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
59	健康増進事業の実施に関する事務　全項目評価書（システム標準化移行後）

個人のプライバシー等の権利利益の保護の宣言

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

特記事項	

評価実施機関名

神奈川県川崎市長

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1月20日

［令和6年10月　様式4］

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	健康増進事業の実施に関する事務
②事務の内容　※	健康増進事業は、健康増進法第17条第1項及び第19条の2に基づき、住民の健康の増進を図るため、生活習慣相談等の実施を行うものである。 そのうち、健康増進法第19条の2に基づき実施する健康増進事業として、次の事業に係る検診等の実施、検診情報の記録管理、統計業務等を行う。 健康増進法第19条の2に基づく健康増進事業（健康診査等） （1）歯周疾患検診 （2）骨粗鬆症検診 （3）肝炎ウイルス検診（※） （4）健康増進法施行規則第4条の2第4号に定める健康診査 （5）健康増進法施行規則第4条の2第5号に定める保健指導 （6）がん検診 ※本市では、同法に基づく肝炎ウイルス検診は未実施。 また、番号法第9条第1項　別表の111の項（健康増進法（平成十四年法律第百三号）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）の規定により、個人番号を用いることになる。
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

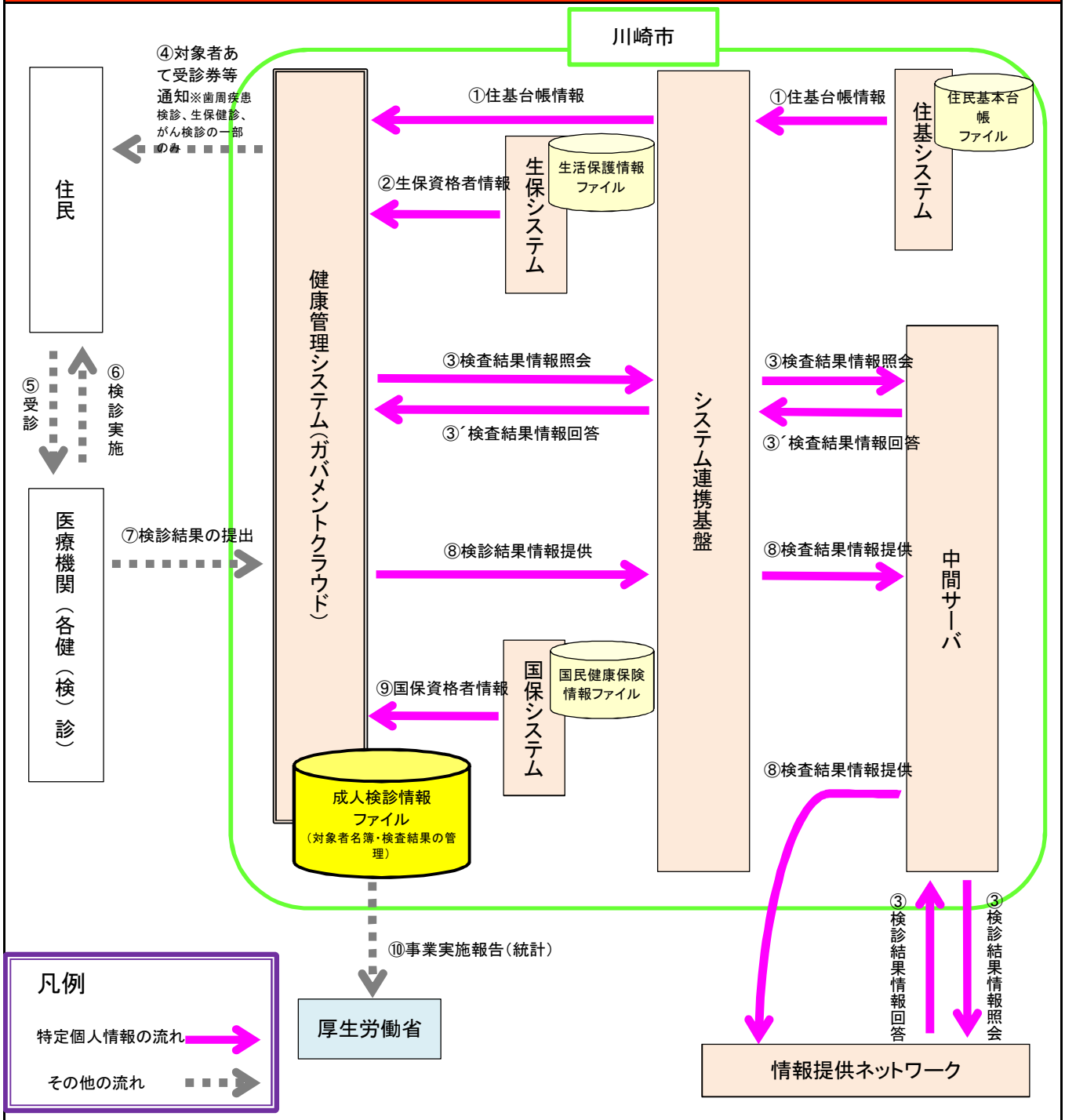
2. 特定個人情報ファイルを取り扱う事務において使用するシステム	
システム1	
①システムの名称	健康管理システム
②システムの機能	1　健診準備機能 健診（検診）ごとの対象者宛名・一覧表の作成及び受診申込み、受診券発行等を行う機能。 2　健診（検診）管理機能 歯周疾患検診、骨粗鬆症検診、健康診査、各がん検診の結果及び要精密検査となった者の結果の管理を行う機能。 3　統計抽出機能 各種統計資料の作成を行うもの。
③他のシステムとの接続	[　]情報提供ネットワークシステム　[○]庁内連携システム [　]住民基本台帳ネットワークシステム　[○]既存住民基本台帳システム [　]宛名システム等　[　]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	システム連携基盤
②システムの機能	1　団体内統合宛名管理機能 既存業務システムから住登者データ、住登外データを受領し、システム連携基盤内の統合宛名DBに団体内統合宛名番号と紐付けて管理を行う。また、個人番号が新規入力されたタイミングで、団体内統合宛名番号の付番を行う。 2　符号要求機能 個人番号を特定済みの団体内統合宛名番号を中間サーバーに登録し、中間サーバーに情報提供用個人識別符号の取得要求・取得依頼を行う。また、中間サーバーから返却された処理通番は住基GWへ送信する。 3　情報提供機能 各業務で管理している番号法第19条第8号に基づく主務省令第2条の表の提供業務情報を受領し、中間サーバーへの情報提供を行う。 4　情報照会機能 中間サーバーへ他団体への情報照会を要求し、返却された照会結果を画面表示または、各業務システムにファイル転送を行う。 5　既存システム連携機能 各業務システム及び中間サーバーと接続し、システム間での情報連携を行う。 6　職員認証・権限管理機能 システム間連携以外で団体内統合宛名管理機能等を利用する職員の認証と職員に付与された権限管理を行い、特定個人情報へのアクセス制御を行う機能。
③他のシステムとの接続	[　]情報提供ネットワークシステム　[　]庁内連携システム [　]住民基本台帳ネットワークシステム　[○]既存住民基本台帳システム [　]宛名システム等　[　]税務システム

	[ ]宛名システム等　　[ ]税務システム [○]その他　（ 中間サーバ　　）

システム3	
①システムの名称	中間サーバー
②システムの機能	中間サーバーは、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）、システム連携基盤等の各システムとデータの受け渡しを行うことで、符号の取得（※1）や各情報保有機関で保有する特定個人情報の照会と提供等の業務を実現する。 （※1）セキュリティの観点より、特定個人情報の照会と提供の際は個人番号を直接利用せず、「符号」を取得して利用する。 1　符号管理機能 情報照会、情報提供に用いる個人の識別子である「符号」と、情報保有機関内で個人を特定するために利用する「団体内統合宛名番号」とを紐付け、その情報を保管・管理する機能。 2　情報照会機能 情報提供ネットワークシステムを介して、特定個人情報(連携対象)の情報照会及び情報提供受領（照会した情報の受領）を行う機能。 3　情報提供機能 情報提供ネットワークシステムを介して、情報照会要求の受領及び当該特定個人情報(連携対象)の提供を行う機能。 4　既存システム接続機能 中間サーバーと各システムとの間で情報照会内容、情報提供内容、特定個人情報（連携対象）、符号取得のための情報等について連携するための機能。 5　情報提供等記録管理機能 特定個人情報(連携対象)の照会、又は提供があった旨の情報提供等記録を生成し、管理する機能。 6　情報提供データベース管理機能 特定個人情報（連携対象）を副本として、保持・管理する機能。 7　データ送受信機能 中間サーバーと情報提供ネットワークシステム（インターフェイスシステム）との間で情報照会、情報提供、符号取得のための情報等について連携するための機能。 8　セキュリティ管理機能 セキュリティを管理する機能。 9　職員認証・権限管理機能 中間サーバーを利用する職員の認証と職員に付与された権限に基づいた各種機能や特定個人情報(連携対象)へのアクセス制御を行う機能。 10　システム管理機能 バッチの状況管理、業務統計情報の集計、稼動状態の通知、保管期限切れ情報の削除を行う機能。
③他のシステムとの接続	[○] 情報提供ネットワークシステム　　[○] 庁内連携システム [　] 住民基本台帳ネットワークシステム　　[　] 既存住民基本台帳システム [○] 宛名システム等　　[　] 税務システム [　] その他　（　　）
システム4	
システム5	
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	
成人検診情報ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	・検診対象者に向けた受診券やクーポン券等の個別通知の発行や検診受診者の結果情報の管理のため ・がん検診、歯周疾患検診、骨粗しょう症検診、生活保護受給者等健康診査の実施に伴う情報管理のため
②実現が期待されるメリット	・対象者を確認し、対象者と個人番号を紐づけることで、行政を効率化して人員や財源を国民サービスに振り向けられることができる。 ・健(検)診の対象者であることを確認し、対象者と受診結果を紐づけることで、経年的な記録の管理・保管等について効率的な事務が可能となる。 ・対象者の健(検)診記録を管理することで、未健診者を迅速に把握でき、また、効率的・効果的な分析・指導を行うことによって健(検)診の適切な精度管理を図ることができる。 ・番号制度の導入により、情報提供ネットワークを通じて他市町村で受診した健(検)診結果を照会することが可能となり、健(検)診記録の完全な管理が可能となる。
5. 個人番号の利用 ※	
法令上の根拠	・番号法第9条第1項 別表の111の項 ・川崎市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条例第3条
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139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139の項
7. 評価実施機関における担当部署	
①部署	健康福祉局保健医療政策部健康増進担当
②所属長の役職名	健康福祉局保健医療政策部健康増進担当課長
8. 他の評価実施機関	
―	

（別添1）事務の内容



（備考）

Ⅰ　健康増進事業の実施に関する事務
① 既存の住基システムから、住民登録のある者の宛名情報を管理する。（システム連携基盤経由連携）
② 既存の生保システムから、生活保護の資格者情報を管理する。（媒体連携）
③ 情報提供ネットワークシステムから、転入者等の検診結果に関する情報を入手し管理する。
④ 住基台帳情報・生活保護資格者情報等から検診対象者の台帳を作成し、対象者宛てに受診券等を個別通知を行う。
※受診券等通知は、歯周疾患検診、健康増進法施行規則第４条の２第４号に定める健康診査（生保健診）、がん検診の一部のみ
⑤ 対象者が医療機関に受診する。
⑥ 医療機関にて対象者が各健（検）診を受ける。
⑦ 検診を実施した医療機関が、対象者の検査結果を川崎市に提出する。
⑧ 健康管理システム（ガバメントクラウド）に記録した検診結果に関する情報を、情報提供ネットワークシステムにより他市区町村に提供する。
⑨ 既存の国保システムから、国保の資格者情報を管理する。（媒体連携）
⑩ 健康管理システム（ガバメントクラウド）に検診結果を記録し、厚生労働省あてに事業の実施報告を行う。

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		
成人検診情報ファイル		
2. 基本情報		
①ファイルの種類　※		[　　システム用ファイル　　] ＜選択肢＞ 1）システム用ファイル 2）その他の電子ファイル（表計算ファイル等）
②対象となる本人の数		[　10万人以上100万人未満　] ＜選択肢＞ 1）1万人未満 2）1万人以上10万人未満 3）10万人以上100万人未満 4）100万人以上1,000万人未満 5）1,000万人以上
③対象となる本人の範囲　※		市内在住の各種検診・健診・検査の実施に伴う受診者
	その必要性	市で実施するがん検診、歯周疾患検診、骨粗しょう症健診、生活保護受給者等健康診査、歯っぴーファミリー健診及び国民健康保険PSA検査の実施に伴う情報を適正に管理する必要があるため。
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 [○] 4情報（氏名、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　（　　）
	その妥当性	識別情報：対象者を正確に特定するために保有 連絡先等情報：対象者の居住地、世帯情報等を把握するために保有 業務関係情報 ・健康・医療関係情報：国民健康保険の資格者情報の管理、本人の健康管理及び健診の受診勧奨を適正に行うために保有 ・生活保護・社会福祉関係情報：生活保護及び中国残留邦人等支援給付の受給情報を把握し、生活保護受給者等健康診査の対象者とする。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成28年4月
⑥事務担当部署		健康福祉局保健医療政策部健康増進担当

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 （ 市民文化局戸籍住民サービス課 ） [ ] 行政機関・独立行政法人等 （ ） [○] 地方公共団体・地方独立行政法人 （ 他市町村 ） [○] 民間事業者 （ 検診実施医療機関 ） [ ] 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 （ ）
③入手の時期・頻度		・連絡先等情報については、庁内連携システムを使用して随時又は本人等から申請を受けた都度入手する。 ・検診受診記録については、検診を行った医療機関から月次単位で入手するとともに、転入者等については情報提供ネットワークシステムを使用して転入時又は転入から一定期間経過後等に入手する。
④入手に係る妥当性		【庁内連携による入手】 番号法第14条、14条第2項において個人番号利用事務実施者は他の個人番号利用事務等実施者に対して個人番号の提供を求めることができるとされている。このため健康増進事業に係る事務において必要な時期に情報を入手するものである。 【情報提供ネットワークシステム等による入手】 検診受診記録は、実施した医療機関から月次で入手する。また、転入者等の前住所地の市区町村における受診記録については、転入時又は前住所地の市区町村において受診記録を入手するまでのタイムラグを考慮して転入から一定期間経過後等に情報提供ネットワークシステムを使用して入手する。
⑤本人への明示		・他の機関から入手する場合：番号法第19条8号。 ・他部署から入手する場合：番号法第9条第2項に基づく条例 ・本人から入手する場合：本人を通じて入手することとし、利用目的を本人に明示する。
⑥使用目的 ※		検診対象者に向けた受診券やクーポン券等の個別通知の発行や、検診受診者の結果情報を経年的に管理し、適切な保健指導をはじめとした支援を実施するために使用する。
	変更の妥当性	
⑦使用の主体	使用部署 ※	健康福祉局保健医療政策部健康増進担当
	使用者数	[10人以上50人未満] ＜選択肢＞ 1）10人未満 2）10人以上50人未満 3）50人以上100人未満 4）100人以上500人未満 5）500人以上1,000人未満 6）1,000人以上
⑧使用方法 ※		1 検診情報の管理事務 医療機関から提出された検診票を、対象者であるか特定し、適正な検診事業の運営を図る。 2 受診勧奨事務 市民の健康増進を図るため、検診についての情報を個別勧奨等を通じ、お知らせする。 3 精密検査への受診勧奨 がん等の早期発見、早期治療を図るため、要精密検査となった受診者の方のうち、精密検査の受診報告がない方へ、精密検査の受診を個別勧奨をとおしてお知らせする。 4 保健指導の実施 受診結果を経年的に把握し、転入者については検査結果を前住所地から引き継ぐことにより、適切な保健指導を実施する。
	情報の突合 ※	連絡先等の4情報と住民票関係情報を突合し、対象者の確認を行う。
	情報の統計分析 ※	特定の個人を判別しうるような情報の統計は行わない。
	権利利益に影響を与え得る決定 ※	検診対象者であるかの決定を行う。

⑨使用開始日	平成28年4月1日

4. 特定個人情報ファイルの取扱いの委託		
委託の有無 ※		[委託する] ＜選択肢＞ 1）委託する 2）委託しない （ 1 ） 件
委託事項1		健康管理システムの運用・保守
①委託内容		健康管理システムの運用・保守
②取扱いを委託する特定個人情報ファイルの範囲		[特定個人情報ファイルの全体] ＜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 ※	「2. ③対象となる本人の範囲」と同じ。
	その妥当性	健康管理システムの安定的な稼働のため、専門的な知識を有し、かつ開発元でもある民間業者であるから
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 （ サーバ室内におけるシステムの直接操作 ）
⑤委託先名の確認方法		川崎市ホームページより「入札情報かわさき」にて確認可能
⑥委託先名		富士通Japan株式会社 川崎市ユニット
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	委託業者からの書面による申請に基づき、妥当性を考慮し書面により許諾を回答する。
	⑨再委託事項	運用・保守業務の一部を再委託
委託事項2～5		
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	健康増進法による健（検）診に関する情報
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	市内在住の検診対象者
⑥提供方法	[○] 情報提供ネットワークシステム [ ] 専用線 [ ] 電子メール [ ] 電子記録媒体（フラッシュメモリを除く。） [ ] フラッシュメモリ [ ] 紙 [ ] その他 （ ）
⑦時期・頻度	情報提供ネットワークシステムを介して特定個人情報の提供を求められた都度
提供先2～5	
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	
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　※		＜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。
②保管期間	期間	［　10年以上20年未満　］ ＜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	令和3年8月5日付け厚生労働省健康局健康課事務連絡『令和4年度向けデータ標準レイアウト改版におけるPHR（パーソナルヘルスレコード）の拡大に向けた対応について』1（3）別紙に基づき、次のとおりとされているため。 ○　がん検診によって把握した情報：5年間 ○　肝炎ウイルス検診によって把握した情報：生涯　※本市では、同法に基づく肝炎ウイルス検診は未実施。 ○　骨粗鬆症検診又は歯周疾患検診によって把握した情報：10年間
③消去方法		＜健康管理システムにおける措置＞ 保管期間を経過後、健康管理システムの保守・運用を行う事業者において、特定個人情報を順次消去する。 ＜システム連携基盤における措置＞ システム連携基盤の特定個人情報（副本）は、原本である業務システムの特定個人情報の消去と同期を取って、データベースから消去する。そのため、通常、システム連携基盤の事業者等が特定個人情報を消去することは無い。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・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。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。
7. 備考		

（別添2）特定個人情報ファイル記録項目

【成人検診情報ファイル】
別紙「地方公共団体基幹業務システムー基本データリスト（健康管理）」参照

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	
成人検診情報ファイル	
2．特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）	
リスク1：　目的外の入手が行われるリスク	
対象者以外の情報の入手を防止するための措置の内容	・検診を受付する委託医療機関において、受診券、本人確認書類（身分証明証等）の確認を実施し、対象者以外の情報を入手することのないよう努める。 ・医療機関から提出された検診票を健康管理システムへと登録する際に、検診票に記載された、氏名、住所、生年月日等と照合を行い、適切な情報のみをシステムへ取込む。
必要な情報以外を入手することを防止するための措置の内容	・健康管理システムを利用する職員を限定し、個人ごとのにユーザID及びパスワードによる認証を行い、認証後は、利用者権限を設定することにより、入手可能な情報に制限をかける。また、健康増進業務に必要な情報以外は入力できないよう、システム上担保されている。 ・申請書類については、必要な情報以外を誤って記載することがないよう、記入例等を工夫する。
その他の措置の内容	―
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2：　不適切な方法で入手が行われるリスク	
リスクに対する措置の内容	・申請書類等本人等を通じて入手する場合は、説明書等を用いて利用目的を本人に明示する。 ・健康管理システムを利用する職員を限定し、個人ごとにユーザID及びパスワードによる認証を行っている。また、認証後は、利用者権限を設定することによって、入手可能な情報に制限をかける。 ・アクセスログを取得し、定期的に確認を行う。
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	検診実施医療機関において、身分証明書の提示などにより、必ず本人確認を行い、対象者以外の情報を入手することのないよう努める。
個人番号の真正性確認の措置の内容	・個人番号カード、通知カード等の提示を受け、個人番号の真正性の確認を行う。 ・既存住基システムから入手した個人番号の照合により、真正性の確認を行う。
特定個人情報の正確性確保の措置の内容	・氏名・住所・生年月日等の個人番号以外の情報を複合的にチェックする。 ・特定個人情報の入力、削除及び訂正を行う際は、正確性を確保するため、入力、削除及び訂正を行った者以外の者が確認する等の確認作業を行う。 ・入力した原本（申請書類等）とデータファイルの照合を行い、入力チェックを行う。 ・入力、削除及び訂正作業に用いた申請書類等は、本市情報セキュリティ基準等に基づいて管理し、保管する。
その他の措置の内容	―
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
リスク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	・申請書類等は、対象者又は当該者と同一の世帯に属する者から受理することを原則とし、それ以外の代理人については、書面により対象者から委任を受けたことを確認できる者であり、かつ代理人の本人確認を行う。 ・特定個人情報が記載された申請書類等は、漏えい及び紛失を防止するため、入力及び照合した後は、施錠可能な場所に保管する。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　2）十分である 3）課題が残されている
特定個人情報の入手（情報提供ネットワークシステムを通じた入手を除く。）におけるその他のリスク及びそのリスクに対する措置	
―	

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	・システム連携基盤の職員認証・権限管理機能により、不適切な端末操作や情報照会などを抑止し、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保する。また、システム連携基盤では、各利用システムごとにIDとパスワードによる認証及びアクセス制御を実施しており、必要のない情報との紐付け等が行われるリスクを防止している。
事務で使用するその他のシステムにおける措置の内容	・健康管理システムは健康増進事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けが行われることはない。 ・情報管理責任者により、利用する職員ごとに業務単位で利用者権限を設定することで、アクセスできる情報を制限している。
その他の措置の内容	―
リスクへの対策は十分か	[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 権限のない者（元職員、アクセス権限のない職員等）によって不正に使用されるリスク	
ユーザ認証の管理	[行っている] <選択肢> 1）行っている 2）行っていない
具体的な管理方法	健康管理システムを利用する職員を限定し、個人ごとにユーザID及びパスワードによる認証を行う。
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	・アクセス権限の発効・失効の管理は、所管課からの報告により実施する。 ・アクセス権限の発効、失効についての記録を残す。
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	・適切なアクセス権限が付与されるよう、利用する職員ごとに業務単位で利用者権限を設定する。 ・操作ログを取得・保管し、不正な利用を分析するため、定期的に確認を行う。
特定個人情報の使用の記録	[記録を残している] <選択肢> 1）記録を残している 2）記録を残していない
具体的な方法	・健康管理システムへのログイン記録、健康管理システムの操作記録、特定個人情報を取り扱った記録（操作日、操作時間、取扱者）等のログ情報を残し、不正な操作がないことについて定期的に確認を行う。
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
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	・操作ログを取得し、定期的に確認を行う。 ・利用する職員への研修等において、事務外利用の禁止等について指導する。
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	・利用権限を業務単位ごとに設定することで、アクセスできる情報を制限する。 ・操作端末へのファイルのダウンロードはできない仕組みとなっている。
リスクへの対策は十分か	[十分である] <選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の使用におけるその他のリスク及びそのリスクに対する措置	

4. 特定個人情報ファイルの取扱いの委託		[　]委託しない
委託先による特定個人情報の不正入手・不正な使用に関するリスク 委託先による特定個人情報の不正な提供に関するリスク 委託先による特定個人情報の保管・消去に関するリスク 委託契約終了後の不正な使用等のリスク 再委託に関するリスク		
情報保護管理体制の確認		①委託先の選定要件として、情報セキュリティマネジメントシステム(ISMS)、ISO9000等の認証の取得及びプライバシーマークの認定等を考慮して選定する。 ②業務委託契約書に次に掲げるものに関する事項を明記し、契約締結にあたり本市の情報セキュリティに関する遵守事項を説明する。 (ア)『川崎市情報セキュリティ基準』等の遵守 (イ) 機密保持 (ウ) 再委託の禁止又は制限 (エ) 指示目的外の使用及び第三者への提供の禁止 (オ) 情報の複写及び複製の禁止 (カ) 情報の帰属 (キ) 情報資産の授受・搬送・保管・廃棄等 (ク) 本市の情報システムの使用やその設置場所への入退室 (ケ) 事故発生時における報告義務 (コ) 事故時等の公表 (サ) 情報セキュリティの確保に必要な管理事項 ③委託する業務で取り扱う情報の機密性を考慮し、委託先の責任者や実施者から必要に応じ、機密保持等に関する誓約書を提出させる。
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	・作業者を限定するため、委託作業者の名簿を事前に提出させる。 ・操作ログを取得、定期的に確認することで、不正な使用がないことを確認する。
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	・アクセスログを取得し、ログイン記録を残す。 ・契約書等に基づき、委託業務が実施されていることを適時確認するとともに、その記録を残す。
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	・委託先から他社への特定個人情報の提供は一切認めないことを契約書上明記する。 ・必要があれば、当市職員が現地調査を行うことも可能とする。
	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	・情報を提供する場合は、日付及び件数等を記載した受渡票等の書類により行い、管理する。
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	委託契約書にて、以下の措置について規定し、必要に応じて現地調査を行う。 ・情報の複写及び複製を行わないこと ・業務終了後、速やかに本市に情報を返却、又は本市の指示に従い、情報を復元できないよう措置を講じ、安全適切に廃棄しなければならない。 ・返却又は廃棄する際は、受渡票等の書類により行うこと

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	1　業務委託契約書に次に掲げるものに関する事項を明記し、契約締結にあたり本市の情報セキュリティに関する遵守事項を説明する。 ・川崎市情報セキュリティ基準等の遵守 ・機密保持 ・再委託の禁止又は制限 ・支持目的外の使用及び第三者への提供の禁止 ・情報の複写及び複製の禁止 ・情報の帰属 ・情報資産の授受・搬送・保管・廃棄等 ・本市の情報システムの使用やその設置場所への入退室 ・事故発生時における報告義務 ・違反事実の公表 ・情報セキュリティの確保に必要な管理事項 2　委託する業務で取り扱う情報の機密性を考慮し、委託先の責任者や実施者から必要に応じ、機密保持等に関する誓約書を提出させる。
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　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	書面による許諾の無い再委託を禁止するとともに、再委託先においては委託先と同等のリスク対策を実施することとしている。
その他の措置の内容		特定個人情報ファイルの適切な取扱いが確保されていることを検証及び確認するため委託先及び再委託先（再々委託以降を行う場合の当該再々委託先等についても同じ。）に対して、監査又は検査を行っている。
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	・提供及び移転する特定個人情報ファイルについては、提供データ作成時に共通システム内のログに作成日時、提供日時等の実行処理結果が記録される仕組みになっている。 ・システム連携基盤では、特定個人情報の提供・移転日時及び提供・移転先について記録を残している。
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	・番号法第9条第2項及び第19条第11号に基づく条例に規定される事項に限り提供又は移転する。 ・同一機関内における移転の際は、提供先の各所管課あて利用の許可を行った場合に、利用内容を確認した上で、必要な情報のみを提供することとしている。 ・システム連携基盤では、不正な情報の提供・移転が行われていないことをシステムログにより確認している。
その他の措置の内容	－
リスクへの対策は十分か	[　十分である　] <選択肢> 1）特に力を入れている　2）十分である 3）課題が残されている
リスク2： 不適切な方法で提供・移転が行われるリスク	
リスクに対する措置の内容	・業務所管課によりアクセス権限を管理し、アクセスできる情報を制限している。 ・操作ログを記録し、誰がいつどの端末から、どの情報を参照したかを把握している。 ・閲覧、データ提供等については、許可書、依頼書等で記録管理している。 ・システム連携基盤では、各利用システムごとにIDとパスワードによる認証及びアクセス制御を実施しており、不適切な方法で特定個人情報がやりとりされることを防止している。
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	・担当職員への特定個人情報保護についての周知徹底を行う。 ・特定個人情報の提供・移転時には、複数の担当者による等、内容の確認を行う。 ・閲覧、データ提供については、許可書、依頼書等で管理している。庁内連携システム等によるデータ提供は、システム上、許可された提供先にのみ提供されるよう制限している。 ・システム連携基盤では、あらかじめ設定された提供・移転先のみが連携可能となっており、また、すべての情報を連携することができない仕組みとなっている。
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	＜システム連携基盤における措置＞ ①システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止している。また、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報照会機能（＊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）番号法第19条第8号に基づく主務省令第2条の表に基づき、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。 ＜中間サーバーの運用における措置＞ ①中間サーバーの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。
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	＜システム連携基盤における措置＞ ①システム連携基盤は自機関向けの中間サーバーとだけ、通信および特定個人情報の入手のみを実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用した特定個人情報の入手のみ実施できるよう設計されるため、安全性が担保されている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。
リスクへの対策は十分か	[　十分である　] ＜選択肢＞ 1）特に力を入れている　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	＜システム連携基盤における措置＞ ①システム連携基盤は、照会対象者に付番された個人番号に基づき、団体内統合宛名番号を付番してインタフェースシステムより処理通番等を入手した上で、情報提供用個人識別符号の取得依頼ができるよう設計されるため、照会対象者の個人番号に基づき正確に情報提供用個人識別符号の紐付けが行われることから、正確な照会対象者に係る特定個人情報を入手することが担保されている。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、特定個人情報保護委員会との協議を経て、総務大臣が設置・管理する情報提供ネットワークシステムを使用して、情報提供用個人識別符号により紐付けられた照会対象者に係る特定個人情報を入手するため、正確な照会対象者に係る特定個人情報を入手することが担保されている。
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	＜システム連携基盤における措置＞ ①情報照会が完了又は中断した情報照会結果などについては、一定期間経過後に当該結果を自動で削除することにより、特定個人情報が漏えい、紛失するリスクを軽減している。 ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止している。また、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①中間サーバーは、情報提供ネットワークシステムを使用した特定個人情報の入手のみを実施するため、漏えい・紛失のリスクに対応している（＊）。 ②既存システムからの接続に対し認証を行い、許可されていないシステムからのアクセスを防止する仕組みを設けている。 ③情報照会が完了又は中断した情報照会結果については、一定期間経過後に当該結果を情報照会機能において自動で削除することにより、特定個人情報が漏えい・紛失するリスクを軽減している。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （＊）中間サーバーは、情報提供ネットワークシステムを使用して特定個人情報を送信する際、送信する特定個人情報の暗号化を行っており、照会者の中間サーバーでしか復号できない仕組みになっている。そのため、情報提供ネットワークシステムでは復号されないものとなっている。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、漏えい・紛失のリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい・紛失のリスクに対応している。 ③中間サーバー・プラットフォーム事業者の業務は、中間サーバー・プラットフォームの運用、監視・障害対応等であり、業務上、特定個人情報へはアクセスすることはできない。 ＜中間サーバーの運用における措置＞ ①中間サーバーの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。
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	＜システム連携基盤における措置＞ ①慎重な対応が求められる情報（DV被害者など）については中間サーバーにて情報照会に対する自動応答がなされないよう、自動応答を不可とする個人（団体内統合宛名番号など）または特定個人情報を管理し、中間サーバーの自動応答不可フラグを設定することで、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。 ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止している。また、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（＊）により、情報提供ネットワークシステムにおける照会許可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、中間サーバーにも格納して、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。 ②情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供ネットワークシステムから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。 ③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。 ④中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （＊）情報提供ネットワークシステムを使用した特定個人情報の提供の要求の受領及び情報提供を行う機能。 ＜中間サーバーの運用における措置＞ ①中間サーバーの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。
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	＜システム連携基盤における措置＞ ①システム連携基盤は、自機関向けの中間サーバーとだけ、通信及び特定個人情報の提供を実施するよう設計されているため、不適切な方法で提供されるリスクに対応している。 ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報提供などを抑止している。また、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①セキュリティ管理機能（＊）により、情報提供ネットワークシステムに送信する情報は、情報照会者から受領した暗号化鍵で暗号化を適切に実施した上で提供を行う仕組みになっている。 ②中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 （＊）暗号化・復号機能と、鍵情報及び照会許可用照合リストを管理する機能。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、不適切な方法で提供されるリスクに対応している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで漏えい･紛失のリスクに対応している。 ③中間サーバー・プラットフォームの保守・運用を行う事業者においては、特定個人情報に係る業務にはアクセスができないよう管理を行い、不適切な方法での情報提供を行えないよう管理している。 ＜中間サーバーの運用における措置＞ ①中間サーバーの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。
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	＜システム連携基盤における措置＞ システム連携基盤は自機関向けの中間サーバーとだけ、通信および特定個人情報の提供のみを実施するよう設計されるため、誤った相手に特定個人情報が提供されるリスクに対応している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能により、情報提供ネットワークシステムに情報提供を行う際には、情報提供許可証と情報照会者への経路情報を受領した上で、情報照会内容に対応した情報提供をすることで、誤った相手に特定個人情報が提供されるリスクに対応している。 ②情報提供データベース管理機能（＊）による、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 ③情報提供データベース管理機能では、情報提供データベースの副本データを既存業務システムの原本と照合するためのエクスポートデータを出力する機能を有している。 （＊）特定個人情報を副本として保存・管理する機能。
リスクへの対策は十分か	[十分である] ＜選択肢＞ 1）特に力を入れている 2）十分である 3）課題が残されている

情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置
＜システム連携基盤における措置＞ ①システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会・情報連携を抑止する。また、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ②システム連携基盤は、自機関向けの中間サーバーとだけ、通信及び特定個人情報の入手・提供のみを実施するよう設計されているため、安全性が担保されている。 ③システム連携基盤と自機関向けの中間サーバーの間は、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・ソフトウェアにおける措置＞ ①中間サーバーの職員認証・権限管理機能では、ログイン時の職員認証の他に、ログイン・ログアウトを実施した職員、時刻、操作内容の記録が実施されるため、不適切な接続端末の操作や、不適切なオンライン連携を抑止する仕組みになっている。 ②情報連携においてのみ、情報提供用個人識別符号を用いることがシステム上担保されており、不正な名寄せが行われるリスクに対応している。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバーと既存システム、情報提供ネットワークシステムとの間は、高度なセキュリティを維持した行政専用のネットワーク（総合行政ネットワーク等）を利用することにより、安全性を確保している。 ②中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ③中間サーバー・プラットフォームでは、特定個人情報を管理するデータベースを地方公共団体ごとに区分管理（アクセス制御）しており、中間サーバー・プラットフォームを利用する団体であっても他団体が管理する情報には一切アクセスできない。 ④特定個人情報の管理を地方公共団体のみが行うことで、中間サーバー・プラットフォームの保守・運用を行う事業者における情報漏えい等のリスクを極小化する。 ＜中間サーバーの運用における措置＞ ①中間サーバーの職員認証・権限管理において、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。

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	＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームを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。	
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	＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③導入しているOS及びミドルウェアについて、必要に応じてセキュリティパッチの適用を行う。 ＜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。	
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	[発生あり]	<選択肢> 1）発生あり 2）発生なし

	その内容	別紙（個人情報に関する重大事故について）を参照
	再発防止策の内容	別紙（個人情報に関する重大事故について）を参照

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	生存者と同じ方法で、法令に定める期間保管する。	
その他の措置の内容		—	
リスクへの対策は十分か		[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
リスク2： 特定個人情報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		・基本4情報等の宛名情報については、既存住基システムとの連携により随時更新される。 ・本人の申請等により、変更等が生じた場合はその都度データを更新している。	
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： 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	・保管期間を経過後、健康管理システムの保守・運用を行う事業者において、特定個人情報を順次消去する。 ・帳票については、本市の規定に基づき、保管・管理を適切に行い、廃棄時にはシュレッダー等による裁断又は焼却処理を行う。 ＜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。	
その他の措置の内容		—	
リスクへの対策は十分か		[十分である]	<選択肢> 1）特に力を入れている 2）十分である 3）課題が残されている
特定個人情報の保管・消去におけるその他のリスク及びそのリスクに対する措置			

別　紙

個人情報に関する重大事故について

事案１　国民健康保険高額療養費支給申請書の紛失

１ 事案の内容

（１） 発生（発覚）時期

令和６年４月８日

（２） 事案の概要

宮前区役所区民サービス部保険年金課において、令和６年３月支給分の国民健康保険高額療養費支給申請書を紛失した。

（３） 原因

事務担当者が足元に個人情報が記載された書類を数日にわたって放置していたことから、個人情報の適正な管理が行われていなかった。

（４） 影響

４０４件（２９５世帯分）の個人情報を紛失した。紛失した書類に含まれる情報は次のとおり。なお、現時点で個人情報の漏洩は確認されていない。

- 世帯主氏名、住所、電話番号
- 個人番号（マイナンバー）※本人の記載があった場合
- 被保険者証記号及び番号、振込先金融機関の情報
- 病院等へ支払った一部負担金の合計額、高額療養費額、支給申請額
- 診療を受けた被保険者の氏名、生年月日、医療機関、実日数、一部負担金の額

（５） 事故発覚後の対応

令和６年４月８日	事務担当者により申請書が所在不明であることが判明
令和６年４月８日～４月２２日	事務担当者による捜索を継続
令和６年５月１日	報道発表
令和６年６月３日	個人情報保護委員会より文書指導

２　再発防止策

（１）国民健康保険事務における再発防止策

・該当事務について、事務手続きのフローを再度、課内で確認するとともに、全職員において、個人情報の厳格な管理を徹底する。

・該当事務以外の事務についても、事務フローの確認と個人情報の取扱いについて、改めてチェックを行う。

・書類の紛失等、事務事故が疑われる場合には、即時に上司に報告することを全職員に対し周知徹

底する。

（２） 評価実施機関（川崎市）における再発防止策

・保護責任者に対して、特定個人情報の安全管理措置（特に、人的及び組織的安全管理措置）に関する研修を実施することとする。また、研修未受講の事務担当者に対し保護責任者から受講を促す。

・全ての特定個人情報保護評価書のⅣ_２．「従業者に対する教育・啓発」項目に、上記の研修についての記載を追加する。

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年に1回、チェックシート等により自己点検を実施することとしている。 ＜中間サーバー･プラットフォームにおける措置＞ ①運用規則等に基づき、中間サーバー･プラットフォーム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。	
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	＜外部監査＞ ・情報統括監理者（CIO）の責任において情報セキュリティ監査人（専門的技術を持った法人）に委託することにより実施している情報セキュリティ監査の中で、特定個人情報ファイルの取扱いの適正性についても併せて監査を実施する。 ・監査の結果については、事務を所管する局の長（情報セキュリティ責任者）に通知し、改善のための措置を検討・実施する。 ＜中間サーバー･プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	

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	・情報セキュリティに関する研修やeラーニング等を利用して、情報セキュリティに関する知識の取得及び情報収集を行うように指導を行う。 ・新人職員や異動者に対して、特定個人情報や情報セキュリティに関する研修等を必要に応じて実施する。 ・本市で発生した特定個人情報に関する重大事故の再発防止の観点から、保護責任者に対して、特定個人情報の安全管理措置（特に、人的及び組織的安全管理措置）に関する研修を実施する。また、研修未受講の事務担当者に対し保護責任者から受講を促す。	

3. その他のリスク対策

【中間サーバー・プラットフォームにおける措置】
・中間サーバー・プラットフォームを活用することにより、統一した設備環境による高レベルのセキュリティ監理（入退室監理等）、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。

＜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。

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	・健康福祉局保健医療政策部健康増進担当 住　　所：〒210-8577　川崎市川崎区宮本町１番地 電話番号：044-200-2431 ・総務企画局コンプライアンス推進・行政情報管理部行政情報課（情報公開担当） 住　　所：〒210-8577　川崎市川崎区宮本町１ 電話番号：044-200-2108
②請求方法	個人情報の保護に関する法律及び川崎市個人情報の保護に関する法律施行条例に基づく開示・訂正等の請求を受け付ける。
特記事項	
③手数料等	[　　無料　　]　＜選択肢＞ 1) 有料　　2) 無料 （手数料額、納付方法：閲覧は無料。ただし、写しの交付を希望する場合は、実費を負担。　　）
④個人情報ファイル簿の公表	[　　行っている　　]　＜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	成人検診情報ファイル
公表場所	川崎市ホームページ（https://www.city.kawasaki.jp/170/page/0000152460.html）
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	健康福祉局保健医療政策部健康増進担当 住　　所：〒210-8577　川崎市川崎区宮本町１番地 電話番号：044-200-2431
②対応方法	―

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和7年1月20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	かわさき情報プラザ、各区役所市政資料コーナー、川崎市ホームページ及び事務所管課において全項目評価書を公開し、ファクス、郵送、持参、専用フォームにて意見を受付予定。
②実施日・期間	令和6年10月9日から11月8日までの30日間
③期間を短縮する特段の理由	期間短縮なし
④主な意見の内容	意見なし
⑤評価書への反映	評価書への反映事項はなし
3. 第三者点検	
①実施日	令和6年11月28日
②方法	川崎市情報公開運営審議会（特定個人情報保護評価点検委員会）において第三者点検を実施。
③結果	川崎市情報公開運営審議会（特定個人情報保護評価点検委員会）から、次のとおり結果通知あり。 健康増進事業の実施に関する事務に係る特定個人情報保護評価に関し、提出を受けた特定個人情報保護評価書を適合性及び妥当性の観点から点検したところ、特定個人情報保護評価指針及び川崎市情報セキュリティ基準にのっとり、特定個人情報ファイルの適正な取扱い及び必要な保護措置がとられているものと考えます。
4. 個人情報保護委員会の承認 【行政機関等のみ】	
①提出日	
②個人情報保護委員会による審査	

（別添3）変更箇所

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和5年1月25日	Ⅰ　7．評価実施機関における担当部署　①部署	健康福祉局保健所健康増進課	健康福祉局保健医療政策部健康増進担当	事後	
令和5年1月25日	Ⅰ　7．評価実施機関における担当部署　②所属長の役職名	健康福祉局保健所健康増進課課長	健康福祉局保健医療政策部健康増進担当課長	事後	
令和5年1月25日	Ⅴ　1．特定個人情報の開示・訂正・利用停止請求①請求先	健康福祉局保健所健康増進課	健康福祉局保健医療政策部健康増進担当	事後	
令和5年1月25日	Ⅴ　1．特定個人情報の開示・訂正・利用停止請求④個人情報ファイル簿の公表	（http://www.city.kawasaki.jp/160/page/0000047748.html）	（http://www.city.kawasaki.jp/170/page/0000047748.html）	事後	
令和5年1月25日	Ⅴ　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	健康福祉局保健所健康増進課	健康福祉局保健医療政策部健康増進担当	事後	
令和5年1月25日	Ⅱ　2．基本情報⑥事務担当部署	健康福祉局保健所健康増進課	健康福祉局保健医療政策部健康増進担当	事後	
令和5年1月25日	Ⅱ　3．特定個人情報の入手・使用④使用の主体　使用部署	健康福祉局保健所健康増進課	健康福祉局保健医療政策部健康増進担当	事後	
令和6年3月26日	Ⅲ　7．特定個人情報の保管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	発生あり	発生なし	事後	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和6年3月26日	Ⅲ　7．特定個人情報の保管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その内容	別紙（個人情報に関する重大事故について）を参照		事後	
令和6年3月26日	Ⅲ　7．特定個人情報の保管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その内容	別紙（個人情報に関する重大事故について）を参照		事後	
令和6年3月26日	Ⅴ　1．特定個人情報の開示・訂正・利用停止請求①請求先	総務企画局情報管理部行政情報課（情報公開担当）	総務企画局コンプライアンス・行政情報管理部行政情報課（情報公開担当）	事後	
令和6年3月26日	Ⅴ　1．特定個人情報の開示・訂正・利用停止請求①請求方法	川崎市個人情報保護条例に基づく開示・訂正等の請求を受け付ける。	個人情報の保護に関する法律及び川崎市個人情報の保護に関する法律施行条例に基づく開示・訂正等の請求を受け付ける。	事後	
令和6年3月26日	Ⅴ　1．特定個人情報の開示・訂正・利用停止請求④個人情報ファイル簿の公表	（http://www.city.kawasaki.jp/170/page/0000047748.html）	（https://www.city.kawasaki.jp/170/page/0000152460.html）	事後	
令和7年1月20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	（省略） また、番号法第9条第1項　別表第1の76の項（健康増進法（平成十四年法律第百三号）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）の規定により、個人番号を用いることになる。	（省略） また、番号法第9条第1項　別表の111の項（健康増進法（平成十四年法律第百三号）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）の規定により、個人番号を用いることになる。	事前	
令和7年1月20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（別添1）事務の内容	成人保健情報管理システム	健康管理システム（ガバメントクラウド）	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20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（別添1）事務の内容	（備考） （省略） ⑧　成人保健情報管理システムに記録した検診結果に関する情報を、情報提供ネットワークシステムにより他市区町村に提供する。 （省略） ⑩　成人保健情報管理システムに検診結果を記録し、厚生労働省あてに事業の実施報告を行う。	（備考） （省略） ⑧　健康管理システム（ガバメントクラウド）に記録した検診結果に関する情報を、情報提供ネットワークシステムにより他市区町村に提供する。 （省略） ⑩　健康管理システム（ガバメントクラウド）に検診結果を記録し、厚生労働省あてに事業の実施報告を行う。	事前	
令和7年1月20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　①システムの名称	成人保健情報管理システム	健康管理システム	事前	
令和7年1月20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	（省略） 3　情報提供機能 　各業務で管理している別表2の提供業務情報を受領し、中間サーバーへの情報提供を行う。 （省略）	（省略） 3　情報提供機能 　各業務で管理している番号法第19条第8号に基づく主務省令第2条の表の提供業務情報を受領し、中間サーバーへの情報提供を行う。 （省略）	事前	
令和7年1月20日	Ⅰ　基本情報5．個人番号の利用　法令上の根拠	・番号法第9条第1項　別表第1の76の項 ・川崎市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条例第3条	・番号法第9条第1項　別表の111の項 ・川崎市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条例第3条	事前	
令和7年1月20日	Ⅰ　基本情報6．情報提供ネットワークシステムによる情報連携②法令上の根拠	【情報照会】 番号法第19条第8号　別表第2の102の2項 【情報提供】 番号法第19条第8号　別表第2の102の2項	【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139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139の項	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅱ　特定個人情報ファイルの概要2．基本④記録される項目　全ての記録項目（別添2）ファイル記録項目	一覧表を削除し、右記を追記	（別添2）特定個人情報ファイル記録項目を参照	事前	
令和7年1月20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	成人保健情報管理システムの運用・保守	健康管理システムの運用・保守	事前	
令和7年1月20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 ①委託内容	成人保健情報管理システムの運用・保守	健康管理システムの運用・保守	事前	
令和7年1月20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 ②取扱いを委託する特定個人情報ファイルの範囲　その妥当性	成人保健情報管理システムの安定的な稼働のため、専門的な知識を有し、かつ開発元でもある民間業者であるから	健康管理システムの安定的な稼働のため、専門的な知識を有し、かつ開発元でもある民間業者であるから	事前	
令和7年1月20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 ⑥委託先名	富士通Japan株式会社　川崎支店	富士通Japan株式会社　川崎市ユニット	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅱ　ファイルの概要5．特定個人情報の提供・移転　提供先1①法令上の根拠	番号法第19条第8号　別表第2（102の2項）	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	事前	
令和7年1月20日	Ⅱ　特定個人情報ファイルの概要6．特定個人情報の保管・消去①保管場所	＜健康管理システム＞ ・健康管理システムは、入退室管理をしている庁舎エリア内の、さらに静脈認証（権限のある者のみ登録）を必要とする部屋に設置した施錠したラック内にサーバを設置し、保管している。 ・サーバへのアクセスはIDとパスワードによる認証が必要となる。 ＜システム連携基盤サーバにおける措置＞ ・システム連携基盤サーバはセキュリティゲートにて入退館管理をしているデータセンター内で、さらに入退室管理を行っている部屋（サーバ室）に設置したサーバ内に保管する。 ＜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。	＜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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅱ　特定個人情報ファイルの概要6．特定個人情報の保管・消去③消去方法	＜成人保健情報管理システムにおける措置＞ ①保管期間を経過後、成人保健情報管理システムの保守・運用を行う事業者において、特定個人情報を順次消去する。 ②ディスク交換やハード更改等の際は、成人保健情報管理システムに係る保守を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ＜システム連携基盤における措置＞ ①システム連携基盤の特定個人情報（副本）は、原本である業務システムの特定個人情報の消去と同期を取って、データベースから消去する。そのため、通常、システム連携基盤の事業者等が特定個人情報を消去することは無い。また、ディスク交換やハード更改等の際は、保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ＜中間サーバー・プラットフォームにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施されるため、通常、中間サーバー・プラットフォームの保守・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。 ②ディスク交換やハード更改等の際は、中間サーバー・プラットフォームの保守・運用を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。	＜健康管理システムにおける措置＞ 保管期間を経過後、健康管理システムの保守・運用を行う事業者において、特定個人情報を順次消去する。 ＜システム連携基盤における措置＞ システム連携基盤の特定個人情報（副本）は、原本である業務システムの特定個人情報の消去と同期を取って、データベースから消去する。そのため、通常、システム連携基盤の事業者等が特定個人情報を消去することは無い。 （省略） ＜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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手 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	（省略） ・医療機関から提出された検診票を成人保健情報管理システムへと登録する際に、検診票に記載された、氏名、住所、生年月日等と照合を行い、適切な情報のみをシステムへ取込む。	（省略） ・医療機関から提出された検診票を健康管理システムへと登録する際に、検診票に記載された、氏名、住所、生年月日等と照合を行い、適切な情報のみをシステムへ取込む。	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手 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吸うための措置の内容	・成人保健情報管理システムを利用する職員を限定し、個人ごとのにユーザID及びパスワードによる認証を行い、認証後は、利用者権限を設定することにより、入手可能な情報に制限をかける。 （省略）	・健康管理システムを利用する職員を限定し、個人ごとのにユーザID及びパスワードによる認証を行い、認証後は、利用者権限を設定することにより、入手可能な情報に制限をかける。 （省略）	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 2. 特定個人情報の入手 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	（省略） ・成人保健情報管理システムを利用する職員を限定し、個人ごとにユーザID及びパスワードによる認証を行っている。また、認証後は、利用者権限を設定することによって、入手可能な情報に制限をかける。 （省略）	（省略） ・健康管理システムを利用する職員を限定し、個人ごとにユーザID及びパスワードによる認証を行っている。また、認証後は、利用者権限を設定することによって、入手可能な情報に制限をかける。 （省略）	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク1：目的を超えた紐付け、事務に必要のない情報との紐付けが行われるリスク 事務で使用するその他のシステムにおける措置の内容	・成人保健情報管理システムは健康増進事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けが行われることはない。 （省略）	・健康管理システムは健康増進事業を行う上で必要な情報のみを保持しており、必要のない情報は記録できないため、紐付けが行われることはない。 （省略）	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（基職員、アクセス権限のない職員等）によって不正に使用されるリスク　ユーザ認証の管理　具体的な管理方法	成人保健情報システムを利用する職員を限定し、個人ごとにユーザID及びパスワードによる認証を行う。	健康管理システムを利用する職員を限定し、個人ごとにユーザID及びパスワードによる認証を行う。	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3. 特定個人情報の使用 リスク2：権限のない者（基職員、アクセス権限のない職員等）によって不正に使用されるリスク　特定個人情報の使用の記録　具体的な方法	・成人保健情報管理システムへのログイン記録、成人保健情報管理システムの操作記録、特定個人情報を取り扱った記録（操作日、操作時間、取扱者）等のログ情報を残し、不正な操作がないことについて定期的に確認を行う。	・健康管理システムへのログイン記録、健康管理システムの操作記録、特定個人情報を取り扱った記録（操作日、操作時間、取扱者）等のログ情報を残し、不正な操作がないことについて定期的に確認を行う。	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
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策6．情報提供ネットワークシステムとの接続　リスク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	＜システム連携基盤における措置＞ ①システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止する。 （省略） （＊2）番号法別表第2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。 （省略）	＜システム連携基盤における措置＞ ①システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止している。 （省略） （＊2）番号法第19条第8号に基づく主務省令第2条の表に基づき、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。 （省略）	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策6．情報提供ネットワークシステムとの接続　リスク4：入手の際に特定個人情報が漏えい・紛失するリスク　リスクに対する措置の内容	（省略） ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止する。 （省略）	（省略） ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止している。 （省略）	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策6．情報提供ネットワークシステムとの接続　リスク5：不正な提供が行われるリスク　リスクに対する措置の内容	（省略） ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止する。また、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（＊）により、情報提供ネットワークシステムにおける照会許可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、中間サーバーにも格納して、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。 （省略）	（省略） ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報照会などを抑止している。また、人事異動や権限変更等が生じた場合は、人事情報を適宜反映することで、その正確性を担保している。 ＜中間サーバー・ソフトウェアにおける措置＞ ①情報提供機能（＊）により、情報提供ネットワークシステムにおける照会許可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、中間サーバーにも格納して、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。 （省略）	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6．情報提供ネットワークシステムとの接続 リスク6：不適切な方法で提供されるリスク　リスクに対する措置の内容	＜システム連携基盤における措置＞ ①システム連携基盤は自機関向けの中間サーバーとだけ通信および特定個人情報の提供のみを実施するよう設計されるため、不適切な方法で提供されるリスクに対応している。 ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報提供などを抑止する。 （省略）	＜システム連携基盤における措置＞ ①システム連携基盤は、自機関向けの中間サーバーとだけ、通信及び特定個人情報の提供を実施するよう設計されているため、不適切な方法で提供されるリスクに対応している。 ②システム連携基盤の職員認証・権限管理機能により、ログイン時の職員認証のほか、ログイン・ログアウトを実施した職員、時刻、操作内容等の記録が実施されるため、不適切な端末操作や情報提供などを抑止している。 （省略）	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 6. 情報提供ネットワークシステムとの接続 リスク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	（省略） ②情報提供データベース管理機能（＊）により、「情報提供データベースへのインポートデータ」の形式チェックと、接続端末の画面表示等により情報提供データベースの内容を確認できる手段を準備することで、誤った特定個人情報を提供してしまうリスクに対応している。 （省略）	（省略） ②情報提供データベース管理機能（＊）による、「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。 （省略）	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策6. 情報提供ネットワークシステムとの接続　情報提供ネットワークシステムとの接続に伴うその他のリスク及びそのリスクに対する措置	（省略） ②システム連携基盤は自機関向けの中間サーバーとだけ通信および特定個人情報の入手・提供のみを実施するよう設計されるため、安全性が担保されている。 （省略）	（省略） ②システム連携基盤は、自機関向けの中間サーバーとだけ、通信及び特定個人情報の入手・提供のみを実施するよう設計されているため、安全性が担保されている。 （省略）	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 ⑤物理的対策　具体的な対策の内容	＜健康管理システムにおける措置＞ ①健康管理システムは、入退室管理をしている庁舎エリア内の、さらに静脈認証（権限のある者のみ登録）を必要とする部屋に設置した施錠したラック内にサーバを設置し、保管している。 ②停電等に備え、災害時の非常用電源装置等を付設している。 ＜システム連携基盤における措置＞ ①システム連携基盤はセキュリティゲートにて入退館管理をしているデータセンター内で、さらに入退室管理を行っている部屋（サーバ室）に設置したサーバ内に保管する。 ②停電等に備え、災害時の非常用電源装置等を付設している。 ③監視設備として監視カメラ等を設置している。 ＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォーム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。	＜中間サーバー・プラットフォームにおける措置＞ ①中間サーバー・プラットフォームを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。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管・消去 ⑥技術的対策　具体的な対策の内容	＜健康管理システムにおける措置＞ ①健康管理システムでは、F／Wや通信の暗号化により、アクセス制限、侵入防止対策を行っている。 ②健康管理システムのサーバには、新種の不正プログラムに対応するためにウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③健康管理システムで利用する端末には、新種の不正プログラムに対応するために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。 ＜システム連携基盤における措置＞ ①システム連携基盤では、F／Wや通信の暗号化により、アクセス制限、侵入防止対策を行っている。 ②システム連携基盤では、新種の不正プログラムに対応するために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。 ＜中間サーバー･プラットフォームにおける措置＞ ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネットワークを効率的かつ包括的に保護する装置）等を導入し、アクセス制限、侵入検知及び侵入防止を行うとともに、ログの解析を行う。 ②中間サーバー・プラットフォームでは、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。	（省略） ＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP（「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和4年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	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管消去　リスク1：特定個人情報の漏洩・滅失・毀損リスク　⑤物理的対策　具体的な対策の内容	＜成人保健情報管理システムにおける措置＞ ①成人保健情報管理システムは、入退室管理をしている庁舎エリア内の、さらに静脈認証（権限のある者のみ登録）を必要とする部屋に設置した施錠したラック内にサーバを設置し、保管している。 （省略）	＜健康管理システムにおける措置＞ ①健康管理システムは、入退室管理をしている庁舎エリア内の、さらに静脈認証（権限のある者のみ登録）を必要とする部屋に設置した施錠したラック内にサーバを設置し、保管している。 （省略）	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管消去　リスク1：特定個人情報の漏洩・滅失・毀損リスク　⑥技術的対策　具体的な対策の内容	＜成人保健情報管理システムにおける措置＞ ①成人保健情報管理システムでは、F／Wや通信の暗号化により、アクセス制限、侵入防止対策を行っている。 ②成人保健情報管理システムのサーバには、新種の不正プログラムに対応するためにウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③成人保健情報管理システムで利用する端末には、新種の不正プログラムに対応するために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。 （省略）	＜健康管理システムにおける措置＞ ①健康管理システムでは、F／Wや通信の暗号化により、アクセス制限、侵入防止対策を行っている。 ②健康管k円光理システムのサーバには、新種の不正プログラムに対応するためにウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ③健康管理システムで利用する端末には、新種の不正プログラムに対応するために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。 （省略）	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管消去　リスク1：特定個人情報の漏洩・滅失・毀損リスク　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	発生あり	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管消去　リスク1：特定個人情報の漏洩・滅失・毀損リスク　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　その内容	右記を追記	別紙（個人情報に関する重大事故について）を参照	事前	
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7. 特定個人情報の保管消去　リスク1：特定個人情報の漏洩・滅失・毀損リスク　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　再発防止策の内容	右記を追記	別紙（個人情報に関する重大事故について）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
令和7年1月20日	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7．特定個人情報の保管・消去　リスク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	・保管期間を経過後、健康管理システムの保守・運用を行う事業者において、特定個人情報を順次消去する。 ・ディスク交換やハード更改等の際は、健康管理システムに係る保守を行う事業者において、保存された情報が読み出しできないよう、物理的破壊又は専用ソフト等を利用して完全に消去する。 ・帳票については、本市の規定に基づき、保管・管理を適切に行い、廃棄時にはシュレッダー等による裁断又は焼却処理を行う。	・保管期間を経過後、健康管理システムの保守・運用を行う事業者において、特定個人情報を順次消去する。 ・帳票については、本市の規定に基づき、保管・管理を適切に行い、廃棄時にはシュレッダー等による裁断又は焼却処理を行う。 ＜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。	事前	
令和7年1月20日	Ⅳ　その他のリスク対策 1．監査 ②監査　具体的な内容	＜内部監査＞ ・総務企画局の情報セキュリティを所管する部署において監査計画を策定し、情報統括監理者（CIO）の責任において定期的に監査を実施する。 ・監査の結果については、事務を所管する局の長（情報セキュリティ責任者）に通知し、改善のための措置を検討・実施する。 ＜外部監査＞ ・情報統括監理者（CIO）の責任において情報セキュリティ監査人（専門的技術を持った法人）に委託することにより実施している情報セキュリティ監査の中で、特定個人情報ファイルの取扱いの適正性についても併せて監査を実施する。 ・監査の結果については、事務を所管する局の長（情報セキュリティ責任者）に通知し、改善のための措置を検討・実施する。 ＜中間サーバー・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。	＜外部監査＞ ・情報統括監理者（CIO）の責任において情報セキュリティ監査人（専門的技術を持った法人）に委託することにより実施している情報セキュリティ監査の中で、特定個人情報ファイルの取扱いの適正性についても併せて監査を実施する。 ・監査の結果については、事務を所管する局の長（情報セキュリティ責任者）に通知し、改善のための措置を検討・実施する。 ＜中間サーバー・プラットフォームにおける措置＞ ・運用規則等に基づき、中間サーバー・プラットフォームについて、定期的に監査を行うこととしている。 ＜ガバメントクラウドにおける措置＞ ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、ISMAPにおいて、クラウドサービス事業者は定期的にISMAP監査機関リストに登録された監査機関による監査を行うこととしている。	事前	

変更日	項目	変更前の記載	変更後の記載	提出時期	提出時期に係る説明
令和7年1月20日	Ⅳ　その他のリスク対策 2. 従業者に対する教育・啓発	右記を追記	・本市で発生した特定個人情報に関する重大事故の再発防止の観点から、保護責任者に対して、特定個人情報の安全管理措置（特に、人的及び組織的安全管理措置）に関する研修を実施する。また、研修未受講の事務担当者に対し保護責任者から受講を促す。	事前	
令和7年1月20日	Ⅳ　その他のリスク対策　3. その他のリスク対策	右記を追記	＜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。	事前	
令和7年1月20日	Ⅴ　開示請求、問合せ　1. 特定個人情報の開示・訂正・利用停止請求　①請求先	・総務企画局コンプライアンス・行政情報管理部行政情報課（情報公開担当）	・総務企画局コンプライアンス推進・行政情報管理部行政情報課（情報公開担当）	事後	