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
45	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

宇都宮市は，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り扱いについて，特定個人情報の漏えいその他の事態発生による個人のプライバシー等の権利権益に与える影響を認識し，このようなリスクを軽減するための適切な措置を講じたうえで，個人のプライバシー等の権利権益の保護を実施していることを宣言する。

特記事項	

評価実施機関名

宇都宮市長

個人情報保護委員会　承認日 【行政機関等のみ】

公表日

［令和7年5月　様式4］

項目一覧

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

Ⅰ　基本情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	予防接種に関する事務
②事務の内容　※	＜定期予防接種に関する事務＞ 予防接種法，予防接種法施行令，予防接種法施行規則，予防接種実施規則，定期接種実施要領，宇都宮市予防接種実施要領，行政手続における特定の個人を識別するための番号の利用等に関する法律（以下，「番号法」という。）及び公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律に基づき，宇都宮市（以下，「本市」という。）が，定期予防接種を行う。また，予防接種の記録の作成，未接種者への積極的勧奨，高齢者の予防接種においては市民税の課税状況に応じた実費の徴収，予防接種による健康被害者に対する給付金の支給を行う。 ①　定期予防接種の実施 ②　定期予防接種の記録の作成 ③　定期予防接種の積極的勧奨 ④　定期予防接種の実費の徴収 ⑤　高齢者の予防接種における自己負担免除申請書の受理（市民税の非課税世帯・生活保護受給者・中国残留邦人等支援法に基づく支援給付の支給決定を受けている方への無料券の発行） ⑥　予防接種による健康被害者に関する請求の受理，給付金の支給 ⑦　情報提供ネットワークシステムを利用した地方税関係情報及び公的給付支給等口座登録簿関係情報の照会 ⑧　情報提供ネットワークを利用した定期予防接種の記録の提供 ＜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＞ 新型インフルエンザ等対策特別措置法，新型インフルエンザ等対策特別措置法施行令及び行政手続における特定の個人を識別するための番号の利用等に関する法律（以下，「番号法」という）に基づき，宇都宮市（以下，「本市」という）が，新型インフルエンザ等が発生した場合に，特定接種や予防接種の実施，予診票の発行等を行う。 ①　特定接種及び予防接種の実施 ②　特定接種及び予防接種の記録の作成 ③　特定接種及び予防接種の実費の徴収 ④　情報提供ネットワークシステムを利用した予防接種記録の照会 ⑤　情報提供ネットワークシステムを利用した予防接種記録の提供 ⑥　予防接種実施後の接種記録等を登録・管理及び他市区町村へ接種記録の照会・提供 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ 本市は、情報連携のため、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 住民が予防接種時に、従来の紙の予診票に代えて、タブレットに搭載された医療機関用アプリ等においてマイナンバーカードを用いることにより、医療機関は住民が事前に入力した予診票情報、接種記録の取得/閲覧/入力が可能となる。 本市は、医療機関から入力された予診票情報、接種記録の取得及び住民への通知が可能となる。
③対象人数	[　30万人以上　]　＜選択肢＞ 1) 1,000人未満　2) 1,000人以上1万人未満 3) 1万人以上10万人未満　4) 10万人以上30万人未満 5) 30万人以上

2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	健康管理システム
②システムの機能	1　対象者検索・照会機能 氏名等のキー情報をもとに，システム台帳から検索・照会を行う。 2　接種券発行機能 検索・照会した対象者の接種券等の発行を行う。 3　接種記録登録機能 ⑴　検索・照会した対象者の予防接種記録の登録を行う。 ⑵　別途作成したパンチデータから一括登録を行う。 4　庁内連携機能 住民基本台帳を基礎情報として利用するため，異動情報を共通基盤システム（庁内連携システム）から受信し，システム台帳の更新を行う。

③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
システム2～5	
システム2	
①システムの名称	団体内統合宛名システム
②システムの機能	1　団体内統合宛名番号採番機能 　業務システムからの要求に応じて，団体内統合宛名番号を採番し，業務システム及び中間サーバーに返却する。 2　番号管理情報更新機能 　住基情報，住登外情報が更新された際に，団体内統合宛名番号，個人番号，宛名番号（個人）の紐づけ情報を更新する。 3　中間サーバー連携機能 　中間サーバー又は中間サーバー接続端末からの要求に応じて，団体内統合宛名番号に紐づく宛名情報を返却する。 4　既存システム連携機能 　既存システムからの要求に応じて，個人番号又は団体内統合宛名番号に紐づく宛名情報を返却する。 5　既存システム連携機能（番号情報） 　既存システムからの要求に応じて又は番号管理情報の変更の際に，宛名番号（業務）に紐づく個人番号又は団体内統合宛名番号を返却する。 6　番号表示機能（番号の紐づけ情報の検索，表示） 　業務システムで団体内統合宛名番号を保持しない又はシステム化されていない業務向けに，番号の紐づけ情報を検索・表示する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
システム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）
②システムの機能	1　庁内連携機能 ⑴　各業務システム間の連携において，各事務システムの連携用テーブルに情報を格納する。 ⑵　各業務システムにおいて，異動等により情報の修正があった場合，その異動情報等で連携用テーブルを修正する。 2　情報照会機能 　各業務システムにおいて，他システムの情報が必要な場合に，他システムの連携テーブルを参照する。 3　中間サーバー連携機能 ⑴　統合DBから，特定個人情報を抽出し，中間サーバーに連携する。 ⑵　業務システムから受信した「他団体への情報照会依頼」を中間サーバーに連携する。 ⑶　中間サーバーから「他団体からの情報提供内容」を取得する。 4　住登外者の登録・更新機能 　住登外者の宛名情報を登録・更新する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[○] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [○] その他　（　）

システム4	
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」と情報保有期間内で個人をを特定するために利用する「団体内統合宛名番号」とを紐づけ，その情報を保管・管理する。 2　情報照会機能 　情報提供ネットワークシステムを介して特定個人情報（連携対象）の情報照会及び情報提供受領（照会した情報の受領）を行う。 3　情報提供機能 　情報提供ネットワークシステムを介して，情報照会要求の受領及び当該特定個人情報（連携対象）の提供を行う。 4　各業務システム接続機能 　中間サーバーと各事務システム，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。 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。 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。 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。 8　セキュリティ管理機能 　暗号化・複合機能と限情報及び照会許可用照合リストを管理する。 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。 10　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　（　　）

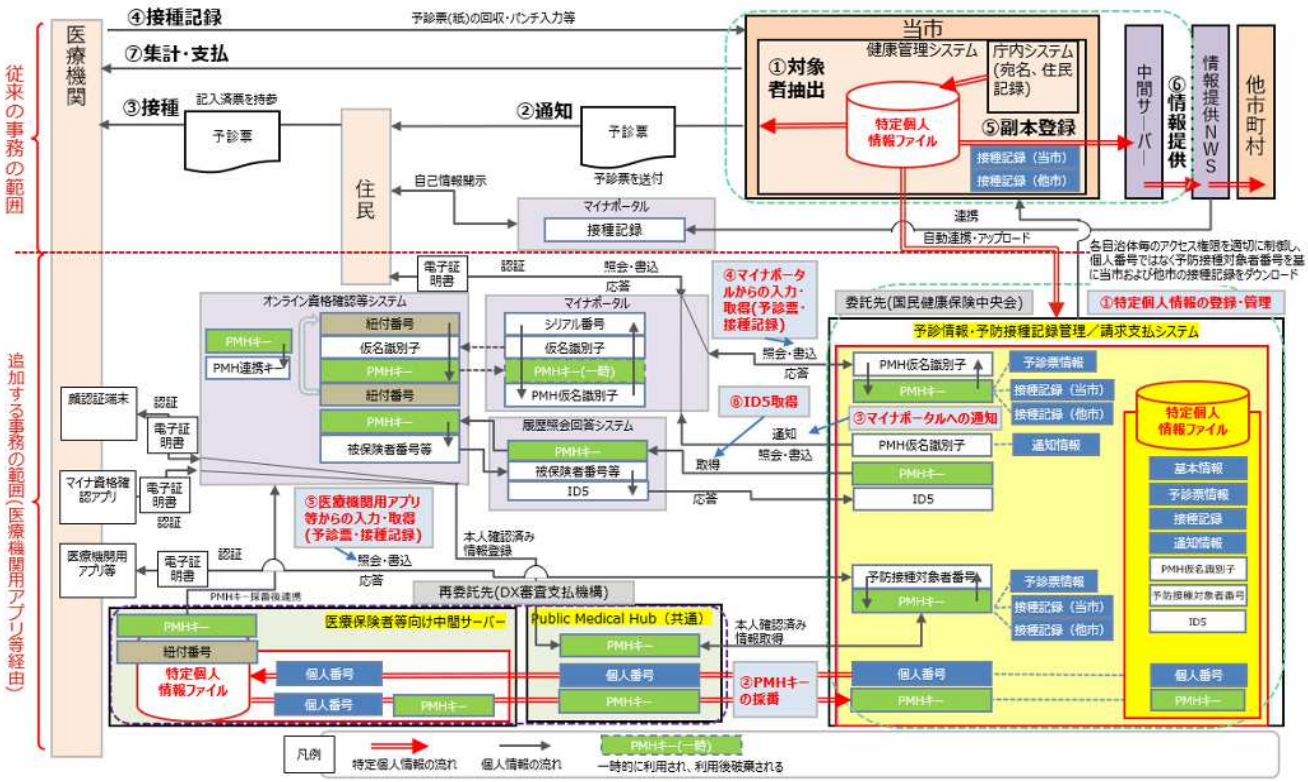
システム5	
①システムの名称	予診情報・予防接種記録管理／請求支払システム
②システムの機能	①予防接種関連データの登録機能 本市区町村は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市区町村で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・予防接種記録管理／請求支払システムに登録する。また、Public Medical 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付くPMH仮名識別子を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く接種記録・通知をマイナポータルへ提供する。また、マイナポータルへログインして予診票の入力画面から情報を入力することにより、予診情報・予防接種記録管理／請求支払システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐付く予診票情報を登録する。 ④情報連携機能（医療機関用アプリ等） ・本人確認情報の格納機能 予防接種対象者が、顔認証端末又はマイナ資格確認アプリを利用してマイナンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリ等は、予診情報・予防接種記録管理／請求支払システムへ本人確認情報を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐付く予防接種対象者番号をキーに予診票情報を医療機関用アプリ等に提供する。また、医療機関が接種記録の入力画面から情報を入力することにより、予診情報・予防接種記録管理／請求支払システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐付く接種記録を登録する。 ⑤情報連携機能（履歴照会回答システム） ・識別子の格納機能 予診情報・予防接種記録管理／請求支払システムは接種記録等の情報を予防接種DBに連携し、予防接種DBにおいて予防接種の有効性・安全性等の調査・研究を行う。予診情報・予防接種記録管理／請求支払システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐づけて予診情報・予防接種記録管理／請求支払システムに連携する。
③他のシステムとの接続	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [　] 宛名システム等　　[　] 税務システム [○] その他　（健康管理システム、マイナポータル、医療機関用アプリ、電子カルテ等、Public Medical Hub、履歴照会回答システム、オンライン資格確認等システム）

システム6～10	
システム6	
①システムの名称	
②システムの機能	
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[　] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [　] 宛名システム等　[　] 税務システム [　] その他　（　）
③他のシステムとの接続	[　] その他　（　）
システム11～15	
システム16～20	
3. 特定個人情報ファイル名	
予防接種ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	予防接種法関連法令に基づき，予防接種時期に応じた既接種者及び未接種者の数を確認し，市内における予防接種の実施状況について的確に把握するため。また，健康被害が発生した際に迅速な救済を図るため。
②実現が期待されるメリット	・予防接種実施状況を把握し，接種率の低い予防接種について接種勧奨を行い，接種率向上の取組を強化できる。 ・接種履歴を把握することで，誤った時期，年齢，回数及び接種間隔による接種を防止する。 ・健康被害が発生した際に，接種状況等を確認・把握し，迅速な救済を図る。
5. 個人番号の利用　※	
法令上の根拠	行政手続における特定の個人を識別するための番号の利用等に関する法律（番号法） （平成25年5月31日法律第27号） ・　番号法第9条第1項　別表14の項 ・　番号法第9条第1項　別表126の項 ・　番号法第19条第6号（委託先への提供） ・　番号法第19条第16号（人の生命，身体又は財産の保護）
6. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　] ＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	【情報照会】 番号法第19条第8号に基づく主務省令第2条の表25の項，27の項，28の項，29の項，153の項 【情報提供】 番号法第19条第8号に基づく主務省令第2条の表25の項，26の項，28の項，153の項，154の項
7. 評価実施機関における担当部署	
①部署	保健福祉部　保健所　保健予防課
②所属長の役職名	保健予防課長
8. 他の評価実施機関	

（別添1）事務の内容

予防接種事務の概要　全体図

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



（備考）

①特定個人情報の登録・管理
・本市区町村は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診情報・予防接種記録管理／請求支払システムにおいて対象者の個人番号を含む対象者情報の登録を行う。（LGWAN回線等経由）
・本市区町村は予診情報・予防接種記録管理／請求支払システムから接種記録等、必要な情報を自動連携またはダウンロードし、健康管理システム等への取込を行う。
・予診情報・予防接種記録管理／請求支払システムへ登録された個人情報へのアクセスは適切に制御される。

②PMHキー採番
・予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対して個人番号を連携することで、オンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼する。
・Public Medical Hubは、医療保険者等向け中間サーバーを経由しPMHキーを採番して予診情報・予防接種記録管理／請求支払システムに回答する。
・医療保険者等向け中間サーバーは、PMHキーと個人番号を紐付けて、PMHキーと紐付番号をオンライン資格確認等システムへ連携する。
・オンライン資格確認等システムは、紐付番号をキーに仮名識別子とPMHキーを紐付けて、マイナポータルに連携する。
・マイナポータルは、新たにPMH用の仮名識別子（PMH仮名識別子）を生成し、シリアル番号、仮名識別子、PMHキーと紐付けて、予診情報・予防接種記録管理／請求支払システムに連携する。（連携後、マイナポータル上からPMHキーは削除される。）以降、③④⑤⑥が可能となる。

③マイナポータルへの通知
・予診情報・予防接種記録管理／請求支払システムからマイナポータル経由で住民向けの通知を行うため、本市区町村は予診情報・予防接種記録管理／請求支払システムを利用してマイナポータルに識別子（PMH仮名識別子）と通知情報を登録する。

④マイナポータルからの入力・取得（予診票・接種記録）
・住民は、マイナポータル経由で予診情報・予防接種記録管理／請求支払システムへの予診票の事前入力や、予診情報・予防接種記録管理／請求支払システムから接種記録や通知情報を閲覧/取得する。

⑤医療機関用アプリ等からの入力・取得（予診票・接種記録）
・医療機関が医療機関用アプリ等を利用し、接種時に住民からマイナンバーカードによる本人確認を経て、事前入力された予診票及び接種記録の閲覧/取得/入力を行う。

⑥ID5取得
・予防接種DBへの接種記録等の連携時に個人を特定する識別子情報として、予診情報・予防接種記録管理／請求支払システムが履歴照会回答システム経由でID5を取得する。

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名		
予防接種ファイル		
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　※		住民基本台帳に記録された本市住民で予防接種の対象者
	その必要性	予防接種業務における重複通知の抑止及び未接種者への接種勧奨事務処理に利用する。
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，その他識別番号（内部番号）：本人確認及び内部情報照会の索引とするために必要 情報：本人確認資料のために必要 連絡先：本人に連絡事項があった際に連絡を取るために必要 健康・医療関係情報；予防接種履歴の管理のために必要 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		令和3年12月1日
⑥事務担当部署		保健福祉部　保健所　保健予防課

3. 特定個人情報の入手・使用		
①入手元 ※		[○] 本人又は本人の代理人 [○] 評価実施機関内の他部署 （ 市民課，生活福祉第1課，第2課 ） [○] 行政機関・独立行政法人等 （ 地方公共団体情報システム機構 ） [○] 地方公共団体・地方独立行政法人 （ 都道府県，他市町村 ） [○] 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		・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／請求支払システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・国が予診情報・予防接種記録管理／請求支払システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本市が個人情報を入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等又は医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。
④入手に係る妥当性		・予防接種を受けたものを特定し，接種歴を適切に記録・保管する必要がある。（予防接種法第9条の3及び予防接種法施行規則第3条） （PMHキー採番処理依頼時に入手される特定個人情報） ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 （その他：個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結び付き特定個人情報となる情報） 本市が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入手し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証（本人確認）の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。
⑤本人への明示		・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。 ・本人又は本人の代理人から入手する情報については、利用目的を明示した上で入手している。マイナポータル等では、本人又は本人の代理人が画面に表示された利用目的を確認して、本人確認することにより入手する。
⑥使用目的 ※		予防接種の実施に関して，住民情報，予防接種履歴の照会・入力等が必要なため。
	変更の妥当性	－
⑦使用の主体	使用部署 ※	保健福祉部 保健所 保健予防課
	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 ※		・本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。 ・本市からの転出者について，転出先市区町村へ当市区町村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。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・情報連携のため、本市は、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ・登録後、予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対してオンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予診情報・予防接種記録管理／請求支払システムに応答する。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予診情報・予防接種記録管理／請求支払システムで共有されることで予診情報・予防接種記録管理／請求支払システムからマイナポータルへの通知、マイナポータルや医療機関用アプリ等から予診情報・予防接種記録管理／請求支払システムの予診票情報及び接種記録の取得/閲覧/入力等といった情報連携が可能となる。
	情報の突合 ※	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。
	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		令和3年12月1日
4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] <選択肢> 1）委託する 2）委託しない （ 2 ） 件
委託事項1		健康管理システム運用管理委託
①委託内容		予防接種法等の改正に対応し，システム改修を行う。
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] <選択肢> 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[10万人以上100万人未満] <選択肢> 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	特定個人情報ファイルの範囲と同様
	その妥当性	システムの運用作業を実施するために，特定個人情報ファイル全体を委託の対象にする必要がある。 専門的ノウハウを有する者が管理することにより，法改正の内容に沿った管理が行える。
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 （ 市役所の入退室管理された情報室内にて，システムを直接操作する。 ）
⑤委託先名の確認方法		宇都宮市入札制度合理化対策実施要領に基づき，入札結果を公表する。
⑥委託先名		株式会社両備システムズ

再委託	⑦再委託の有無 ※	[　　再委託する　　] ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	委託先から提出された再委託承認申請に基づき，再委託の理由，再委託先の管理・監督方法，再委託先の名称，代表者及び所在地，再委託する業務内容，再委託する業務に含まれる情報の種類，再委託先のセキュリティ管理体制等により判断した上で，再委託を承認している。
	⑨再委託事項	システム改修に係る現地での要件定義，設計，プログラム製造，テスト作業
委託事項2～5		
委託事項2		予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱
①委託内容		予診情報・予防接種記録管理／請求支払システムの利用・情報連携業務及び運用保守業務
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの一部] ＜選択肢＞ 1）特定個人情報ファイルの全体 2）特定個人情報ファイルの一部
	対象となる本人の数	[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
	対象となる本人の範囲 ※	予防接種法等関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、〇〇県国民健康保険団体連合会（以下、〇〇県国保連合会という。）及び国保中央会は特定個人情報にアクセスすることはない。
③委託先における取扱者数		[　　10人以上50人未満　　] ＜選択肢＞ 1）10人未満　2）10人以上50人未満 3）50人以上100人未満　4）100人以上500人未満 5）500人以上1,000人未満　6）1,000人以上
④委託先への特定個人情報ファイルの提供方法		[　]専用線　[　]電子メール　[　]電子記録媒体（フラッシュメモリを除く。） [　]フラッシュメモリ　[　]紙 [〇]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		栃木県国保連合会
再委託	⑦再委託の有無 ※	[　　再委託する　　] ＜選択肢＞ 1）再委託する　2）再委託しない
	⑧再委託の許諾方法	書面又は電磁的方法による承諾
	⑨再委託事項	・予診情報・予防接種記録管理／請求支払システムの運用保守 ・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。

委託事項3		
①委託内容		
②取扱いを委託する特定個人情報ファイルの範囲		[ ] ＜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	[ ] ＜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 ※	
	その妥当性	
③委託先における取扱者数		[ ] ＜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		
⑥委託先名		
再委託	⑦再委託の有無 ※	[ ] ＜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 （ 1 ）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区町村長
①法令上の根拠	番号法第19条第8号別表に定める情報照会者
②提供先における用途	番号法第19条第8号別表に掲げる事務を処理するため
③提供する情報	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
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」と同一
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	本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
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 [ ] 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	
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		
①保管場所　※		＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜自治体中間サーバー・プラットフォームにおける措置＞ ①自治体中間サーバー・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自治体中間サーバーのデータベース内に保存され，バックアップもデータベース上に保存される。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務〉 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。なお、以下のとおりセキュリティ対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。
②保管期間	期間	［　定められていない　］ ＜選択肢＞ 1）1年未満　2）1年　3）2年 4）3年　5）4年　6）5年 7）6年以上10年未満　8）10年以上20年未満　9）20年以上 10）定められていない
	その妥当性	予防接種法施行令第６条の２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	＜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。 ＜中間サーバ・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・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。 ・ 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。 ・ 中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務〉 ・本市の領域に保管されたデータのみ、予診情報・予防接種記録管理／請求支払システムを用いて消去することができる。 ・本市区町村の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日（作成日）を起点として3年が経過した時点で、自動的に削除される。
7．備考	

（別添2）特定個人情報ファイル記録項目

予防接種情報ファイル

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　受診日（接種日）
12　受診年度（接種年度）
13　接種種別
14　接種回数
15　接種判定
16　接種日年齢
17　年度末年齢
18　基準日年齢
19　実施医療機関
20　問診医
21　接種医
22　接種番号
23　実施場所
24　メーカー
25　ロットナンバー
26　接種量
27　未接種理由
28　特記事項
29　予診フラグ
30　更新日
31　更新時刻
32　更新者職員番号

※　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。

<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加の記録項目>
(1)対象者情報
・個人番号
・PMHキー
・PMH仮名識別子
・基本5情報（カナ・氏名・住所・生年月日・性別）
・保護者氏名
・自治体コード
・自治体業務ID
・連携ファイル名
・連携日時
・連携処理ステータス/エラー内容
・制御フラグ（リカバリー/不開示/閲覧停止）
・変更区分
・消除の異動日
・その他管理番号・ID等（予防接種対象者番号）
・その他区分等（接種対象者区分/減免区分）
(2)ユーザー情報
・機関マスタID
・機関ユーザーID
・メールアドレス
・ユーザー氏名
・ユーザー区分
・ユーザー権限ID
・個人番号閲覧可能フラグ
・ユーザー削除フラグ

(3)予診票情報
・項目ID
・管理ID
・更新日時
・回答ID
・回答内容
・回答処理ステータス
・回答日時
・接種不可フラグ
・予防接種設定ID
・予防接種管理ID
・組み合わせ番号
・強制失効日
・勧奨情報（ルールID、勧奨日）
(4)予防接種記録情報
・予防接種記録ID
・予防接種管理ID
・接種日
・接種同意フラグ
・医療機関コード
・医師名
・実施場所
・実施区分
・接種区分
・GTINコード
・ワクチンメーカー名
・ワクチン名（ワクチン一般名/ワクチン通称/ワクチン販売名）
・ロット番号
・接種量
・接種部位
・接種方法
・ワクチン有効期限
・要注意接種フラグ
・特別の事情
・海外接種フラグ
・更新日時
・最新/削除フラグ
・その他区分等（接種対象者区分/減免区分）

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

1．特定個人情報ファイル名	
予防接種ファイル	
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	各種申請書等の受付時，窓口において届け出内容や母子健康手帳，身分証明書などの本人確認書類を確認することで，対象者以外の予防接種履歴等の情報入手を防止している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療機関の受付窓口で本人確認の後、医療機関用アプリ等又は顔認証端末でマイナンバーカードを利用した認証により本人の情報のみが対象者として連携される。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、マイナンバーカードを利用した認証により、本人以外からの情報の入力を防止する。 ・既存事務において本人確認を行った個人番号を既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムに連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。
必要な情報以外を入手することを防止するための措置の内容	・申請書等については，必要な情報のみを記載する様式とし，窓口での記載指導により必要な情報以外は記載させないようにする。 ・本人が必要な情報以外を誤って記載することがないように，記載要領を整備する。 ＜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的に制御している。 ・医療機関から医療機関用アプリ等を介して入力される際は、定められたインターフェース仕様に沿って決められたデータ項目のみが連携されるようシステム的に制御している。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、定められたデータ項目のみが入力されるようシステム的に制御している。 ・「生年月日等をチェックすることで紐付け誤りを防止する機能（以下、「紐付け誤り防止機能」という。）により、誤った情報が紐付けられるリスクを低減する。
その他の措置の内容	本人以外又は必要な情報以外を入手しないよう，取扱職員に対する教育を行う。
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	・窓口において申請等があった場合，記載された申請書等は，窓口から離席する際は携行する等，職員の管理下に置くことを徹底する。 ・保健情報管理システムを操作する職員に個別のユーザーIDと静脈認証を行っており，不適切な方法で特定個人情報の入手ができない仕組みとしている。 ・保健情報管理システムへのログイン履歴を管理しているため，誰がいつ何の情報を入手したかわかるようになっている。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予診情報・予防接種記録管理／請求支払システムへは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステム的に制御している。 ・予診情報・予防接種記録管理／請求支払システムのデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。
リスクへの対策は十分か	［　　十分である　　］　＜選択肢＞ 1）特に力を入れている　　2）十分である 3）課題が残されている

リスク3： 入手した特定個人情報が不正確であるリスク	
入手の際の本人確認の措置の内容	・窓口において，対面で本人確認書類の提示を受け、本人確認を行う。 ・個人番号カードがない場合には，統合端末により本人確認情報と個人番号の対応付けの確認を行う。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号は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。
個人番号の真正性確認の措置の内容	・個人番号カードの提示を受ける。 ・個人番号カードがない場合には，統合端末により本人確認情報と個人番号の対応付けの確認を行う。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号は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。
特定個人情報の正確性確保の措置の内容	・入手した情報は，提出された申請書等により突合し，確認している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 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	・個人情報の記載のある文書は，鍵付きの書庫に保管する。 ＜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／請求支払システムと支払基金の医療保険者等向け中間サーバーは、Public Medical Hubを経由した閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。 ・健康管理システムは、予診情報・予防接種記録管理／請求支払システムへの連携時にLGWAN回線による閉域網で接続され、通信内容は情報漏洩を防止するために暗号化される。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	

3. 特定個人情報の使用

リスク1： 目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
宛名システム等における措置の内容	番号連携システムは、法令に定められた部署以外からのアクセスが行えないような仕組みを構築する。 また，番号連携システムへは，権限のない者の接続を認めない。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予診情報・予防接種記録管理／請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予診情報・予防接種記録管理／請求支払システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。
事務で使用するその他のシステムにおける措置の内容	

その他の措置の内容		ー
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	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 1　ユーザーの認証方法 ・　業務端末から保健情報管理システムを利用する際，ユーザーID（職員番号）と生体認証（指静脈）による二要素認証を行い，認証後は利用機能の認可機能により，システム上で利用可能な機能を制限することで，利用を許可された者以外の不正利用が行えないよう制限している。 ・　システムの利用できる端末を管理・制御することにより，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。 2　なりすましが行われないための対策 生体認証（指静脈）によりシステムへログインすることで，なりすましによる利用を完全に排除している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市は、予診情報・予防接種記録管理／請求支払システムのアクセス権限を管理する管理者を定める。 ・予診情報・予防接種記録管理／請求支払システムのログインはユーザID・パスワードで行う。 ・予診情報・予防接種記録管理／請求支払システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予診情報・予防接種記録管理／請求支払システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。
アクセス権限の発効・失効の管理		[　行っている　] ＜選択肢＞ 1）行っている　2）行っていない
	具体的な管理方法	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 1　発効管理 所属長の許可を得た上で経営管理課に依頼を行い，経営管理課にてその必要性を十分確認した上で必要なアクセス権限を個人単位で付与している。 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、所属長が把握した上で、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。 2　失効管理 ・　職員等は，業務上必要がなくなった場合は，ユーザー登録を抹消するようにしている。 ・　利用者抹消（異動，退職等）に伴うユーザーIDの取扱いについて，人事課から随時情報提供を受けて，確実な失効を行っている。 ・　大量異動が行われる年度初めに，全てのユーザーIDのチェックを行い，不要なユーザーIDの失効を行っている。 ＜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	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ① 業務内容と従事者に対応したアクセス権限のパターンを作成し，担当業務以外の情報に無用にアクセスできないようにシステム上制限している。 ② 権限の付与は，所属長が管理権限を有する職員を必要最低限の人数で指定している。 ③ ユーザーIDの取扱い等について，離席時のログアウトの徹底等の運用ルールを定めている。 ④ 所属長は、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。 ＜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	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ① 情報システムの運用において実施した作業について，参照・更新履歴を記録している。 ② 各種アクセス記録及び情報セキュリティの確保に必要な記録（利用者，端末機，操作日時，操作内容等）を取得し，一定期間保存している。 ③ アクセス記録等が詐取，改ざん，誤消去等されないように，操作権限は必要最低限の人数にしか与えないなどの必要な措置を講じている。 ④ 個人を特定した検索および特定後の異動処理や帳票の印刷などの操作ログの記録を行っている。 ⑤ 記録したログについては，一定の期間保管し，定期に及び必要に応じて確認が行える仕組みとする。 ＜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＞ ・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		① 登録された端末以外からは，システムにアクセスできない仕組みとしている。 ② 端末PCについては，アクセス権限が付与された職員以外の不正アクセスの対策として，一定時間の離席の際に，自動ログオフを設定している。
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　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		1　教育・啓発 ・　各課で選任されている情報セキュリティ担当者を対象に，「情報セキュリティの普及・啓発に係る取組み」に必要な知識の習得及び意識レベルの向上を目的とした研修を実施している。 ・　毎年度，異動者（管理職を含む）及び新規採用の職員等を対象とした，情報セキュリティに関する研修を実施している。 ・　業務外での使用禁止を指導徹底している。 ・　定期的に情報セキュリティに関する自己点検を行っている。 ・　他市町村等での類似の事象が発生・報道された際には随時周知を行い注意喚起している。 2　違反行為を行った職員に対する措置 ・　違反行為を行った者に対して，宇都宮市個人情報保護条例第6章（罰則）規定及びその違反行為の程度によっては地方公務員法による懲戒の対象としている。 ＜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、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	① 業務上で必要なファイルの複製は，持出操作ができないようシステム上制御している。 ② 業務端末では外部記憶装置を使用しないよう周知して運用している。 ③ 委託契約上，委託先による特定個人情報の無断複製を禁止している。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置〉 ・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	
その他，特定個人情報の使用にあたり，以下の措置を講じる。 ① 一定時間操作がない場合，端末にロックがかかり，再度認証を行わなければ画面表示，操作を不可とすることで，長時間にわたる本人確認情報を表示させない。 ② 端末のディスプレイを，来庁者から見えない位置に置くとともに，覗き見防止フィルターにより担当職員外からの覗き見を制限している。 ③ 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。	
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	① 業者選定に際しては，本市の入札参加有資格者名簿登載業者であることを原則とし，同等業務の履行実績の有無，確認を行い，特定個人情報の保護を適切に行える委託先であることを確認する。 ② 契約時には個人情報等の保護に係る誓約書，業務従事者届，業務従事者の経歴書，業務従事者からの秘密保持に関する誓約書，実施体制図の提出，セキュリティ等に関する社員教育の実施状況の確認を義務付けている。 ③ 委託契約書に個人情報保護に関する規定を設けることで確実な業務履行を担保している。 〈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、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栃木県国保連合会に委託し、栃木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	委託契約書に以下の規定を設ける。 ・アクセス権限を付与する従業者数を必要最小限に限定する。 ・従業者に付与するアクセス権限を必要最小限にする。 ・アクセス者数と付与したアクセス権限を報告する。 庁内での作業では，委託先の申請を受けて従業者ごとにIDを発行し，担当者を限定するほか，アクセス権限を委託元で管理する。 ＜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	健康管理システム内での特定個人情報の更新・参照・発行の記録をアクセスログとして記録する。 （アクセスログ項目：処理日時、職員情報、部署情報、端末情報、処理事由、処理内容など）アクセスログは媒体に7年間保管している。 ＜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	個人情報の取扱いについて，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・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	個人情報の取扱いについて，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・委託先（再委託先及び再々委託先を含む。）には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・本市は委託契約に基づき、委託先（再委託先及び再々委託先を含む。）から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。

特定個人情報の消去ルール		[　　定めている　　] ＜選択肢＞ 1）定めている　　2）定めていない
	ルールの内容及びルール遵守の確認方法	委託契約書に，以下の措置をとる旨を規定する。 ① 個人情報を保有している場合，契約期間終了後若しくは保管期間の経過後，速やかに消去する。 ② 廃棄の際は廃棄履歴を作成し保存する。 ③ 委託契約の報告条項に基づき，定期的に特定個人情報の取扱いについて書面にて報告させ，必要があれば本市職員が現地調査する。 〈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	個人情報の取扱いについては，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。 ① 契約終了又は解除された後においても秘密保持すること。 ② 従事者に対して宇都宮市個人情報保護条例で定める罰則の教示を行うこと。 ③ 個人情報の収集の制限と適正管理を行うこと。 ④ 本市の許可なき個人情報の複写及び持ち出しの禁止 ⑤ 目的外の使用と第三者への提供の禁止 ⑥ 個人情報の返還と廃棄に関すること。 ⑦ 事故発生時の速やかな報告 ⑧ 契約事項の違反による損害賠償の担保 〈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〉 栃木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	委託契約書において，本市の承諾を得ない再委託を禁止している。また，承諾を得た場合でも通常の委託業務と同様の措置を義務付けている。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置〉 ・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、点検結果について栃木県国保連合会及び本市に年1回報告を行う。

その他の措置の内容	<予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> ・委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。
リスクへの対策は十分か	[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報ファイルの取扱いの委託におけるその他のリスク及びそのリスクに対する措置	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		**[ ] 提供・移転しない**
リスク1： 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転の記録	[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	① 共通基盤システム（庁内連携システム）による情報の移転を行う情報をあらかじめ仕様にて取り決め，住民情報の変更データ等を随時自動で提供する仕組みを構築している。仕様で定めた以外の情報の抜き取りを各システムから行うことは不可能で，共通基盤システム（庁内連携システム）への提供ログはシステム内に自動で保管され，刑事訴訟手続上の証拠保全のため，刑事訴訟法第250条第2項第4号（長期15年未満の懲役又は禁錮に当たる罪）の公訴時効である7年分保存している。随時でデータの移転を行う際は，対象データの使用目的や詳細を記載した依頼文書を移転先より提出させ，詳細を記録している。 ② 自動で移転を行うもの以外，つまり紙・電子媒体等による場合についても，自動で提供する仕組み同様に決裁行為をもって必要な許可の上に成立するものとし，その仕様・詳細について記録を残し，一定期間保存している。	
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	
ルールの内容及びルール遵守の確認方法	① 共通基盤システム（庁内連携システム）による情報の移転の仕様を定める際に関係各課と協議を行い，法令上の根拠等を確認した上でシステムを構築 し，適切なタイミングで自動で提供する仕組みを構築している。随時で行う際も，その都度不適切な移転でないことを確認し，決裁行為を経た上で行っている。 ② 特定個人情報の提供・移転については，宇都宮市個人情報保護条例の内容に基づき，ルールを定めている。	
その他の措置の内容	① 入室権限を厳格に管理している情報システム室にサーバを設置し，情報の持ち出しを制限している。 ② 共通基盤システム（庁内連携システム）において，特定個人情報ファイルを扱うシステムへのアクセス権限を有する者を厳格に管理し，基本的に電子記録媒体の接続は禁止しており，情報の持ち出しを制限している。 ③ 特定個人情報ファイルを扱うシステムへのアクセス権限を限定し，事務に必要な情報に限定して連携している。 ④ 特定個人情報の提供を行う場合は，許可された電子記録媒体を使用し，ファイルの暗号化，パスワード設定を行い，持ち出しすることとしている。	
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	
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	① 移転を行う情報をあらかじめ仕様にて取り決め，仕様で定めた以外の情報の抜き取りを各システムから行うことは制限されており，各システムへの提供ログはシステム内に自動で保管され，認証できない相手先への情報の移転はなされないことがシステム上担保されている。 ② 随時でデータの移転を行う際は，対象データの使用目的や詳細を記載した依頼文書を移転先より提出させ，詳細を記録している。媒体にて他課に移転する際は，パスワードの付与を行い，第三者への漏えいを防止している。 ③ 共通基盤システム（庁内連携システム）において，連携手段として情報連携の記録が逐一保存され，不適切な方法による特定個人情報の移転を防止している。	
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： 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	① 情報の移転はほとんどが共通基盤システム（庁内連携システム）を介した自動によるものである。随時の作業については，記録媒体を依頼所管課の担当者に直接手渡しすること等により誤移転を防いでいる。 ② システムごとにIDとパスワードを取り決め，認証行為を行った上で，定義したデータ種別・項目に限定して連携している。
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
特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）におけるその他のリスク及びそのリスクに対する措置	

6．情報提供ネットワークシステムとの接続	**[ ] 接続しない（入手） [ ] 接続しない（提供）**
リスク1： 目的外の入手が行われるリスク	
リスクに対する措置の内容	中間サーバー・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用照合リスト（※2）との照合を情報提供ネットワークシステムに求め，情報提供ネットワークシステムから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	1 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。 2 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が不正確であるリスク	
リスクに対する措置の内容	中間サーバー・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て，情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため，正確な照会対象者に係る特定個人情報を入手することが担保されている。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

リスク4： 入手の際に特定個人情報が漏えい・紛失するリスク	
リスクに対する措置の内容	1 本市における措置 法令（番号法）の規定により認められる機関以外からの情報提供要求を受け付けないよう，システムにより制御する。また，情報提供の記録（提供が認められなかった場合，その記録）を残す。 情報照会・情報提供の記録が逐一保存される仕組みが確立した庁内連携システムを通してやりとりすることで，不適切な方法で特定個人情報が漏えい・紛失することを防止する。 2 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。（※） 既存システムからの接続に対し認証を行い，許可されていないシステムからのアクセスを防止する仕組みを設けている。 情報照会が完了又は中断した情報照会結果については，一定期間経過後に当該結果を情報照会機能において自動で消去することにより，特定個人情報が漏えい・紛失するリスクを軽減している。 中間サーバーの職員認証・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。 3 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	1 本市における措置 法令（番号法）の規定により認められる機関以外からの情報提供要求を受け付けないよう，システムにより制御する。また，情報提供の記録（提供が認められなかった場合，その記録）を残す。 2 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用照合リストを情報提供ネットワークシステムから入手し，中間サーバにも格納して，情報提供機能により，照会許可用照会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，特定個人情報が不正に提供されるリスクに対応している。 特に慎重な対応が求められる情報については自動応答を行わないように自動応答不可フラグを設定し，特定個人情報の提供を行う際に，送信内容を改めて確認し，提供を行うことで，センシティブな特定個人情報が不正に提供されるリスクに対応している。 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	1 本市における措置 情報の提供は，権限を有する者だけが処理の実行が可能な仕組みとなっている。また，提供の記録を逐一保存することで，不適切な方法で提供されることを防止する。 2 中間サーバー・ソフトウェアにおける措置 ⑴ 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。 ⑵ 中間サーバーの職員認証・権限管理機能では，ログイン時の職員認証の他に，ログイン・ログアウトを実施した職員，時刻，操作内容の記録が実施されるため，不適切な接続端末の操作や，不適切なオンライン連携を抑止する仕組みになっている。 (※)暗号化・復号機能と，鍵情報及び照会許可用照合リストを管理する機能 3 中間サーバー・プラットフォームにおける措置 ⑴ 中間サーバーと各事務システム，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。 ⑵ 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。 ⑶ 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	1 本市における措置 誤った情報を提供・移転してしまうリスクへの措置 提供・移転する情報のチェックを行い，誤った情報が作成されないことをシステム上で担保する。 誤った相手に提供・移転してしまうリスクへの措置 共通基盤システム（庁内連携システム）では，番号法に基づき認められる情報のみ認められた相手にしか移転できないよう，システムの仕組みとして担保されている。 2 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の管理機能（※）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
1 本市における措置 本市では，情報提供ネットワークシステムとの全ての連携（接続）は，中間サーバーが行う構成となっており，情報提供ネットワークシステム側から，本市の業務システムへのアクセスはできない。 2 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。 3 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行うことで，中間サーバー・プラットフォームの事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。

7. 特定個人情報の保管・消去		
リスク1： 特定個人情報の漏えい・滅失・毀損リスク		
①NISC政府機関統一基準群	[政府機関ではない]	<選択肢> 1）特に力を入れて遵守している 2）十分に遵守している 3）十分に遵守していない 4）政府機関ではない
②安全管理体制	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
③安全管理規程	[十分に整備している]	<選択肢> 1）特に力を入れて整備している 2）十分に整備している 3）十分に整備していない
④安全管理体制・規程の職員への周知	[十分に周知している]	<選択肢> 1）特に力を入れて周知している 2）十分に周知している 3）十分に周知していない
⑤物理的対策	[十分に行っている]	<選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
具体的な対策の内容		1 本市における措置 宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 サーバー設置場所 サーバーを設置する情報システム室から外部に通ずるドアは最小限とし，ICカードと生体認証等にて立入を制限の上，入退室管理システムにより24時間入退室を監視している。 端末設置場所 ① 職員等は，パソコン等の端末について，第三者に使用されること又は情報システム管理者の許可なく情報を閲覧されることがないように，離席時の端末のロック等，適切な措置を講じている。 ② 業務終了後は，パソコン等の端末を施錠できる場所へ保管し又は事務所を施錠することで，盗難を防止している。 記録媒体・紙媒体の保管場所 ① 情報を記録した記録媒体や情報が印刷された文書等について，第三者に使用されること又は情報システム管理者の許可なく情報を閲覧されることがないように容易に閲覧されない場所（施錠可能な事務所内倉庫や保管庫）へ保管している。 ② 遠隔地保管を行うバックアップ用LTOメディアは，経営管理課が一括管理しており，所管課との受渡しは記録簿にて管理を行っている。 2 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。 ＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスの利用

⑥技術的対策	[　　十分に行っている　　]	＜選択肢＞ 1）特に力を入れて行っている　　2）十分に行っている 3）十分に行っていない
具体的な対策の内容	1　本市における措置 宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ウイルス対策 ①　職員等は記録媒体を使う場合，コンピューターウイルス等の感染を防止するために，本市が管理している記録媒体のみを利用している。 ②　サーバー及びパソコン等の端末に，コンピューターウイルス等の不正プログラム対策ソフトウェアを常駐させている。 ③　不正プログラム対策ソフトウェアを導入し，定期的に当該ソフトウェア及びパターンファイルの更新を実施し，常に最新の状態を保っている。 不正アクセス対策 ①　健康管理システムは，外部のインターネットと物理的に接続していない。 ②　情報システム管理者はセキュリティに関する事案を検知するため，情報システムを常時監視し，障害が起きた際にも速やかに対応できるようにしている。 2　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，ログの解析を行っている。 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っている。 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っている。 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。 ＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年10月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。）又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・予診情報・予防接種記録管理／請求支払システムは論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、予診情報・予防接種記録管理／請求支払システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予診情報・予防接種記録管理／請求支払システムとの通信は暗号化を行うことにより、	

		通信内容の秘匿及び盗聴防止の対応をしている。 ・本市の端末と予診情報・予防接種記録管理／請求支払システムとの通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。
⑦バックアップ		[十分に行っている] <選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑧事故発生時手順の策定・周知		[十分に行っている] <選択肢> 1）特に力を入れて行っている 2）十分に行っている 3）十分に行っていない
⑨過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[発生なし] <選択肢> 1）発生あり 2）発生なし
	その内容	ー
	再発防止策の内容	ー
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で安全管理措置を実施する。
その他の措置の内容		ー
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		既存住民基本台帳システムと日次で連携している。 <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	① ディスク交換やハード更改等の際は，保存された情報が読み出しできないよう，外部事業者による物理的破壊又は専用ソフト等を利用した完全消去を実施する。 ② 紙媒体は保管期間ごとに分けて保管し，保管期間が過ぎているものについて外部業者による溶解処理を行う。 【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	ー
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	1　本市における措置 担当部署において，評価書の記載内容どおりの運用がなされているか，年1回チェックを実施する。 2　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	1　本市における措置 定期的に内部監査を実施し，個人情報保護に関する規定・体制の整備，安全管理措置及び安全管理措置の職員への周知・教育等の状況を確認し，監査結果を踏まえて体制や規定を改善する。 2　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・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。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 本市は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に職員等の当該システムの利用を管理し、必要な監査を行う。
2. 従業者に対する教育・啓発		
従業者に対する教育・啓発		[　　十分に行っている　　] ＜選択肢＞ 1) 特に力を入れて行っている　2) 十分に行っている 3) 十分に行っていない
	具体的な方法	1　本市における措置 ①　職員に対しては，個人情報保護及び情報セキュリティに関する知識習得や意識レベルの向上を目的とした研修を行う。 ②　違反行為を行った者に対しては，その都度指導の上，違反行為の程度によっては懲戒の対象となりうる。 ③　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・研修の実施，個人情報の安全管理についての責任体制の整備，その他秘密保持に関する事項を記載し，遵守させる。 2　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・プラットフォームの運用に携わる職員及び事業者に対し，セキュリティ研修等を実施することとしている。 ②　中間サーバー・プラットフォームの業務に就く場合は運用規則等について研修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、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又はガバメントクラウド運用管理補助者が責任を有する。
ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。
具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。
＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞
　本市は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。

Ⅴ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	〒321-0974　宇都宮市竹林町９７２番地 宇都宮市　保健福祉部　保健所　保健予防課 電話番号：028-626-1114
②請求方法	・開示請求については，宇都宮市個人情報保護条例第１４条第１項の規定に基づき，個人情報開示請求書に必要事項を記入し，提出する。 ・訂正・利用停止請求については，宇都宮市個人情報保護条例第２３条第１項の規定に基づき，個人情報訂正等請求書に必要事項を記入し，提出する。
特記事項	市ホームページに開示請求の方法及び個人情報開示請求書を掲載している。
③手数料等	[　　有料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：　　）
④個人情報ファイル簿の公表	[　行っていない　]　＜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	〒321-0974　宇都宮市竹林町９７２番地 宇都宮市　保健福祉部　保健所　保健予防課 電話番号：028-626-1114
②対応方法	・問い合わせへの回答について，関係法令等に照らし，適切に回答する。 ・情報漏えい等の重大な事案に関する問い合わせについて，関係部署に速やかに連絡し，協議のうえ対応するとともに，再発防止策を検討する。

Ⅵ　評価実施手続

1．基礎項目評価	
①実施日	
②しきい値判断結果	［　　基礎項目評価及び全項目評価の実施が義務付けられる　　］ ＜選択肢＞ 1）基礎項目評価及び全項目評価の実施が義務付けられる 2）基礎項目評価及び重点項目評価の実施が義務付けられる（任意に全項目評価を実施） 3）基礎項目評価の実施が義務付けられる（任意に全項目評価を実施） 4）特定個人情報保護評価の実施が義務付けられない（任意に全項目評価を実施）
2．国民・住民等からの意見の聴取	
①方法	・パブリックコメント方式による意見募集を実施する。 ・実施に関しては，市ホームページ上で意見募集している旨掲載する。 ・市ホームページ，保健予防課，地区市民センター等において案の閲覧を行う。 ・意見は電子メール，FAX，郵送，持参にて受け付ける。
②実施日・期間	令和8年11月25日～令和8年12月24日（30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	宇都宮市個人情報保護運営審議会
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
	表紙 評価書名	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基礎項目評価書	予防接種に関する事務　基礎項目評価書	事前	
	表紙 個人のプライバシー等の権利利益の保護の宣言	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	予防接種に関する事務	事前	
	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	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	予防接種に関する事務	事前	
	Ⅰ基本情報 1. 特定個人情報ファイルを取り扱う事務 ②事務の概要	別添を参照	別添を参照	事前	
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム1	①システムの名称 保健情報管理システム	①システムの名称 健康管理システム	事前	
	Ⅰ基本情報 2. 特定個人情報ファイルを取り扱う事務において使用するシステム5	別添を参照	別添を参照	事前	
	（別添1）事務内容 （備考）	別添を参照	別添を参照	事前	
	Ⅱ特定個人情報ファイルの概要 2. 基本情報 ④記録される項目 その妥当性	個人番号，その他識別番号（内部番号）：本人確認及び内部情報照会の索引とするために必要 情報：本人確認資料のために必要 連絡先：本人に連絡事項があった際に連絡を取るために必要 健康・医療関係情報；予防接種履歴の管理のために必要	個人番号，その他識別番号（内部番号）：本人確認及び内部情報照会の索引とするために必要 情報：本人確認資料のために必要 連絡先：本人に連絡事項があった際に連絡を取るために必要 健康・医療関係情報；予防接種履歴の管理のために必要 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。	事前	
	Ⅱ特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ③入手の時期・頻度	・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 ・他市区町村から接種記録の照会を受ける都度	・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／請求支払システムがPMHキーの採番処理依頼時に都度、Public Medical Hubから特定個人情報を入手する。 ・国が予診情報・予防接種記録管理／請求支払システムに登録した予診票のひな形に対して、住民が接種前にマイナポータル等を介して予診票情報を入力することにより、本市が個人情報を入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。 ・接種時に、医療機関のタブレットに搭載された医療機関用アプリ等又は医療機関での顔認証端末を用いて、住民がマイナンバーカードで認証することにより、医療機関が入力した予診票情報、接種記録を個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結びついて特定個人情報となる。	事前	

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 ④入手に係る妥当性	・予防接種を受けたものを特定し，接種歴を適切に記録・保管する必要がある。（予防接種法第9条の3及び予防接種法施行規則第3条）	・予防接種を受けたものを特定し，接種歴を適切に記録・保管する必要がある。（予防接種法第9条の3及び予防接種法施行規則第3条） （PMHキー採番処理依頼時に入手される特定個人情報） ・特定個人情報は、外部との情報連携のため、PMHキーの採番処理依頼時にPublic Medical Hubを経由して医療保険者等向け中間サーバーから自動的に入手される。 （その他：個人情報として入手し、予診情報・予防接種記録管理／請求支払システムにおいて個人番号と結び付き特定個人情報となる情報） 本市が入手する特定個人情報のうち、既存事務と同様に予診票に事前入力される事項は、本人又は本人の代理人から情報を入手し、予診票の医師記入欄及び接種記録は、予防接種を実施する医療機関から入手する。 ・予診票の事前入力のオンライン化により、住民の利便性の向上が図られる。マイナポータルではマイナンバーカードによる認証（本人確認）の後、本人又は本人の代理人の同意に基づいて情報が入力される。接種を受託する医療機関は、当該情報確認し、接種の可否を判断する。 ・医療機関において、タブレットに搭載された医療機関用アプリ等を用いた予診票の確認・接種記録がオンライン化されることにより住民及び医療機関の利便性の向上が図られる。また、情報の入手期間が短縮されることにより行政事務の効率化が図られる。医療機関での本人確認後、医療機関用アプリ等又は顔認証端末を用いて本人又は本人の代理人がマイナンバーカードで認証することにより、医療機関が予診票情報を確認して予診・問診を行い、接種後に接種記録の入力を行う。	事前	
	Ⅱ特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑤本人への明示	・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。	・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。 ・本人又は本人の代理人から入手する情報については、利用目的を明示した上で入手している。マイナポータル等では、本人又は本人の代理人が画面に表示された利用目的を確認して、本人確認することにより入手する。	事前	
	Ⅱ特定個人情報ファイルの概要 3. 特定個人情報の入手・使用 ⑧使用方法	・本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。 ・本市からの転出者について，転出先市区町村へ当市区町村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。	・本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。 ・本市からの転出者について，転出先市区町村へ当市区町村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。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・情報連携のため、本市は、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び予防接種管理情報の紐付け及び登録を行う。 ・登録後、予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対してオンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hubを経由して予診情報・予防接種記録管理／請求支払システムに応答する。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルと予診情報・予防接種記録管理／請求支払システムで共有されることで予診情報・予防接種記録管理／請求支払システムからマイナポータルへの通知、マイナポータルや医療機関用アプリ等から予診情報・予防接種記録管理／請求支払システムの予診票情報及び接種記録の取得/閲覧/入力等といった情報連携が可能となる。	事前	
	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取り扱いの委託 委託事項1	保健情報管理システム	健康管理システム	事前	
	Ⅱ特定個人情報ファイルの概要 4. 特定個人情報ファイルの取り扱いの委託 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（特例臨時接種）事務に関するワクチン接種記録システム（VRS）内に記録されている令和6年9月30日時点の特定個人情報ファイルの保管	予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱	事前	
	Ⅱ特定個人情報ファイルの概要 6. 特定個人情報の保管・削除 ①保管場所	別添を参照	別添を参照	事前	
	Ⅱ特定個人情報ファイルの概要 6. 特定個人情報の保管・削除 ③消去方法	別添を参照	別添を参照	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2.特定個人情報の入手 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	各種申請書等の受付時，窓口において届け出内容や母子健康手帳，身分証明書などの本人確認書類を確認することで，対象者以外の予防接種履歴等の情報入手を防止している。	各種申請書等の受付時，窓口において届け出内容や母子健康手帳，身分証明書などの本人確認書類を確認することで，対象者以外の予防接種履歴等の情報入手を防止している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療機関の受付窓口で本人確認の後、医療機関用アプリ等又は顔認証端末でマイナンバーカードを利用した認証により本人の情報のみが対象者として連携される。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、マイナンバーカードを利用した認証により、本人以外からの情報の入力を防止する。 ・既存事務において本人確認を行った個人番号を既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムに連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2.特定個人情報の入手 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	・申請書等については，必要な情報のみを記載する様式とし，窓口での記載指導により必要な情報以外は記載させないようにする。 ・本人が必要な情報以外を誤って記載することがないように，記載要領を整備する。	・申請書等については，必要な情報のみを記載する様式とし，窓口での記載指導により必要な情報以外は記載させないようにする。 ・本人が必要な情報以外を誤って記載することがないように，記載要領を整備する。 ＜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的に制御している。 ・医療機関から医療機関用アプリ等を介して入力される際は、定められたインターフェース仕様に沿って決められたデータ項目のみが連携されるようシステム的に制御している。 ・本人が、マイナポータルへログインし、予診票情報を入力する際には、定められたデータ項目のみが入力されるようシステム的に制御している。 ・「生年月日等をチェックすることで紐付け誤りを防止する機能（以下、「紐付け誤り防止機能」という。）により、誤った情報が紐付けられるリスクを低減する。	事前	
	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 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	・窓口において申請等があった場合，記載された申請書等は，窓口から離席する際は携行する等，職員の管理下に置くことを徹底する。 ・保健情報管理システムを操作する職員に個別のユーザーIDと静脈認証を行っており，不適切な方法で特定個人情報の入手ができない仕組みとしている。 ・保健情報管理システムへのログイン履歴を管理しているため，誰がいつ何の情報を入手したかわかるようになっている。 ＜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)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。	・窓口において申請等があった場合，記載された申請書等は，窓口から離席する際は携行する等，職員の管理下に置くことを徹底する。 ・保健情報管理システムを操作する職員に個別のユーザーIDと静脈認証を行っており，不適切な方法で特定個人情報の入手ができない仕組みとしている。 ・保健情報管理システムへのログイン履歴を管理しているため，誰がいつ何の情報を入手したかわかるようになっている。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hubを経由した予診情報・予防接種記録管理／請求支払システムへは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステム的に制御している。 ・予診情報・予防接種記録管理／請求支払システムのデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2.特定個人情報の入手 リスク3：入手した特定個人情報が不正確であるリスク 入手の際の本人確認の措置の内容	・窓口において，対面で本人確認書類の提示を受け、本人確認を行う。 ・個人番号カードがない場合には，統合端末により本人確認情報と個人番号の対応付けの確認を行う。	・窓口において，対面で本人確認書類の提示を受け、本人確認を行う。 ・個人番号カードがない場合には，統合端末により本人確認情報と個人番号の対応付けの確認を行う。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号は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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2.特定個人情報の入手 リスク3：入手した特定個人情報が不正確であるリスク 個人番号の真正性確認の措置の内容	・個人番号カードの提示を受ける。 ・個人番号カードがない場合には，統合端末により本人確認情報と個人番号の対応付けの確認を行う。	・個人番号カードの提示を受ける。 ・個人番号カードがない場合には，統合端末により本人確認情報と個人番号の対応付けの確認を行う。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムが提供した個人番号は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。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2.特定個人情報の入手 リスク3：入手した特定個人情報が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	・入手した情報は，提出された申請書等により突合し，確認している。	・入手した情報は，提出された申請書等により突合し，確認している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 個人番号及び基本情報の正確性は、既存事務において住基システムとの連携等により担保されている。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2.特定個人情報の入手 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	・個人情報の記載のある文書は，鍵付きの書庫に保管する。	・個人情報の記載のある文書は，鍵付きの書庫に保管する。 ＜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。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用 リスク1：目的を超えた紐づけ，事務に必要のない情報との紐づ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	番号連携システムは、法令に定められた部署以外からのアクセスが行えないような仕組みを構築する。 また，番号連携システムへは，権限のない者の接続を認めない。	番号連携システムは、法令に定められた部署以外からのアクセスが行えないような仕組みを構築する。 また，番号連携システムへは，権限のない者の接続を認めない。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムにアクセスする本市の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・予診情報・予防接種記録管理／請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関用アプリ等や住民から予診情報・予防接種記録管理／請求支払システムに接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用 リスク2：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 ユーザー認証の管理 具体的な管理方法	別添を参照	別添を参照	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用 リスク2：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 アクセス権限の発行・失効の管理 具体的な管理方法	別添を参照	別添を参照	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用 リスク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	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ①　業務内容と従事者に対応したアクセス権限のパターンを作成し，担当業務以外の情報に無用 　にアクセスできないようにシステム上制限している。 ②　権限の付与は，所属長が管理権限を有する職員を必要最低限の人数で指定している。 ③　ユーザーIDの取扱い等について，離席時のログアウトの徹底等の運用ルールを定めている。 ④　所属長は、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。	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ①　業務内容と従事者に対応したアクセス権限のパターンを作成し，担当業務以外の情報に無用 　にアクセスできないようにシステム上制限している。 ②　権限の付与は，所属長が管理権限を有する職員を必要最低限の人数で指定している。 ③　ユーザーIDの取扱い等について，離席時のログアウトの徹底等の運用ルールを定めている。 ④　所属長は、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。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・共用IDは発行せず、必ず個人に対し、ユーザーIDを発行する。 ・管理者が定期的に管理表を確認し、必要に応じて見直しを行う。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用 リスク2：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	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ①　情報システムの運用において実施した作業について，参照・更新履歴を記録している。 ②　各種アクセス記録及び情報セキュリティの確保に必要な記録（利用者，端末機，操作日時， 　操作内容等）を取得し，一定期間保存している。 ③　アクセス記録等が詐取，改ざん，誤消去等されないように，操作権限は必要最低限の人数 　にしか与えないなどの必要な措置を講じている。 ④　個人を特定した検索および特定後の異動処理や帳票の印刷などの操作ログの記録を行っている。 ⑤　記録したログについては，一定の期間保管し，定期に及び必要に応じて確認が行える仕組みとする。	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ①　情報システムの運用において実施した作業について，参照・更新履歴を記録している。 ②　各種アクセス記録及び情報セキュリティの確保に必要な記録（利用者，端末機，操作日時， 　操作内容等）を取得し，一定期間保存している。 ③　アクセス記録等が詐取，改ざん，誤消去等されないように，操作権限は必要最低限の人数 　にしか与えないなどの必要な措置を講じている。 ④　個人を特定した検索および特定後の異動処理や帳票の印刷などの操作ログの記録を行っている。 ⑤　記録したログについては，一定の期間保管し，定期に及び必要に応じて確認が行える仕組みとする。 ＜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＞ ・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	
	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	1　教育・啓発 ・　各課で選任されている情報セキュリティ担当者を対象に，「情報セキュリティの普及・啓発に係る取組み」に必要な知識の習得及び意識レベルの向上を目的とした研修を実施している。 ・　毎年度，異動者（管理職を含む）及び新規採用の職員等を対象とした，情報セキュリティに関する研修を実施している。 ・　業務外での使用禁止を指導徹底している。 ・　定期的に情報セキュリティに関する自己点検を行っている。 ・　他市町村等での類似の事象が発生・報道された際には随時周知を行い注意喚起している。 2　違反行為を行った職員に対する措置 ・　違反行為を行った者に対して，宇都宮市個人情報保護条例第6章（罰則）規定及びその違反行為の程度によっては地方公務員法による懲戒の対象としている。	1　教育・啓発 ・　各課で選任されている情報セキュリティ担当者を対象に，「情報セキュリティの普及・啓発に係る取組み」に必要な知識の習得及び意識レベルの向上を目的とした研修を実施している。 ・　毎年度，異動者（管理職を含む）及び新規採用の職員等を対象とした，情報セキュリティに関する研修を実施している。 ・　業務外での使用禁止を指導徹底している。 ・　定期的に情報セキュリティに関する自己点検を行っている。 ・　他市町村等での類似の事象が発生・報道された際には随時周知を行い注意喚起している。 2　違反行為を行った職員に対する措置 ・　違反行為を行った者に対して，宇都宮市個人情報保護条例第6章（罰則）規定及びその違反行為の程度によっては地方公務員法による懲戒の対象としている。 ＜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、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	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用 リスク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	①　業務上で必要なファイルの複製は，持出操作ができないようシステム上制御している。 ②　業務端末では外部記憶装置を使用しないよう周知して運用している。 ③　委託契約上，委託先による特定個人情報の無断複製を禁止している。	①　業務上で必要なファイルの複製は，持出操作ができないようシステム上制御している。 ②　業務端末では外部記憶装置を使用しないよう周知して運用している。 ③　委託契約上，委託先による特定個人情報の無断複製を禁止している。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置〉 ・既存システム（各業務システム）から特定個人情報を抽出したCSVファイルを予診情報・予防接種記録管理／請求支払システムへ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・本市の既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムへの特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線（LGWAN又はその他の閉域網回線）を利用した接続のみが認められる。 ・予診情報・予防接種記録管理／請求支払システムでは、権限のある者しか個人番号にはアクセスできないように制御している。 ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	①　業者選定に際しては，本市の入札参加有資格者名簿登載業者であることを原則とし，同等業務の履行実績の有無，確認を行い，特定個人情報の保護を適切に行える委託先であることを確認する。 ②　契約時には個人情報等の保護に係る誓約書，業務従事者届，業務従事者の経歴書，業務従事者からの秘密保持に関する誓約書，実施体制図の提出，セキュリティ等に関する社員教育の実施状況の確認を義務付けている。 ③　委託契約書に個人情報保護に関する規定を設けることで確実な業務履行を担保している。	①　業者選定に際しては，本市の入札参加有資格者名簿登載業者であることを原則とし，同等業務の履行実績の有無，確認を行い，特定個人情報の保護を適切に行える委託先であることを確認する。 ②　契約時には個人情報等の保護に係る誓約書，業務従事者届，業務従事者の経歴書，業務従事者からの秘密保持に関する誓約書，実施体制図の提出，セキュリティ等に関する社員教育の実施状況の確認を義務付けている。 ③　委託契約書に個人情報保護に関する規定を設けることで確実な業務履行を担保している。 〈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、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栃木県国保連合会に委託し、栃木県国保連合会は国保中央会に再委託することとする。 特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）に基づき、国保中央会の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	委託契約書に以下の規定を設ける。 ・アクセス権限を付与する従業者数を必要最小限に限定する。 ・従業者に付与するアクセス権限を必要最小限にする。 ・アクセス者数と付与したアクセス権限を報告する。 庁内での作業では，委託先の申請を受けて従業者ごとにIDを発行し，担当者を限定するほか， アクセス権限を委託元で管理する。	委託契約書に以下の規定を設ける。 ・アクセス権限を付与する従業者数を必要最小限に限定する。 ・従業者に付与するアクセス権限を必要最小限にする。 ・アクセス者数と付与したアクセス権限を報告する。 庁内での作業では，委託先の申請を受けて従業者ごとにIDを発行し，担当者を限定するほか， アクセス権限を委託元で管理する。 〈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〉 ・本市がアクセス権限の管理状況を確認できる。 ・本市は、アクセス権限を付与する者を必要最小限に限定する。 ・本市は、アクセス権限を付与する範囲を必要最小限に限定する。 ・本市は、アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再々委託先（PMHキー採番や運用保守）のみに付与される。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取り扱いの記録 具体的な制限方法	保健情報管理システム内での特定個人情報の更新・参照・発行の記録をアクセスログとして記録する。 （アクセスログ項目：処理日時、職員情報、部署情報、端末情報、処理事由、処理内容など）アクセス ログは媒体に7年間保管している。	健康管理システム内での特定個人情報の更新・参照・発行の記録をアクセスログとして記録する。 （アクセスログ項目：処理日時、職員情報、部署情報、端末情報、処理事由、処理内容など）アクセス ログは媒体に7年間保管している。 〈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／請求支払システムは特定個人情報の取り扱いのログを保存し、本市は特定個人情報に係る操作のログを閲覧・出力できる。 ※再々委託先（PMHキー採番や運用保守）に係る特定個人情報の取扱いログに限られる。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 委託先から他者への提供に関するルールの内容及びルール遵守の確認方法	個人情報の取扱いについて，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。	個人情報の取扱いについて，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置〉 ・委託先（再委託先及び再々委託先を含む。）から他者への提供は行わない。 ・本市は委託契約に基づき、委託先（再委託先及び再々委託先を含む。）から他者への提供が行われていないことを確認できる。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 特定個人情報の提供ルール 委託元と委託先間の提供に関するルールの内容及びルール遵守の確認方法	個人情報の取扱いについて，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。	個人情報の取扱いについて，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置〉 ・委託先（再委託先及び再々委託先を含む。）には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・本市は委託契約に基づき、委託先（再委託先及び再々委託先を含む。）から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 特定個人情報の消去ルール ルールの内容及びルール遵守の確認方法	委託契約書に，以下の措置をとる旨を規定する。 ①　個人情報を保有している場合，契約期間終了後若しくは保管期間の経過後，速やかに消去する。 ②　廃棄の際は廃棄履歴を作成し保存する。 ③　委託契約の報告条項に基づき，定期的に特定個人情報の取扱いについて書面にて報告させ，必要があれば本市職員が現地調査する。	委託契約書に，以下の措置をとる旨を規定する。 ①　個人情報を保有している場合，契約期間終了後若しくは保管期間の経過後，速やかに消去する。 ②　廃棄の際は廃棄履歴を作成し保存する。 ③　委託契約の報告条項に基づき，定期的に特定個人情報の取扱いについて書面にて報告させ，必要があれば本市職員が現地調査する。 〈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、本市区町村は消去について国保中央会から報告を受けることができ、それにより消去状況について確認が可能と	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 委託契約書中の特定個人情報ファイルの取り扱いに関する規定 既定の内容	別添を参照	別添を参照	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 再委託先による特定個人情報ファイルの適切な取扱いの確保 具体的な方法	追加	委託契約書において，本市の承諾を得ない再委託を禁止している。また，承諾を得た場合でも通常の委託業務と同様の措置を義務付けている。 〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置〉 ・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、点検結果について栃木県国保連合会及び本市に年１回報告を行う。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 その他の措置の内容	追加	〈予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置〉 ・委託契約書に以下の規定を設ける。 委託先及び再委託先は、従業者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。	事前	
	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：特定個人情報の漏洩・滅失・毀損リスク ⑤物理的リスク 具体的な対策の内容	別添を参照	別添を参照	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去 リスク1：特定個人情報の漏洩・滅失・毀損リスク ⑥技術的リスク 具体的な対策の内容	別添を参照	別添を参照	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去 リスク2：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	既存住民基本台帳システムと日次で連携している。	既存住民基本台帳システムと日次で連携している。 <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。	事前	
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去 リスク3：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	①　ディスク交換やハード更改等の際は，保存された情報が読み出しできないよう，外部事業者による物理的破壊又は専用ソフト等を利用した完全消去を実施する。 ②　紙媒体は保管期間ごとに分けて保管し，保管期間が過ぎているものについて外部業者による溶解処理を行う。 【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。	①　ディスク交換やハード更改等の際は，保存された情報が読み出しできないよう，外部事業者による物理的破壊又は専用ソフト等を利用した完全消去を実施する。 ②　紙媒体は保管期間ごとに分けて保管し，保管期間が過ぎているものについて外部業者による溶解処理を行う。 【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。	事前	
	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	1　本市における措置 　担当部署において，評価書の記載内容どおりの運用がなされているか，年1回チェックを実施する。 2　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。	1　本市における措置 　担当部署において，評価書の記載内容どおりの運用がなされているか，年1回チェックを実施する。 2　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。	事前	
	Ⅳ　その他のリスク対策 1.監査 ②監査 具体的な内容	1　本市における措置 　定期的に内部監査を実施し，個人情報保護に関する規定・体制の整備，安全管理措置及び安全管理措置の職員への周知・教育等の状況を確認し，監査結果を踏まえて体制や規定を改善する。 2　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・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。	1　本市における措置 　定期的に内部監査を実施し，個人情報保護に関する規定・体制の整備，安全管理措置及び安全管理措置の職員への周知・教育等の状況を確認し，監査結果を踏まえて体制や規定を改善する。 2　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・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。 <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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
	Ⅳ　その他のリスク対策 2従事者に対する教育・啓発 従事者に対する教育・啓発 具体的な方法	1　本市における措置 ①　職員に対しては，個人情報保護及び情報セキュリティに関する知識習得や意識レベルの向上を目的とした研修を行う。 ②　違反行為を行った者に対しては，その都度指導の上，違反行為の程度によっては懲戒の対象となりうる。 ③　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・研修の実施，個人情報の安全管理についての責任体制の整備，その他秘密保持に関する事項を記載し，遵守させる。 2　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・プラットフォームの運用に携わる職員及び事業者に対し，セキュリティ研修等を実施することとしている。 ②中間サーバー・プラットフォームの業務に就く場合は運用規則等について研修を行うこととしている。	1　本市における措置 ①　職員に対しては，個人情報保護及び情報セキュリティに関する知識習得や意識レベルの向上を目的とした研修を行う。 ②　違反行為を行った者に対しては，その都度指導の上，違反行為の程度によっては懲戒の対象となりうる。 ③　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・研修の実施，個人情報の安全管理についての責任体制の整備，その他秘密保持に関する事項を記載し，遵守させる。 2　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・プラットフォームの運用に携わる職員及び事業者に対し，セキュリティ研修等を実施することとしている。 ②中間サーバー・プラットフォームの業務に就く場合は運用規則等について研修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、適切な指導を行う。	事前	
	Ⅳ　その他のリスク対策 3.その他のリスク対策	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又はガバメントクラウド運用管理補助者が責任を有する。 ガバメントクラウド上での業務アプリケーションの運用等に障害が発生する場合等の対応については、原則としてガバメントクラウドに起因する事象の場合は、国はクラウド事業者と契約する立場から、その契約を履行させることで対応する。また、ガバメントクラウドに起因しない事象の場合は、地方公共団体に業務アプリケーションサービスを提供するASP又はガバメントクラウド運用管理補助者が対応するものとする。具体的な取り扱いについて、疑義が生じる場合は、地方公共団体とデジタル庁及び関係者で協議を行う。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 本市は、情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。	事前	