前	標準準拠システムへ移行するにあたり、事前に提出
令和8年4月1日	I-1-②事務の内容		〇新型コロナウイルス感染症対策に係る予防接種事務	事後	VRSの廃止に伴う変更
令和8年4月1日	I-2-②事務の内容		〇新型コロナウイルス感染症対策に係る予防接種事務	事後	VRSの廃止に伴う変更
令和8年4月1日	I-2-システム1-③、 I-2-システム2-③	福祉システム	生活保護システム、障害者福祉システムに修正	事後	自己点検
令和8年4月1日	I-5個人番号の利用		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VRSを用い	事後	VRSの廃止に伴う変更
令和8年4月1日	(別添1)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の内容(追加)及び 新型コロナワクチン	事後	VRSの廃止に伴う変更
令和8年4月1日	II-3-②入手方法		その他から VRS を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	II-3-③、④、⑤及び⑧		<新型コロナウイルス感染症対策に係る予防接種事務>に関する記述を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	II-4-⑥委託先名		富士通Japan株式会社 を削除	事後	自己点検
令和8年4月1日	II-4-委託事項2		削除	事後	VRSの廃止に伴う変更
令和8年4月1日	II-5-提供先3-②及び⑥ II-5-提供先4-②及び⑥		新型コロナウイルス感染症対策に係る予防接種事務 及び VRS を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	II-6-①及び③		<VRSにおける追加措置>に関する記述を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	(別添2)特定個人情報ファイル記録項目		<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>に関する記述を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	III-2及び3		<VRSにおける追加措置>に関する記述を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	III-2、3及び4		<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>に関する記述を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	III-7特定個人情報の保管・消去		<VRSにおける措置>に関する記述を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	IV-1、2及び3		<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>に関する記述を削除	事後	VRSの廃止に伴う変更
令和8年4月1日	V-1-②請求方法	豊橋市個人情報保護条例における開示・訂正・利用停止請求の各手続きに即した書類及び本	個人情報保護の保護に関する法律、豊橋市個人情報の保護に関する法律施行条例及び豊橋市個	事後	自己点検
令和8年7月1日	I-1-②事務の内容		<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	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	I-2-システム4		予診情報・予防接種記録管理/請求支払システムを追加	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	(別添1)事務の内容		予防接種における住民からの予防票入力及び接種記録の取得、医療機関からの予防票取得、	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	II-2-④入手方法		<予診情報・予防接種記録管理/請求支払システムを活用した情報連携に係る予防接種事務	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1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	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	II-4-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	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	II-6-①及び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	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	(別添2)特定個人情報ファイル記録項目		<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	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	III-2、3、4及び7		<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	事前	予防接種デジタル化を実施するにあたり、事前に提出
令和8年7月1日	IV-1、2及び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	事前	予防接種デジタル化を実施するにあたり、事前に提出