特定個人情報保護評価書（重点項目評価書）

評価書番号	評価書名
25	健康増進法に基づく健康診査等の実施に関する事務　重点項目評価書

個人のプライバシー等の権利利益の保護の宣言
吹田市は、健康増進法に基づく健康診査等の実施に関する事務において特定個人情報ファイルを取り扱うにあたり、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うることを認識し、特定個人情報の漏えいその他の事態が発生するリスクを軽減させるため、番号法及び個人情報保護に関する法令を遵守するとともに、特定個人情報ファイルの保護と安全な利用について適切な措置を実施することで、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
大阪府吹田市長

公表日
令和7年10月24日

［令和7年5月　様式3］

項目一覧

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	健康増進法に基づく健康診査等の実施に関する事務
②事務の内容	吹田市では、健康増進法に基づき市民の健康増進のため各種健康診査、健康診査結果を基にした保健指導等を行っている。 【評価対象事務の概要】 行政手続における特定の個人を識別するための番号の利用に関する法律（以下、「番号法」という。）の規定に従い、特定個人情報を市民の健康に関する事務について取り扱う。 （事務内容） ①健康増進法等に基づく各種健康診査（胃・肺・大腸・子宮・乳がん検診、骨粗しょう症検診、B型C型肝炎ウィルス検診、吹田市歯科健康診査）の実施 ②健康診査の結果通知、受診勧奨、健康手帳の交付等の事務 ③がん検診受診者で要精検者への受診勧奨及び管理に伴う事務 ④疾病予防その他健康に関する健康教育・相談等、保健指導の実施または受診勧奨に関する事務 ⑤番号法に基づき、情報提供に必要な個人情報の提供 ⑥情報提供ネットワークシステムを通じた各関係機関等との情報連携 ⑦成人保健事務の実施に必要な情報の取得 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務＞ ・情報連携のため、本市区町村は、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む受診者情報、問診情報及び検診結果の紐付け及び登録を行う。 ・住民は、マイナポータル等を介して問診情報の入力、検診結果及び通知の取得/閲覧が可能となる。 ・住民が、検診時に、従来の紙の問診票に代えて、マイナンバーカードをタブレットに搭載された検診施設アプリ又は医療機関のシステムで用いることにより、医療機関・検診会場（以下、検診施設等）において住民が事前に入力した問診情報、検診結果の取得/閲覧/入力が可能となる。 ・自治体は、検診施設等から入力された問診情報、検診結果の取得及び住民への通知が可能となる。
③対象人数	[　10万人以上30万人未満　] ＜選択肢＞ 1) 1,000人未満　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

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	健康情報管理システム（成人保健）
②システムの機能	1. 照会機能　：住民基本情報を検索、照会する機能 2. 検診予約管理機能　：集団検診の予約項目の入力、修正、削除する機能 3. 帳票発行機能　：集団検診の宛名書、検診料免除証明書、結果通知書等の発行機能 4. 検診情報登録　：健（検）診結果の情報を登録し、個人ごとに台帳として管理する機能 5. 統計機能　：検診受診履歴を国、府への報告用に集計する機能 6. 情報照会機能　：中間サーバコネクタを通じ、特定個人情報（連携対象）の照会及び提供、受領（照会した情報の受領）する機能
③他のシステムとの接続	[　] 情報提供ネットワークシステム　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　[　] 既存住民基本台帳システム [○] 宛名システム等　[　] 税務システム [○] その他　（ 中間サーバコネクタ　）
システム2～5	
システム2	
①システムの名称	中間サーバ
	【符号管理機能】 ・符号管理機能は、情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する。 【情報照会機能】 ・情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会及び情報提供受領（照会した情報の受領）を行う。 【情報提供機能】 ・情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報（連携対象）の提供を行う。

②システムの機能	【既存システム接続機能】 ・中間サーバーと既存システム、宛名システム及び住民記録システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携する。 【情報提供等記録管理機能】 ・特定個人情報（連携対象）の照会、又は提供があった旨の情報提供等記録を生成し、管理する。 【情報提供データベース管理機能】 ・特定個人情報（連携対象）を副本として、保持・管理する。 【データ送受信機能】 ・中間サーバ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。 【セキュリティ管理機能】 【職員認証・権限管理機能】 ・中間サーバ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。 【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、稼動状態の通知、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3	
①システムの名称	Public Medical Hub　（PMH）
②システムの機能	＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務＞ ①雛形の登録 問診票項目、通知文言等の雛形をPublic Medical Hub（PMH）へ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 本市区町村で管理している個人番号、受診者情報、問診情報及び検診結果をPublic Medical Hub（PMH）に登録し、社会保険診療報酬支払基金（以下、「支払基金」という。なお、今後「医療情報基盤・診療報酬審査支払機構」に改名予定）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 マイナポータルからのPublic Medical Hub（PMH）初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けてPublic Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 自治体検診の対象者は、マイナポータルへログインしてマイナンバーカードの電子証明書のシリアル番号に紐付くPMH仮名識別子を利用した照会を行う。Public Medical Hub（PMH）は、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く検診結果・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問診票の入力画面から情報を入力することにより、Public Medical Hub（PMH）はPMH仮名識別子からPMHキーを特定し、PMHキーに紐付く問診情報を登録する。 ④情報連携機能（検診施設アプリ） ・識別子の格納機能 検診施設アプリはマイナンバーカードの電子証明書のシリアル番号を用いてマイナポータル経由でPublic Medical Hub（PMH）に接続する。検診施設アプリからのPublic Medical Hub（PMH）初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けてPublic Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 検診施設アプリは、マイナンバーカードの電子証明書のシリアル番号を用いてマイナポータル経由で、Public Medical Hub（PMH）へPMH仮名識別子を利用した照会を行う。Public Medical Hub（PMH）は、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く問診情報を検診施設アプリに提供する。また、検診施設等が検診結果の入力画面から情報を入力することにより、Public Medical Hub（PMH）はPMH仮名識別子からPMHキーを特定し、PMHキーに紐付く検診結果を登録する。
	[　] 情報提供ネットワークシステム　　[　] 庁内連携システム

③他のシステムとの接続	[　] 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、医療保険者等向け中間サーバー、検診施設アプリ）
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	
健康増進事業情報管理ファイル	
4. 個人番号の利用 ※	
法令上の根拠	・番号法第9条第1項　別表111の項 ・番号法別表の主務省令で定める事務を定める命令第54条 ・番号法第19条第6号（委託先への提供）
5. 情報提供ネットワークシステムによる情報連携 ※	
①実施の有無	[　　実施する　　]　　＜選択肢＞ 1) 実施する 2) 実施しない 3) 未定
②法令上の根拠	【個人情報の照会】 ・番号法第19条第8号に基づく主務省令第2条の表139の項 【個人情報の提供】 ・番号法第19条第8号に基づく主務省令第2条の表139の項
6. 評価実施機関における担当部署	
①部署	健康医療部　成人保健課
②所属長の役職名	課長
7. 他の評価実施機関	

Ⅱ　特定個人情報ファイルの概要

1. 特定個人情報ファイル名	
健康増進事業情報管理ファイル	
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 ※	住民基本台帳記載の吹田市住民(転出、死亡等の事由により住民票が削除された者を含む。)で、健康診査等の対象者。
その必要性	健康増進法に基づく健康診査事務を行うにあたり、住民が事業の対象者であるかの確認をした上で、健康診査の記録、検診の予約管理、受診勧奨通知の発送等を行う必要があるため。
④記録される項目	[　　100項目以上　　] ＜選択肢＞ 1）10項目未満　2）10項目以上50項目未満 3）50項目以上100項目未満　4）100項目以上
主な記録項目 ※	・識別情報 [○] 個人番号　[○] 個人番号対応符号　[○] その他識別情報（内部番号） ・連絡先等情報 [○] 5情報（氏名、氏名の振り仮名、性別、生年月日、住所）　[○] 連絡先（電話番号等） [○] その他住民票関係情報 ・業務関係情報 [　] 国税関係情報　[○] 地方税関係情報　[○] 健康・医療関係情報 [　] 医療保険関係情報　[　] 児童福祉・子育て関係情報　[　] 障害者福祉関係情報 [　] 生活保護・社会福祉関係情報　[　] 介護・高齢者福祉関係情報 [　] 雇用・労働関係情報　[　] 年金関係情報　[　] 学校・教育関係情報 [　] 災害関係情報 [○] その他　（ Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務＞ ・自治体検診記録情報　）
その妥当性	【個人番号対応符号】 中間サーバーコネクタを通じ、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）を行うため 【識別情報】 健（検）診の対象者を特定するため 【連絡先等情報】 健（検）診票の送付及び受診勧奨等の通知、また、届出内容の不備等の際に問い合わせを行うため 【地方税関係情報】 検診費用助成の要件確認を行うため 【健康・医療関係情報】 対象者の健（検）診情報を健（検）診記録として適正に記録・保管するため <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> ・識別情報（その他識別情報） PMHキー、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 検診管理番号…PMH内で検診の種類を区別するために必要となる。 ・業務関係情報（その他） 検診情報…PMH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1を参照。
⑤保有開始日	平成27年10月1日
⑥事務担当部署	健康医療部　成人保健課

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　（ 住民票担当部署、市民税担当部署 ） [　] 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　（ ） [○] 民間事業者　（ 検診施設等、支払基金 ） [　] その他　（ ）
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　（ 医療保険者等向け中間サーバー、検診施設アプリ、マイナポータル ）
③使用目的 ※		健康増進事業の実施に関して、住民情報、検診結果情報の照会、入力等が必要なため。
④使用の主体	使用部署	健康医療部　成人保健課
	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
⑤使用方法		①健康増進法等に基づく各種健康診査（胃・肺・大腸・子宮・乳がん検診、骨粗しょう症検診、B型C型肝炎ウィルス検診、吹田市歯科健康診査）の実施 ②健康診査の結果通知、受診勧奨、健康手帳の交付等の事務 ③がん検診受診者で要精検者への受診勧奨及び管理に伴う事務 ④疾病予防その他健康に関する健康教育・相談等、保健指導の実施または受診勧奨に関する事務 <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> ・情報連携のため、本市区町村は、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む受診者情報、問診情報及び検診結果の紐付け及び登録を行う。 ・登録後、Public Medical Hub（PMH）は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub（PMH）が連動するためのPMH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（PMH）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Public Medical Hub（PMH）で共有されることでPublic Medical Hub（PMH）からマイナポータルへの通知、マイナポータルや検診施設アプリ（マイナポータル経由）からPublic Medical Hub（PMH）の問診情報及び検診結果の取得/閲覧/入力等といった情報連携が可能となる。
	情報の突合	氏名、生年月日、住所等により本人を検索し住民情報、検診履歴を確認する。
⑥使用開始日		平成28年1月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 4 ） 件
委託事項1		情報管理システム入力データ作成業務
①委託内容		健(検)診受診票(紙)に記載されている内容(個人番号は含まれない)のうち検診台帳に必要な項目の電子データ化
②委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
③委託先名		株式会社インターフェイス
再委託	④再委託の有無 ※	[再委託しない] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項2～5		
委託事項2		システムの運用・保守業務、法制度改正に伴う改修作業業務
①委託内容		システム運用・保守業務、法制度改正に伴う改修作業、ガバメントクラウド移行及び標準準拠システム移行業務
②委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
③委託先名		株式会社両備システムズ
再委託	④再委託の有無 ※	[再委託しない] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項3		健康情報管理システム(成人保健)のうち共通基盤部分の構築･運用業務
①委託内容		健康情報管理システム(成人保健)のうち共通基盤部分の構築･運用業務の委託
②委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
③委託先名		日本電気株式会社
再委託	④再委託の有無 ※	[再委託する] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑤再委託の許諾方法	再委託の制限事項内で本市が認める場合、委託先からの書面による申請に基づき、許諾
	⑥再委託事項	健康情報管理システムのうち共通基盤部分の構築･運用業務の一部
委託事項4		遠隔地保管
①委託内容		特定個人情報データ滅失等に備えたデータバックアップデータの遠隔地保管
②委託先における取扱者数		[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
③委託先名		日本電気株式会社

再委託	④再委託の有無 ※	[再委託しない] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑤再委託の許諾方法	
	⑥再委託事項	
委託事項5		Public Medical Hub（PMH）を活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱
①委託内容		Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務
②委託先における取扱者数		[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
③委託先名		国（デジタル庁）
再委託	④再委託の有無 ※	[再委託する] ＜選択肢＞ 1）再委託する 2）再委託しない
	⑤再委託の許諾方法	書面又は電磁的方法による承諾
	⑥再委託事項	PMHキーの付与、情報連携業務及び運用保守業務
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	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139の項
②提供先における用途	健康増進法による健康増進事業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	健康増進事業の実施に関する情報
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	健康増進法第19条の二、第19条の四の対象となる者
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	①の照会の都度、または他市町村への検診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

保管場所 ※	【吹田市における措置】 ・入退室管理区域内に設置するサーバー内に保管する。管理区域については、入室権限を持つ者を限定し、入退室管理カードにより権限の有無の確認し、入退室者名と時刻を記録するなど入退室管理を行っている。 ・届出書等も保管年限内は、鍵付の文書保管倉庫内での保管を義務付けている。 ・文書保管倉庫の最終退出者は、退出時に施錠を行っており、外部の者が入室できないようにしている。 ・ガバメントクラウド移行後は、クラウド事業者において国が認可しているAWSにサーバーが設置され、クラウド事業者のデータセンター（IDC）を経由して運用する。クラウド事業者のデータセンター（IDC）は、セキュリティレベルや生態認証等が設けられておりセキュリティが担保されている。 【中間サーバ・プラットフォームにおける措置】 ・中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバ室への入室を厳重に管理する。 ・特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。 【ガバメントクラウドにおける措置】 ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> Public Medical Hub（PMH）は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。なお、以下のとおりセキュリティ対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・論理的に区分された本市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国（デジタル庁）や検診施設等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。

7. 備考

<Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務>
・本市区町村の領域に保管されたデータのみ、Public Medical Hub（PMH）を用いて消去することができる。
・本市区町村の領域に保管されたデータは、他機関から消去できない。
※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、
　消去することができない。
・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。
・不要となったバックアップファイルは、古いものから順に自動削除される。

（別添1）特定個人情報ファイル記録項目

健康情報管理システムデータファイル（健康増進事業情報関連）

個人基本情報

項番	項目
1	識別番号
2	履歴番号
3	世帯番号
4	住民種別
5	住民状態
6	個人番号
7	氏名漢字
8	氏名フリガナ
9	性別
10	生年月日（日付）
11	続柄
12	世帯者氏名漢字
13	世帯者氏名フリガナ
14	現住所
15	現方書
16	現郵便番号
17	前住所
18	前方書
19	前郵便番号
20	転出先住所コード
21	転出先住所
22	転出先方書
23	転出先郵便番号
24	転出先区分
25	住民票記載住民年月日
26	本来の住民となった年月日
27	住民となった届出年月日
28	住民となった増異動事由
29	住所を定めた異動年月日
30	住所を定めた届出年月日
31	住所を定めた異動事由
32	住民でなくなった異動年月日
33	住民でなくなった異届出年月日
34	住民でなくなった減異動事由
35	異動事由
36	国籍地域
37	通称名漢字
38	通称名フリガナ
39	アルファベット氏名
40	漢字併記氏名
41	氏名カタカナ表記
42	市内住所コード
43	異動日
44	異動届出日
45	詳細異動事由
46	現住所（本番）
47	現住所（枝番）

健康増進事業関係情報（共通）

項番	項目
60	健（検）診種別
61	健（検）診日
62	健（検）診場所
63	市内医療機関情報
64	市外医療機関情報
65	健康手帳発行の有無
66	国保の有無
67	請求年月
68	相当年度（課税すべき年度）
69	課税非課税区分
70	未申告区分
71	市区町村民税額
72	市区町村民税均等割額
73	市区町村民税所得割額
74	更新年月日
75	更新者氏名
76	更新回数

健康増進事業関係情報（各種がん検診等）

項番	項目
77	カルテ番号
78	結果区分
79	事後方針
80	精密検査実施場所
81	精検医療機関情報
82	精検年月日
83	精密検査結果
84	費用徴収区分
85	パンチ処理日
86	グループ番号
87	ID
88	連番

健康増進事業関係情報（健康診査）

項番	項目
89	身体計測
90	血圧測定
91	尿検査
92	心電図検査
93	眼底検査
94	前年度検査結果
95	血液検査
96	理学的所見
97	治療中の疾患
98	喫煙の有無
99	判定

48　現住所(枝枝番)
49　転入前住所
50　転入前方書
51　転入前郵便番号
52　転出予定異動日
53　転出予定届出日
54　転出実定異動日
55　転出実定届出日
56　世帯主氏名優先区分
57　外国人氏名優先区分
58　削除フラグ
59　更新日時

<PublicMedicalHub(PMH)を活用した情報連携に係る自治体検診事務における追加の記録項目>

(1)対象者情報
・変更区分
・個人番号(マイナンバー)
・消除の異動日
・自治体別本人キー
・検診対象者番号
・氏名
・氏名カナ
・住所
・生年月日
・性別
・不開示フラグ
・検診管理番号(複数)
・受診年度(複数)
・検診実施日(複数)

(2)ユーザー情報
・自治体ユーザーID
・メールアドレス
・ユーザー_姓
・ユーザー_名
・ユーザー区分
・地方公共団体コード
・マイナンバー閲覧可能フラグ
・トークン
・削除フラグ
・登録日
・登録者
・更新日

(3)問診票情報
・更新者
・個人番号(マイナンバー)
・氏名
・氏名カナ
・住所
・生年月日
・性別
・自治体検診管理ID
・削除フラグ
・検診対象者番号
・検診管理番号
・実施年度
・検診実施日
・検診担当者_1
・検診担当者_2
・検診担当者_3
・検診担当者_4
・検診担当者_5
・検診担当者_6
・検診担当者_7
・検診担当者_8
・検診担当者_9
・請求額
・医療機関コード
・会場コード
・全国共通自治体検診項目マスタID(複数)
・自治体別自治体検診項目ID(複数)
・自治体検診結果情報(複数)
・自治体別問診票項目マスタID(複数)
・自治体別問診票項目マスタID(複数)
・問診票回答_内容(複数)

(4)検診結果情報
・個人番号(マイナンバー)
・氏名
・氏名カナ
・住所
・生年月日
・性別
・自治体検診管理ID
・削除フラグ
・検診対象者番号
・検診管理番号
・実施年度・検診実施日
・検診担当者_1
・検診担当者_2
・検診担当者_3
・検診担当者_4
・検診担当者_5
・検診担当者_6
・検診担当者_7
・検診担当者_8
・検診担当者_9
・請求額
・医療機関コード
・会場コード
・全国共通自治体検診項目マスタID(複数)
・自治体別自治体検診項目ID(複数)
・自治体検診結果情報(複数)
・自治体別問診票項目マスタID(複数)
・問診票回答_内容(複数)
・問診票回答_コメント(複数)

・問診票回答_コメント（複数）

Ⅲ　リスク対策　※(7. ②を除く。)

1. 特定個人情報ファイル名	
健康増進事業情報管理ファイル	
2. 特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク:　目的外の入手が行われるリスク	
リスクに対する措置の内容	【窓口等での届出による入手における措置】 ・情報の入手の際には、届出窓口において、本人確認書類（身分証明書）の提示を求めるなどにより、厳格に本人確認を行う。 ・届出内容等については、複数の職員が確認し、対象者以外の情報の入手を防止する。 【システムにおける措置】 ・職員に配置される端末はユーザIDによる識別とパスワードによる認証を用いて起動するものとしている。 ・健康情報管理システムを利用する必要がある職員を特定し、ユーザIDによる識別及び生体認証を用いての利用とすることで端末が不正に利用されることを防いでいる。 ・システム上での庁内連携により特定個人情報を入手する場合、いつ、誰が、何のために（どの業務のために）入手したかの操作履歴（ログ）をシステム上で保存している。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hub（PMH）へは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMH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。 ・Public Medical Hub（PMH）のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。
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	
・対象者から情報を入手する際は所定の様式を用いることで健康診査等の実施に関する事務に必要な情報以外を入手することを防止する。 ・庁内連携による住民情報等の入手にあたっては、データ連携項目を必要最小限に留め、不要な項目の取得を行わない設計にすることで不要項目取得のリスクを回避している。	
3. 特定個人情報の使用	
リスク1:　目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク	
リスクに対する措置の内容	・健康情報管理システムには、当該事務に関係のない情報を保有しない。 ・健康情報管理システムの機能以外からは、個人番号にアクセスできないようにアクセス制御を行っている。 ・特定個人情報ファイルには、適切な権限がある担当者のみがアクセスできるよう設計されている。また、適切な権限がある担当者からのアクセスであっても個人番号を表示する必要がない業務（機能）からのアクセスについては、個人番号を画面表示しない設計としている。 ・特定個人情報を使用できる事務については、業務マニュアルに記載し、定期的に職員研修を実施している。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置＞ ・Public Medical Hub（PMH）にアクセスする本市区町村の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・Public Medical Hub（PMH）では、権限のある者しか個人番号にはアクセスできないように制御している。 ・検診施設アプリや住民からマイナポータルAPI経由でPublic Medical Hub（PMH）に接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。
リスクへの対策は十分か	[　　十分である　　]　＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2:　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[　行っている　]　＜選択肢＞ 1）行っている　2）行っていない

	具体的な管理方法	・健康情報管理システムを利用する必要がある職員を特定し、ユーザIDによる識別と生体認証による認証を実施している。 ・アクセス権限の発効・失効の管理 識別情報（ユーザID/パスワード）の発行・更新・廃棄は、人事異動や退職時など、あらかじめ定められたルールに基づいて随時行っている。 健康情報管理システムにアクセスする職員へのアクセス権限は定期的に見直しを行い、指定した職員のみがアクセスできるようにしている。 ・アクセス権限の管理 アクセス可能なユーザIDは必要最小限とし、漏えい等が発生しないように厳重に管理している。 ユーザIDについては、定期的にチェックを行い、不要なIDが使用不可になっているかを確認している。また、利用期間が明確になったものについては、ユーザIDに有効期限を設定し、期限到来により自動的に失効するようにしている。 ・特定個人情報の使用の記録 ユーザIDとともに、健康情報管理システムへのアクセス、操作（登録、更新、印刷、外部媒体への出力等）のアクセス記録をログとして保管している。 上記アクセス記録について、確認が必要となった場合には即座に確認できる仕組みを準備している。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市区町村は、Public Medical Hub（PMH）のアクセス権限を管理する管理者を定める。 ・Public Medical Hub（PMH）のログインはユーザID・パスワードで行う。 ・Public Medical Hub（PMH）へのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・Public Medical Hub（PMH）における特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム（各業務システム）からPublic Medical Hub（PMH）への連携は、アクセス権限を持つ者のみ実施が可能となっている。
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
【従業者が事務外で使用するリスクに対する措置】 ・外部媒体へのデータのコピーや印刷を制御することで、許可なく持ち出せないようにしている。 ・各種ログを取得しているため、業務外利用をした場合には特定可能であることを職員に周知し、事務外の利用を抑止している。 【特定個人情報ファイルが不正に複製されるリスクに対する措置】 ・特定個人情報ファイルの外部媒体への出力は、特定のアクセス権限を持ったユーザのみが、特定の端末及び特定の記録媒体への書き出しのみに限定している。 ・職員（非常勤、臨時職員含む）が特定個人情報を取り扱う作業を行う場合は、インターネットへの接続、電子メールの使用、外部記録媒体への出力が不可能な端末によって行っている。

4. 特定個人情報ファイルの取扱いの委託	[　　] 委託しない
リスク: 委託先における不正な使用等のリスク	
委託契約書中の特定個人情報ファイルの取扱いに関する規定	[　　定めている　　] ＜選択肢＞ 1）定めている　2）定めていない
規定の内容	・情報システムの運用、保守等を外部委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結している。 ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守 ・委託先の責任者、委託内容、作業者、作業場所の特定 ・提供されるサービスレベルの保証 ・従業員に対する教育の実施 ・提供された情報の目的外利用及び受託者以外の者への提供の禁止 ・業務上知り得た情報の守秘義務 ・再委託に関する制限事項の遵守 ・委託業務終了時の情報資産の返還、廃棄等 ・委託業務の定期報告及び緊急時報告義務 ・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等) ・市による監査、検査 <Public Medical Hub(PMH)を活用した情報連携に係る自治体検診事務における追加措置> 特定個人情報の適正な取扱いに関するガイドライン(行政機関等編)を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項
再委託先による特定個人情報ファイルの適切な取扱いの担保	[　　十分に行っている　　] ＜選択肢＞ 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない　4）再委託していない
具体的な方法	委託者の承諾を得た場合に再委託を可能としている。その場合は、再委託先は特定個人情報ファイルの取扱い等について、委託先と同様の措置を行うことを義務付けている。 <Public Medical Hub(PMH)を活用した情報連携に係る自治体検診事務における追加措置> ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるデジタル庁が、再委託先における特定個人情報ファイルの管理状況の定期的な点検(年1回程度又は随時)を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、必要があると認めるときはデジタル庁に報告を求めることができる。
その他の措置の内容	<Public Medical Hub(PMH)を活用した情報連携に係る自治体検診事務における追加措置> ・委託契約書に以下の規定を設ける。 委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。
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	
【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に対する措置】 ・委託先から他社への提供は認めていない。 ・情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明している。 ・必要に応じて吹田市は現地調査・確認を行えることとしている。 【委託先による特定個人情報の保管・消去、委託契約終了後の不正な使用等に関するリスクに対する措置】 ・委託先から任意の様式により消去結果に係る報告書を提出させる。 ・必要に応じて吹田市は現地調査・確認を行えることとしている。	

5. 特定個人情報の提供・移転（委託や情報提供ネットワークシステムを通じた提供を除く。）		[　　]提供・移転しない
リスク: 不正な提供・移転が行われるリスク		
特定個人情報の提供・移転に関するルール	[　　定めている　　]	<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	番号法第19条第8号、同法第22条、別表第二の102の2の項、番号法別表第二の主務省令で定める事務及び情報を定める命令第50条に基づき、提供を行う。	
その他の措置の内容	-	
リスクへの対策は十分か	[　　十分である　　]	<選択肢> 1）特に力を入れている　　2）十分である 3）課題が残されている

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
特定個人情報の提供は、国の定める必須事項のみとし、最小限としている。

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	【健康情報管理システムのソフトウェアにおける措置】 ・中間サーバへの情報照会処理については、業務システム側で操作ログを記録しており、処理実施者、操作内容を把握可能である。中間サーバコネクタと業務システム間のデータ連携処理についても、業務システム側で処理結果ログを記録しており、データ送受信日時、内容等を把握可能である。 【健康情報管理システムの運用における措置】 ・権限を持った職員が所属長の承認を得たうえで情報照会・入手を行う。 ・健康情報管理システムで記録している操作ログは、適宜、健康情報管理システムからリストの出力を行い、目的外の入手が行われていないことの確認を行う。 ・定められたルールに基づく入手を職員に周知、徹底を行う。 【中間サーバー・ソフトウェアにおける措置】 ・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。 ・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: 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	【健康情報管理システムのソフトウェアにおける措置】 ・中間サーバへの情報提供処理については、業務システム側で自動送信を行い、かつ、手動送信においても操作ログを記録しており、処理実施者、操作内容を把握可能である。 中間サーバコネクタと業務システム間のデータ連携処理についても、業務システム側で処理結果ログを記録しており、データ送受信日時、内容等を把握可能である。 【健康情報管理システムの運用における措置】 ・健康情報管理システムで記録している操作ログは、適宜、健康情報管理システムからリストの出力を行い、目的外の提供が行われていないことの確認を行う。 【中間サーバ・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

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・ソフトウェアにおける措置】 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・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・プラットフォームにおける措置】 ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・中間サーバと団体についてはVPN等の技術を利用し、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・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・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・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。

7. 特定個人情報の保管・消去

リスク: 特定個人情報の漏えい・滅失・毀損リスク			
①事故発生時手順の策定・周知		[十分に行っている]	<選択肢> 1）特に力を入れて行っている　2）十分に行っている 3）十分に行っていない
②過去3年以内に、評価実施機関において、個人情報に関する重大事故が発生したか		[発生あり]	<選択肢> 1）発生あり　2）発生なし
	その内容	令和6年（2024年）12月、放課後児童クラブの職員が、クラブ在籍児童2名の要配慮個人情報が含まれる資料を自宅に持ち帰り、後日、出勤途上に当該資料を紛失した。資料はその数時間後に紛失したと推測される駐輪場で発見されたが、個人情報漏えいのおそれは残る。 同日中に当該職員への聞き取り調査を実施し、翌日には対象児童の保護者に謝罪及び状況説明を行った。 二次被害等の報告や相談は受けていない。	
	再発防止策の内容	本件発生前に作成していた個人情報取扱いマニュアルにおいて、個人情報を記載した文書は原則持ち出さないことを規定しており、当該職員も持ち出し禁止の認識は持っていたが、業務多忙を理由に持ち帰ってしまった。本事案を受け、放課後児童クラブの全職員に対して、個人情報が漏えいすれば、本人及びその保護者に多大な損害を与え、引いては本市職員の信頼を失うことにつながるなど、個人情報を取り扱うことの重大性を再認識させるとともに、改めてルールの遵守を厳命した。 また、年4回開催している全クラブ職員が集まる場において、毎回、個人情報取扱いの研修を実施することとした。	

その他の措置の内容	・物理的対策 ＜吹田市における措置＞ ・サーバ室と、データ、プログラム等を含んだ記録媒体及び帳票等の可搬媒体を保管する保管室は、他の部屋とは区別して専用の部屋とする。 ・サーバー室と保管室の出入口には機械による入退室を管理する設備を設置し、認証に必要なカードについては貸出簿を作成して管理する。 ・サーバー室と保管室の入退室管理を徹底するため出入口の場所を限定する。 ・事務室内の端末は、ワイヤロックで施錠する。 ・特定個人情報を扱う窓口職員は、特定個人情報を記した書類は机上に放置せず、紛失漏えい不能な保管を行う。 ・特定個人情報を取り扱う職員が離席する際には、ログオフを義務づけ、一定時間操作が行われない場合はスクリーンセーバーの自動起動設定により、端末画面上の個人情報を保護する。 ・特定個人情報を保管した媒体の運用ルールを定め、遵守している。 ・ガバメントクラウド移行後は、クラウド事業者において国が認可しているAWSにサーバーが設置され、クラウド事業者のデータセンター（IDC）を経由して運用する。クラウド事業者のデータセンター（IDC）は、セキュリティレベルや生態認証等が設けられておりセキュリティが担保されている。 ＜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・プラットフォームをデータセンターに構築し、設置場所への入退室者管理、有人監視及び施錠管理をすることとしている。また、設置場所はデータセンター内の専用の領域とし、他テナントとの混在によるリスクを回避する。 ＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 ・技術的対策 ＜吹田市における措置＞ ・ウィルス対策ソフトを導入し、定期的にパターンファイルの更新を行っている。 ・団体内統合宛名システムは個別のセグメントに配置し、当該セグメントへの通信はファイアウォールにより制御している。 ・使用されていないネットワークスイッチのポートを閉鎖している。 ・ガバメントクラウド移行後は、クラウド事業者において国が認可しているAWSにサーバーが設置され、クラウド事業者のデータセンター（IDC）を経由して運用する。クラウド事業者のデータセンター（IDC）は、セキュリティレベルや生態認証等が設けられておりセキュリティが担保されている。 ＜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・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。

	<Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置> 〇物理的対策 Public Medical Hub（PMH）は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。 〇技術的対策 Public Medical Hub（PMH）は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・論理的に区分された本市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国（デジタル庁）や検診施設等及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・本市区町村の端末とPublic Medical Hub（PMH）との通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ・本市区町村の端末とPublic Medical Hub（PMH）との通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。
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
・届出書類等については、特定個人情報の漏洩及び紛失を防止するため、入力及び照合した後は、鍵付の書庫に保管する。 ・個々の端末はデータファイルが保存されないようシステム制御している。 ・保管期間が経過した特定個人情報を記録した媒体は、復元不可能な状態で確実に消去・廃棄している。 <ガバメントクラウドにおける措置> ・データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 <標準準拠システムにおける措置> ・標準準拠システムへの移行においては、本市ネットワークを経由して、AWSに直接データを移動させる。 ・外部に持ち出すことなくセキュアな通信のみで移動させ、紛失や漏洩がないように移行、保管する。 ・移行データファイルは、稼働後に完全に削除する。

8. 監査	
実施の有無	[○] 自己点検　　[○] 内部監査　　[　　] 外部監査

9. 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	＜吹田市における措置＞ ・毎年、職員に対し、個人情報保護に関する研修を実施している。（eラーニングを含む） ・毎年、所属内のシステム担当者に対し、教育を実施している。 ・集合教育は必要に応じて実施している。 ・委託事業者に対しては、秘密保持契約を締結し、その中で個人情報保護に関する周知徹底を義務付けている。 ・評価書記載事項と運用実態のチェックを行っている。 ・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 ・個人情報保護に関する技術的安全管理措置 ＜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、定期的な研修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。 ・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。

10. 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リテラシー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。

Ⅳ　開示請求、問合せ

1. 特定個人情報の開示・訂正・利用停止請求	
①請求先	吹田市役所　市民部　市民総務室 住所：〒564-8550　大阪府吹田市泉町１丁目３番４０号 電話番号：06-6384-1456
②請求方法	指定様式による書面の提出により開示、訂正、利用停止請求を受け付ける。
③法令による特別の手続	―
④個人情報ファイル簿への不記載等	―
2. 特定個人情報ファイルの取扱いに関する問合せ	
①連絡先	吹田市　健康医療部　成人保健課 住所：〒564-0072　大阪府吹田市出口町１９番２号（吹田市立保健センター５階） 電話番号：06-6339-1212
②対応方法	問い合わせの受付時に受付票等を記載することにより、対応について記録を残す。

Ⅴ　評価実施手続

1. 基礎項目評価	
①実施日	令和7年10月24日
②しきい値判断結果	[　　基礎項目評価及び重点項目評価の実施が義務付けられる　　] ＜選択肢＞ 1）基礎項目評価及び重点項目評価の実施が義務付けられる 2）基礎項目評価の実施が義務付けられる（任意に重点項目評価を実施） 3）特定個人情報保護評価の実施が義務付けられない（任意に重点項目評価を実施）
2. 国民・住民等からの意見の聴取 【任意】	
①方法	―
②実施日・期間	―
③主な意見の内容	―
3. 第三者点検 【任意】	
①実施日	―
②方法	―
③結果	―

（別添2）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
平成28年11月18日	【Ⅰ基本情報】 6．評価実施機関における担当部署	①部署　　福祉保健部保健センター ②所属長　安井　修	①部署　　健康医療部保健センター ②所属長　北川　幸子	事後	
平成28年11月18日	【Ⅱ特定個人情報ファイルの概要】 2．基本情報	⑥事務担当部署　福祉保健部保健センター	⑥事務担当部署　健康医療部保健センター	事後	
平成28年11月18日	【Ⅱ特定個人情報ファイルの概要】 3．特定個人情報の入手・使用	④使用の主体 使用部署　福祉保健部保健センター	④使用の主体 使用部署　健康医療部保健センター	事後	
平成28年11月18日	【Ⅳ開示請求、問合せ】 1．特定個人情報の開示・訂正・利用停止請求	請求先　吹田市市民生活部市民相談室情報公開課 住所：〒564-8550　大阪府吹田市泉町1丁目3番40号 電話番号：06－6384－1456	吹田市役所　健康医療部　保健センター 住所：〒564-0072　大阪府吹田市出口町19番2号（吹田市立総合福祉会館3階） 電話番号：06-6339-1212	事後	
平成28年11月18日	【Ⅴ評価実施手続】 1．基礎項目評価	①実施日　平成27年9月15日	①実施日　平成28年8月1日	事後	
平成29年9月6日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託	③委託先名　インフォメーションテクノロジーサービス株式会社	③委託先名　日本コムシンク株式会社	事後	
平成29年9月6日	【Ⅴ評価実施手続】 1．基礎項目評価	①実施日　平成28年8月1日	①実施日　平成29年8月1日	事後	
平成30年8月22日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託	委託事項1　健康情報管理システム（成人保健）入力データ作成業務	委託事項1　情報管理システム入力データ作成業務	事後	
令和2年1月31日	【Ⅰ基本情報】 2．特定個人情報ファイルを取り扱う事務において使用するシステム	システム1 ②システムの機能　（中略） 【接種情報の統計に関する機能】 指定した予防接種の期間ごとの接種件数、接種年齢、接種医療機関等の情報を表示及び帳票を出力する。	システム1 ②システムの機能　（中略） 【接種情報の統計に関する機能】 指定した予防接種の期間ごとの接種件数、接種年齢、接種医療機関等の情報を表示及び帳票を出力する。	事後	
令和2年1月31日	【Ⅰ基本情報】 2．特定個人情報ファイルを取り扱う事務において使用するシステム	システム1 ③他のシステムとの接続 [　]その他（　　）	システム1 ③他のシステムとの接続 [○]その他（中間サーバコネクタ）	事後	

令和2年1月31日	【Ⅰ基本情報】 6．評価実施機関における担当部署	②所属長　北川　幸子	②所属長　保健センター所長	事後	
令和2年1月31日	【Ⅱ特定個人情報ファイルの概要】 ④記録される項目	50項目以上100項目未満	100項目以上	事後	
令和2年1月31日	【Ⅱ特定個人情報ファイルの概要】 ④記録される項目　主な記録項目	[　] 個人番号対応符号	[○] 個人番号対応符号	事後	
令和2年1月31日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託　委託事項1	③委託先名　日本コムシンク株式会社	③委託先名　株式会社アイ・オー・プロセス	事後	
令和2年1月31日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託　委託事項2	③委託先名　株式会社I・C・S	③委託先名　株式会社両備システムズ	事後	
令和2年1月31日	【Ⅲリスク対策】 8．監査	[○]自己点検 [　]内部監査	[○]自己点検 [○]内部監査	事後	
令和2年1月31日	【Ⅴ評価実施手続】 1．基礎項目評価	①実施日　平成30年8月1日	①実施日　令和2年1月31日	事後	
令和4年2月28日	【Ⅰ基本情報】 1．特定個人情報ファイルを取り扱う事務		以下の項目を追加 ⑤番号法別表第二に基づき、情報提供に必要な個人情報の提供 ⑥情報提供ネットワークシステムを通じた各関係機関等との情報連携 ⑦成人保健事務の実施に必要な情報の取得	事前	
令和4年2月28日	【Ⅰ基本情報】 2．特定個人情報ファイルを取り扱う事務において使用するシステム　システム1②システムの機能		以下の項目を追加 6．情報照会機能　：中間サーバコネクタを通じ、特定個人情報（連携対象）の照会及び提供、受領（照会した情報の受領）する機能	事前	
令和4年2月28日	【Ⅰ基本情報】 2．特定個人情報ファイルを取り扱う事務において使用するシステム　システム1③他のシステムとの接続	[　　]その他（　　）	[　○　]その他（中間サーバコネクタ）	事前	

令和4年2月28日	【Ⅰ基本情報】 2. 特定個人情報ファイルを取り扱う事務において使用するシステム　システム2①システムの名称		中間サーバ	事前	
令和4年2月28日	【Ⅰ基本情報】 2. 特定個人情報ファイルを取り扱う事務において使用するシステム　システム2②システムの機能		【符号管理機能】 　・符号管理機能は、情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で 　個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する。 【情報照会機能】 　・情報照会機能は、情報提供ネットワークシステムを介して、特定個人情報（連携対象）の情報照会 及び情報提供受領（照会した情報の受領）を行う。 【情報提供機能】 ・情報提供機能は、情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報（連携対象）の提供を行う。 【既存システム接続機能】 　・中間サーバーと既存システム、宛名システム及び住民記録システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携する。	事前	
令和4年2月28日	【Ⅰ基本情報】 2. 特定個人情報ファイルを取り扱う事務において使用するシステム　システム2③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[○]宛名システム等	事前	
令和4年2月28日	【Ⅰ基本情報】 5. 情報提供ネットワークシステムによる情報連携※　①実施の有無	実施しない	実施する	事前	

令和4年2月28日	【Ⅰ基本情報】 6．評価実施機関における担当部署	②所長	②センター長	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 2．基本情報　④記録される項目　その妥当性		以下の項目を追加 【個人番号対応符号】 中間サーバコネクタを通じ、特定個人情報（連携対象）の照会及び提供、受領（照会した情報の受領）する機能	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 3．特定個人情報の入手・使用 ②入手方法	[　　]情報提供ネットワークシステム	[　○　]情報提供ネットワークシステム	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5．特定個人情報の提供・移転（委託に伴うものを除く。）　提供・移転の有無	[　　]行っていない	[　○　　]提供を行っている（　1　）件	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5．特定個人情報の提供・移転（委託に伴うものを除く。）　①法令上の根拠		番号法第19条第8号、第22条、別表第二102の2の項、番号法別表第二の主務省令で定める事務及び情報を定める命令第50条	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5．特定個人情報の提供・移転（委託に伴うものを除く。）　②提供先における用途		健康増進法による健康増進事業の実施に関する事務であって主務省令で定めるもの	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5．特定個人情報の提供・移転（委託に伴うものを除く。）　③提供する情報		健康増進事業の実施に関する情報	事前	

令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5. 特定個人情報の提供・移転（委託に伴うものを除く。） 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]	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5. 特定個人情報の提供・移転（委託に伴うものを除く。） ⑤提供する情報の対象となる範囲		健康増進法第19条の二、第19条の四の対象となる者	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5. 特定個人情報の提供・移転（委託に伴うものを除く。） ⑥提供方法		[○]情報提供ネットワークシステム	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 5. 特定個人情報の提供・移転（委託に伴うものを除く。） ⑦時期・頻度		①の照会の都度、または他市町村への検診記録の照会を行う必要性が生じた都度	事前	
令和4年2月28日	【Ⅱ特定個人情報ファイルの概要】 6. 特定個人情報の保管・消去 保管場所 ※		以下の項目を追加 【吹田市における措置】 ・入退室管理区域内に設置するサーバー内に保管する。管理区域については、入室権限を持つ者を限定し、入退室管理カードにより権限の有無の確認し、入退室者名と時刻を記録するなど入退室管理を行っている。 ・届出書等も保管年限内は、鍵付の文書保管倉庫内での保管を義務付けている。 ・文書保管倉庫の最終退出者は、退出時に施錠を行っており、外部の者が入室できないようにしている。 【中間サーバ・プラットフォームにおける措置】 ・中間サーバ・プラットフォームはデータセンターに設置しており、データセンターへの入館及びサーバ室への入室を厳重に管理する。 ・特定個人情報は、サーバ室に設置された中間サーバのデータベース内に保存され、バックアップもデータベース上に保存される。	事前	

令和4年2月28日	【Ⅲリスク対策】 2. 特手個人情報の入手(情報提供ネットワークシステムを通じた入手を除く。) 特手個人情報の入手(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		・対象者から情報を入手する際は所定の様式を用いることで健康診査等の実施に関する事務に必要な情報以外を入手することを防止する。 ・庁内連携による住民情報等の入手にあたっては、データ連携項目を必要最小限に留め、不要な項目の取得を行わない設計にすることで不要項目取得のリスクを回避している。	事前	
令和4年2月28日	【Ⅲリスク対策】 5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。) 特定個人情報の提供・移転に関するルール		[定めている]	事前	
令和4年2月28日	【Ⅲリスク対策】 5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。) 特定個人情報の提供・移転に関するルール ルールの内容及びルール遵守の確認方法		番号法第19条第8号、同法第22条、別表第二の102の2の項、番号法別表第二の主務省令で定める事務及び情報を定める命令第50条に基づき、提供を行う。	事前	
令和4年2月28日	【Ⅲリスク対策】 5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。) リスクへの対策は十分か		[十分である]	事前	
令和4年2月28日	【Ⅲリスク対策】 5. 特定個人情報の提供・移転(委託や情報提供ネットワークシステムを通じた提供を除く。) 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		特定個人情報の提供は、国の定める必須事項のみとし、最小限としている。	事前	

令和4年2月28日	【Ⅲリスク対策】 6．情報提供ネットワークシステムとの接続　リスク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		以下の項目を追加 【健康情報管理システムのソフトウェアにおける措置】 ・中間サーバへの情報照会処理については、業務システム側で操作ログを記録しており、処理実施者、操作内容を把握可能である。中間サーバコネクタと業務システム間のデータ連携処理についても、業務システム側で処理結果ログを記録しており、データ送受信日時、内容等を把握可能である。 【健康情報管理システムの運用における措置】 ・権限を持った職員が所属長の承認を得たうえで情報照会・入手を行う。 ・健康情報管理システムで記録している操作ログは、適宜、健康情報管理システムからリストの出力を行い、目的外の入手が行われていないことの確認を行う。 ・定められたルールに基づく入手を職員に周知、徹底を行う。	事前	
	（続き） 【Ⅲリスク対策】 6．情報提供ネットワークシステムとの接続　リスク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】 ・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。 ・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。		

令和4年2月28日	【Ⅲリスク対策】 6. 情報提供ネットワークシステムとの接続　リスク1：目的外の入手が行われるリスク　リスクへの対策は十分か		十分である	事前	
令和4年2月28日	【Ⅲリスク対策】 6. 情報提供ネットワークシステムとの接続　リスク2：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		以下の項目を追加 【健康情報管理システムのソフトウェアにおける措置】 ・中間サーバへの情報提供処理については、業務システム側で自動送信を行い、かつ、手動送信においても操作ログを記録しており、処理実施者、操作内容を把握可能である。中間サーバコネクタと業務システム間のデータ連携処理についても、業務システム側で処理結果ログを記録しており、データ送受信日時、内容等を把握可能である。 【健康情報管理システムの運用における措置】 ・健康情報管理システムで記録している操作ログは、適宜、健康情報管理システムからリストの出力を行い、目的外の提供が行われていないことの確認を行う。	事前	

	（続き） 【Ⅲリスク対策】 6．情報提供ネットワークシステムとの接続　リスク2：不正な提供が行われるリスク　リスクに対する措置の内容		【中間サーバ・ソフトウェアにおける措置】 ・情報提供機能（※）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		

令和4年2月28日	【Ⅲリスク対策】 6．情報提供ネットワークシステムとの接続　リスク2：不正な提供が行われるリスク　リスクへの対策は十分か		十分である	事前	
令和4年2月28日	【Ⅲリスク対策】 6．情報提供ネットワークシステムとの接続　情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置		以下の項目を追加 【中間サーバ・ソフトウェアにおける措置】 ・中間サーバの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ・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・プラットフォームにおける措置】 ・中間サーバと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ・中間サーバと団体についてはVPN等の技術を利用し、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・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・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・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。	事前	
令和4年7月22日	【Ⅰ基本情報】 6．評価実施機関における担当部署①部署	健康医療部　保健センター	健康医療部　成人保健課	事後	
令和4年7月22日	【Ⅰ基本情報】 6．評価実施機関における担当部署②所属長	センター長	課長	事後	

令和4年7月22日	【Ⅱ特定個人情報ファイルの概要】 3．特定個人情報の入手・使用 ④仕様の主体　使用部署	健康医療部　保健センター	健康医療部　成人保健課	事後	
令和4年7月22日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託　委託事項1③委託先名	株式会社アイ・オー・プロセス	株式会社インターフェイス	事後	
令和4年7月22日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託　委託事項2④再委託の有無	再委託する	再委託しない	事後	
令和4年7月22日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託　委託事項2④再委託の許諾方法	再委託の制限事項内で本市が認める場合、委託先からの書面による申請に基づき、許諾		事後	
令和4年7月22日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託　委託事項2④再委託事項	健康情報管理システム再構築業務の一部（主として構築に係る部分）		事後	
令和4年7月22日	【Ⅱ特定個人情報ファイルの概要】 4．特定個人情報ファイルの取扱いの委託　委託事項4②委託先名	株式会社ワンビシアーカイブス大阪支店	日本電気株式会社	事後	
令和4年7月22日	[Ⅳ開示請求・問合せ]2．特定個人情報ファイルの取扱いに関する問合せ　①連絡先	吹田市役所　健康医療部　保健センター 住所：〒564-0072　大阪府吹田市出口町19番2号（吹田市立総合福祉会館3階） 電話番号：06－6339－1212	吹田市　健康医療部　成人保健課 住所：〒564-0072　大阪府吹田市出口町19番2号（吹田市立保健センター3階） 電話番号：06－6339－1212	事後	
令和4年7月22日	[Ⅴ評価実施手続]1．基礎項目評価　①実施日	①実施日　令和4年2月28日	①実施日　令和4年6月30日	事後	
令和6年11月28日	Ⅰ　基本情報 1.特定個人情報ファイルを取り扱う事務　②事務の内容	吹田市では、健康増進法に基づき市民の健康増進のため各種健康診査、健康診査結果を基にした保健指導等を行っている。	吹田市では、健康増進法に基づき市民の健康増進のため各種健康診査、健康診査結果を基にした保健指導等を行っている。	事後	特定個人情報保護評価指針の重要な変更の対象外（番号法関係法令の一部改正及び歯科健康診査の名称変更に係る変更）
令和6年11月28日	Ⅰ　基本情報 4.個人番号の利用※　法令上の根拠	・番号法第9条第1項　別表第一第76項 ・行政手続における特定の個人を識別するための番号の利用等に関する法律別表第一の主務省令で定める事務を定める命令第54条	・番号法第9条第1項　別表111の項 ・番号法別表の主務省令で定める事務を定める命令第54条 ・番号法第19条第6号（委託先への提供）	事後	特定個人情報保護評価指針の重要な変更の対象外（番号法関係法令の一部改正に係る変更）

令和6年11月28日	Ⅰ　基本情報 5.情報提供ネットワークシステムによる情報連携※　②法令上の根拠	照会：番号法第19条8号、別表第二102の2の項、番号法別表第二の主務省令で定める事務及び情報を定める命令第50条 提供：番号法第22条、別表第二102の2の項、番号法別表第二の主務省令で定める事務及び情報を定める命令第50条	【個人情報の照会】 ・番号法第19条第8号に基づく主務省令第2条の表139の項 【個人情報の提供】 ・番号法第19条第8号に基づく主務省令第2条の表139の項	事後	特定個人情報保護評価指針の重要な変更の対象外（番号法関係法令の一部改正に係る変更）
令和6年11月28日	Ⅱ　特定個人情報ファイルの概要 3.特定個人情報の入手・使用 ⑤使用方法	①健康増進法等に基づく各種健康診査（胃・肺・大腸・子宮・乳がん検診、骨粗しょう症検診、B型C型肝 炎ウィルス検診、成人歯科健康診査）の実施 ②健康診査の結果通知、受診勧奨、健康手帳の交付等の事務 ③がん検診受診者で要精検者への受診勧奨及び管理に伴う事務 ④疾病予防その他健康に関する健康教育・相談等、保健指導の実施または受診勧奨に関する事務	①健康増進法等に基づく各種健康診査（胃・肺・大腸・子宮・乳がん検診、骨粗しょう症検診、B型C型肝 炎ウィルス検診、吹田市歯科健康診査）の実施 ②健康診査の結果通知、受診勧奨、健康手帳の交付等の事務 ③がん検診受診者で要精検者への受診勧奨及び管理に伴う事務 ④疾病予防その他健康に関する健康教育・相談等、保健指導の実施または受診勧奨に関する事務	事後	特定個人情報保護評価指針の重要な変更の対象外（歯科健康診査の名称変更に係る変更）
令和6年11月28日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項2　①委託内容	システムの運用・保守業務、法制度改正に伴う改修作業	システム運用・保守業務、法制度改正に伴う改修作業、ガバメントクラウド移行及び標準準拠システム移行業務	事前	特定個人情報保護評価指針の重要な変更（地方公共団体情報システムの標準化に係る変更）
令和6年11月28日	Ⅱ　特定個人情報ファイルの概要 5.特定個人情報の提供・移転（委託に伴うものを除く。）　提供先1　①法令上の根拠	番号法第19条第8号、第22条、別表第二102の2の項、番号法別表第二の主務省令で定める事務及び情報を定める命令第50条	番号法第19条第8号に基づく主務省令第2条の表139の項	事後	特定個人情報保護評価指針の重要な変更の対象外（番号法関係法令の一部改正に係る変更）

令和6年11月28日	Ⅱ　特定個人情報ファイルの概要 6.特定個人情報の保管・消去 保管場所※	【吹田市における措置】 記載省略 【中間サーバ・プラットフォームにおける措置】 記載省略	【吹田市における措置】 記載省略（以下の内容を追記） ・ガバメントクラウド移行後は、クラウド事業者において国が認可しているAWSにサーバーが設置され、クラウド事業者のデータセンター（IDC）を経由して運用する。クラウド事業者のデータセンター（IDC）は、セキュリティレベルや生態認証等が設けられておりセキュリティが担保されている。 【中間サーバ・プラットフォームにおける措置】 記載省略 【ガバメントクラウドにおける措置】 ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。	事前	特定個人情報保護評価指針の重要な変更（地方公共団体情報システムの標準化に係る変更）
令和6年11月28日	Ⅲ　リスク対策 6.情報提供ネットワークシステムとの接続　リスク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	【健康情報管理システムのソフトウェアにおける措置】 記載省略 【健康情報管理システムの運用における措置】 記載省略 【中間サーバー・ソフトウェアにおける措置】 記載省略 （※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。	【健康情報管理システムのソフトウェアにおける措置】 記載省略 【健康情報管理システムの運用における措置】 記載省略 【中間サーバー・ソフトウェアにおける措置】 記載省略 （※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。	事後	特定個人情報保護評価指針の重要な変更の対象外（番号法関係法令の一部改正に係る変更）

令和6年11月28日	Ⅲ　リスク対策 7.特定個人の保管・消去　リスク：特定個人情報の漏えい・滅失・毀損リスク その他の措置の内容 ・物理的対策	＜吹田市における措置＞ 記載省略 ＜中間サーバー・プラットフォームにおける措置＞ 記載省略	＜吹田市における措置＞ 記載省略（以下の内容を追記） ・ガバメントクラウド移行後は、クラウド事業者において国が認可しているAWSにサーバーが設置され、クラウド事業者のデータセンター（IDC）を経由して運用する。クラウド事業者のデータセンター（IDC）は、セキュリティレベルや生態認証等が設けられておりセキュリティが担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ 記載省略 ＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。	事前	特定個人情報保護評価指針の重要な変更（地方公共団体情報システムの標準化に係る変更）
令和6年11月28日	Ⅲ　リスク対策 7.特定個人の保管・消去　リスク：特定個人情報の漏えい・滅失・毀損リスク その他の措置の内容 ・技術的対策	＜吹田市における措置＞ 記載省略 ＜中間サーバー・プラットフォームにおける措置＞ 記載省略	＜吹田市における措置＞ 記載省略（以下の内容を追記） ・ガバメントクラウド移行後は、クラウド事業者において国が認可しているAWSにサーバーが設置され、クラウド事業者のデータセンター（IDC）を経由して運用する。クラウド事業者のデータセンター（IDC）は、セキュリティレベルや生態認証等が設けられておりセキュリティが担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ 記載省略	事前	特定個人情報保護評価指針の重要な変更（地方公共団体情報システムの標準化に係る変更）

	（続き） Ⅲ　リスク対策 7.特定個人の保管・消去　リスク：特定個人情報の漏えい・滅失・毀損リスク その他の措置の内容 ・技術的対策		＜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。		

令和6年11月28日	Ⅲ　リスク対策 7.特定個人の保管・消去　リスク：特定個人情報の漏えい・滅失・毀損リスク 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	・届出書類等については、特定個人情報の漏洩及び紛失を防止するため、入力及び照合した後は、鍵付の書庫に保管する。 ・個々の端末はデータファイルが保存されないようシステム制御している。 ・保管期間が経過した特定個人情報を記録した媒体は、復元不可能な状態で確実に消去・廃棄している。	・届出書類等については、特定個人情報の漏洩及び紛失を防止するため、入力及び照合した後は、鍵付の書庫に保管する。 ・個々の端末はデータファイルが保存されないようシステム制御している。 ・保管期間が経過した特定個人情報を記録した媒体は、復元不可能な状態で確実に消去・廃棄している。 ＜ガバメントクラウドにおける措置＞ ・データの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等に準拠したプロセスにしたがって確実にデータを消去する。 ＜標準準拠システムにおける措置＞ ・標準準拠システムへの移行においては、本市ネットワークを経由して、AWSに直接データを移動させる。 ・外部に持ち出すことなくセキュアな通信のみで移動させ、紛失や漏洩がないように移行、保管する。 ・移行データファイルは、稼働後に完全に削除する。	事前	特定個人情報保護評価指針の重要な変更（地方公共団体情報システムの標準化に係る変更）

令和6年11月28日	Ⅲ　リスク対策 10,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＞ 記載省略	＜中間サーバー･プラットフォームにおける措置＞ 記載省略 ＜ガバメントクラウドにおける措置＞ ･ガバメントクラウドについては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。 ･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。	事前	特定個人情報保護評価指針の重要な変更（地方公共団体情報システムの標準化に係る変更）
令和6年11月28日	Ⅳ　開示請求、問合せ 1.特定個人情報の開示・訂正・利用停止請求 ②請求方法	吹田市個人情報保護条例第１４条に基づき、必要事項を記載した開示請求書を提出する。 （市ホームページ上に、請求先、請求方法等を掲載している。）	指定様式による書面の提出により開示、訂正、利用停止請求を受け付ける。	事後	特定個人情報保護評価指針の重要な変更の対象外（個人情報保護条例廃止に係る修正）
令和6年11月28日	Ⅳ　開示請求、問合せ 2.特定個人情報ファイルの取扱いに関する問合わせ ①連絡先	吹田市　健康医療部　成人保健課 住所：〒564-0072　大阪府吹田市出口町１９番２号（吹田市立保健センター3階） 電話番号：06-6339-1212	吹田市　健康医療部　成人保健課 住所：〒564-0072　大阪府吹田市出口町１９番２号（吹田市立保健センター5階） 電話番号：06-6339-1212	事後	特定個人情報保護評価指針の重要な変更の対象外（執務室の場所変更に係る修正）
令和6年11月28日	Ⅴ　評価実施手続 ①実施日	2022/6/30	2024/10/31	事後	特定個人情報保護評価指針の重要な変更の対象外（時点修正）

令和7年3月21日	Ⅲ　リスク対策 7.特定個人の保管・消去　リスク：特定個人情報の漏えい・滅失・毀損リスク ②過去3年以内に評価実施期間において、個人情報に関する重大事故が発生したか	発生なし	発生あり	事後	特定個人情報保護評価指針による重要な変更箇所に当たらないため
令和7年3月21日	Ⅲ　リスク対策 7.特定個人の保管・消去　リスク：特定個人情報の漏えい・滅失・毀損リスク ②その内容		令和6年（2024年）12月、放課後児童クラブの職員が、クラブ在籍児童2名の要配慮個人情報が含まれる資料を自宅に持ち帰り、後日、出勤途上に当該資料を紛失した。資料はその数時間後に紛失したと推測される駐輪場で発見されたが、個人情報漏えいのおそれは残る。 同日中に当該職員への聞き取り調査を実施し、翌日には対象児童の保護者に謝罪及び状況説明を行った。二次被害等の報告や相談は受けていない。	事後	特定個人情報保護評価指針による重要な変更箇所に当たらないため
令和7年3月21日	Ⅲ　リスク対策 7.特定個人の保管・消去　リスク：特定個人情報の漏えい・滅失・毀損リスク ②再発防止策の内容		本件発生前に作成していた個人情報取扱いマニュアルにおいて、個人情報を記載した文書は原則持ち出さないことを規定しており、当該職員も持ち出し禁止の認識は持っていたが、業務多忙を理由に持ち帰ってしまった。本事案を受け、放課後児童クラブの全職員に対して、個人情報が漏えいすれば、本人及びその保護者に多大な損害を与え、引いては本市職員の信頼を失うことにつながるなど、個人情報を取り扱うことの重大性を再認識させるとともに、改めてルールの遵守を厳命した。 また、年4回開催している全クラブ職員が集まる場において、毎回、個人情報取扱いの研修を実施することとした。	事後	特定個人情報保護評価指針による重要な変更箇所に当たらないため

令和7年10月24日	Ⅰ　基本情報 1.特定個人情報ファイルを取り扱う事務 ②事務の内容		以下の項目を追加 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務＞ ・情報連携のため、本市区町村は、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む受診者情報、問診情報及び検診結果の紐付け及び登録を行う。 ・住民は、マイナポータル等を介して問診情報の入力、検診結果及び通知の取得/閲覧が可能となる。 ・住民が、検診時に、従来の紙の問診票に代えて、マイナンバーカードをタブレットに搭載された検診施設アプリ又は医療機関のシステムで用いることにより、医療機関・検診会場（以下、検診施設等）において住民が事前に入力した問診情報、検診結果の取得/閲覧/入力が可能となる。 ・自治体は、検診施設等から入力された問診情報、検診結果の取得及び住民への通知が可能となる。		
令和7年10月24日	Ⅰ　基本情報 ２．特定個人情報ファイルを取り扱う事務において使用するシステム ①システムの名称		以下の項目を追加 Public Medical Hub　（PMH）		

令和7年10月24日	Ⅰ　基本情報 ２．特定個人情報ファイルを取り扱う事務において使用するシステム ②システムの機能		以下を追加 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務＞ ①雛形の登録 　問診票項目、通知文言等の雛形をPublic Medical Hub（PMH）へ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 　本市区町村で管理している個人番号、受診者情報、問診情報及び検診結果をPublic Medical Hub（PMH）に登録し、社会保険診療報酬支払基金（以下、「支払基金」という。なお、今後「医療情報基盤・診療報酬審査支払機構」に改名予定）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 　マイナポータルからのPublic Medical Hub（PMH）初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けてPublic Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 　自治体検診の対象者は、マイナポータルへログインしてマイナンバーカードの電子証明書のシリアル番号に紐付くPMH仮名識別子を利用した照会を行う。Public Medical Hub（PMH）は、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く検診結果・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問診票の入力画面から情報を入力することにより、Public Medical Hub（PMH）はPMH仮名識別子からPMHキーを特定し、PMHキーに紐付く問診情報を登録する。		

令和7年10月24日	（続き） Ⅰ　基本情報 ２．特定個人情報ファイルを取り扱う事務において使用するシステム ②システムの機能		④情報連携機能（検診施設アプリ） ・識別子の格納機能 　検診施設アプリはマイナンバーカードの電子証明書のシリアル番号を用いてマイナポータル経由でPublic Medical Hub（PMH）に接続する。検診施設アプリからのPublic Medical Hub（PMH）初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けてPublic Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 　検診施設アプリは、マイナンバーカードの電子証明書のシリアル番号を用いてマイナポータル経由で、Public Medical Hub（PMH）へPMH仮名識別子を利用した照会を行う。Public Medical Hub（PMH）は、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く問診情報を検診施設アプリに提供する。また、検診施設等が検診結果の入力画面から情報を入力することにより、Public Medical Hub（PMH）はPMH仮名識別子からPMHキーを特定し、PMHキーに紐付く検診結果を登録する。		
令和7年10月24日	Ⅰ　基本情報 ２．特定個人情報ファイルを取り扱う事務において使用するシステム ③他のシステムとの接続		以下の内容を追記 ［〇］その他 （健康管理システム、マイナポータル、医療保険者等向け中間サーバー、検診施設アプリ）		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 2.基本情報 ④使用方法 主な記録項目		以下の内容を追記 ［〇］その他 <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> ・自治体検診記録情報		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 2.基本情報 ④使用方法 その妥当性		以下の内容を追記 <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> ・識別情報（その他識別情報） 　PMHキー、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 　検診管理番号…PMH内で検診の種類を区別するために必要となる。 ・業務関係情報（その他） 　検診情報…（自治体検診事務の適切な実施にあたり必要となる情報を管理し、）PMHが、外部と情報連携するために必要となる。		

令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 3.特定個人情報の入手・使用 ①入手元		以下の内容を追記 [〇]民間事業者 （検診施設等、支払基金）		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 3.特定個人情報の入手・使用 ②入手方法		以下の内容を追記 [〇]その他 （医療保険者等向け中間サーバー、検診施設アプリ、マイナポータル）		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 3.特定個人情報の入手・使用 ⑤使用方法		以下の内容を追記 <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> ・情報連携のため、本市区町村は、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む受診者情報、問診情報及び検診結果の紐付け及び登録を行う。 ・登録後、Public Medical Hub（PMH）は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub（PMH）が連動するためのPMH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（PMH）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Public Medical Hub（PMH）で共有されることでPublic Medical Hub（PMH）からマイナポータルへの通知、マイナポータルや検診施設アプリ（マイナポータル経由）からPublic Medical Hub（PMH）の問診情報及び検診結果の取得/閲覧/入力等といった情報連携が可能となる。		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項5		Public Medical Hub（PMH）を活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項5　①委託内容		Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務		

令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項5　②委託先における取扱者数		10人以上50人未満		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項5　③委託先名		国（デジタル庁）		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項5　④再委託の有無		再委託する		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項5　⑤再委託の許諾方法		書面又は電磁的方法による承諾		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 4.特定個人情報の取扱いの委託 委託事項5　⑥再委託事項		PMHキーの付与、情報連携業務及び運用保守業務		

令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 ６．特定個人情報の保管・消去 保管場所		以下の内容を追記 <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> Public Medical Hub（PMH）は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。なお、以下のとおりセキュリティ対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・論理的に区分された本市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国（デジタル庁）や検診施設等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。		
令和7年10月24日	Ⅱ　特定個人情報ファイルの概要 ７．備考		以下の内容を追記 <Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務> ・本市区町村の領域に保管されたデータのみ、Public Medical Hub（PMH）を用いて消去することができる。 ・本市区町村の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、古いものから順に自動削除される。		

令和7年10月24日	Ⅲ　リスク対策 ２．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。） リスクに対する措置の内容		以下の内容を追記 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置＞ ・医療保険者等向け中間サーバーからPublic Medical Hub（PMH）へは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMH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。 ・Public Medical Hub（PMH）のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。		
令和7年10月24日	Ⅲ　リスク対策 ３．特定個人情報の使用 リスク1：　目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク リスクに対する措置の内容		以下の内容を追記 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置＞ ・Public Medical Hub（PMH）にアクセスする本市区町村の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・Public Medical Hub（PMH）では、権限のある者しか個人番号にはアクセスできないように制御している。 ・検診施設アプリや住民からマイナポータルAPI経由でPublic Medical Hub（PMH）に接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。		
令和7年10月24日	Ⅲ　リスク対策 ３．特定個人情報の使用 リスク2：　権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク 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 具体的な管理方法		以下の内容を追記 ＜Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市区町村は、Public Medical Hub（PMH）のアクセス権限を管理する管理者を定める。 ・Public Medical Hub（PMH）のログインはユーザID・パスワードで行う。 ・Public Medical Hub（PMH）へのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・Public Medical Hub（PMH）における特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム（各業務システム）からPublic Medical Hub（PMH）への連携は、アクセス権限を持つ者のみ実施が可能となっている。		

令和7年10月24日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 委託契約書中の特定個人情報ファイルの取扱いに関する規定 規定の内容		以下の内容を追記 <Public Medical Hub(PMH)を活用した情報連携に係る自治体検診事務における追加措置> 特定個人情報の適正な取扱いに関するガイドライン(行政機関等編)を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項		
令和7年10月24日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 再委託先による特定個人情報ファイルの適切な取扱いの担保 具体的な管理方法		以下の内容を追記 <Public Medical Hub(PMH)を活用した情報連携に係る自治体検診事務における追加措置> <Public Medical Hub(PMH)を活用した情報連携に係る自治体検診事務における追加措置> ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるデジタル庁が、再委託先における特定個人情報ファイルの管理状況の定期的な点検(年1回程度又は随時)を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、必要があると認めるときはデジタル庁に報告を求めることができる。		
令和7年10月24日	Ⅲ リスク対策 4. 特定個人情報ファイルの取扱いの委託 その他の措置の内容		以下の内容を追記 <Public Medical Hub(PMH)を活用した情報連携に係る自治体検診事務における追加措置> ・委託契約書に以下の規定を設ける。 委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。		

令和7年10月24日	Ⅲ　リスク対策 7.特定個人情報の保管・消去 その他の措置の内容 （〇物理的対策）		<Public Medical Hub（PMH）を活用した情報連携に係る自治体検診事務における追加措置> 〇物理的対策 Public Medical Hub（PMH）は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスを利用している。		
令和7年10月24日	（続き） Ⅲ　リスク対策 7.特定個人情報の保管・消去 その他の措置の内容 （〇技術的対策）		〇技術的対策 Public Medical Hub（PMH）は、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015またはCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。		

令和7年10月24日	（続き） Ⅲ　リスク対策 7.特定個人情報の保管・消去 その他の措置の内容 （〇技術的対策）		主に以下の技術的対策を講じている。 ・論理的に区分された本市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国（デジタル庁）や検診施設等及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、外部からの侵入検知・通知機能を備えている。 ・本市区町村の端末とPublic Medical Hub（PMH）との通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ・本市区町村の端末とPublic Medical Hub（PMH）との通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。		
令和7年10月24日	Ⅴ　評価実施手続 ①実施日	令和6年10月31日	令和7年9月30日		