変更箇所別添

変更日	項目	変更前の記載	変更後の記載
	Ⅰ基本情報 1．特定個人情報ファイルを取り扱う事務 ②事務の概要	新型インフルエンザ等対策特別措置法，新型インフルエンザ等対策特別措置法施行令及び行政手続における特定の個人を識別するための番号の利用等に関する法律（以下，「番号法」という）に基づき，宇都宮市（以下，「本市」という）が，新型インフルエンザ等が発生した場合に，特定接種や予防接種の実施，予診票の発行等を行う。 ①　特定接種及び予防接種の実施 ②　特定接種及び予防接種の記録の作成 ③　特定接種及び予防接種の実費の徴収 ④　情報提供ネットワークシステムを利用した予防接種記録の照会 ⑤　情報提供ネットワークシステムを利用した予防接種記録の提供 ⑥　予防接種実施後の接種記録等を登録・管理及び他市区町村へ接種記録の照会・提供 ⑦　予防接種実施後の接種者からの申請に基づく新型コロナウイルス感染症予防接種証明書の交付	＜定期予防接種に関する事務＞ 予防接種法，予防接種法施行令，予防接種法施行規則，予防接種実施規則，定期接種実施要領，宇都宮市予防接種実施要領，行政手続における特定の個人を識別するための番号の利用等に関する法律（以下，「番号法」という。）及び公的給付の支給等の迅速かつ確実な実施のための預貯金口座の登録等に関する法律に基づき，宇都宮市（以下，「本市」という。）が，定期予防接種を行う。また，予防接種の記録の作成，未接種者への積極的勧奨，高齢者の予防接種においては市民税の課税状況に応じた実費の徴収，予防接種による健康被害者に対する給付金の支給を行う。 ①　定期予防接種の実施 ②　定期予防接種の記録の作成 ③　定期予防接種の積極的勧奨 ④　定期予防接種の実費の徴収 ⑤　高齢者の予防接種における自己負担免除申請書の受理（市民税の非課税世帯・生活保護受給者・中国残留邦人等支援法に基づく支援給付の支給決定を受けている方への無料券の発行） ⑥　予防接種による健康被害者に関する請求の受理，給付金の支給 ⑦　情報提供ネットワークシステムを利用した地方税関係情報及び公的給付支給等口座登録簿関係情報の照会 ⑧　情報提供ネットワークを利用した定期予防接種の記録の提供 ＜新型インフルエンザ等対策特別措置法による予防接種の実施に関する事務＞ 新型インフルエンザ等対策特別措置法，新型インフルエンザ等対策特別措置法施行令及び行政手続における特定の個人を識別するための番号の利用等に関する法律（以下，「番号法」という）に基づき，宇都宮市（以下，「本市」という）が，新型インフルエンザ等が発生した場合に，特定接種や予防接種の実施，予診票の発行等を行う。 ①　特定接種及び予防接種の実施 ②　特定接種及び予防接種の記録の作成 ③　特定接種及び予防接種の実費の徴収 ④　情報提供ネットワークシステムを利用した予防接種記録の照会 ⑤　情報提供ネットワークシステムを利用した予防接種記録の提供 ⑥　予防接種実施後の接種記録等を登録・管理及び他市区町村へ接種記録の照会・提供 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務＞ 本市は、情報連携のため、予診情報・予防接種記録管理／請求支払システムへ本事務に係る対象者の個人番号を含む対象者情報、予診票情報及び接種記録の紐付け及び登録を行う。 住民は、マイナポータルを介して予診票情報の入力並びに接種記録及び通知の取得/閲覧が可能となる。 住民が予防接種時に、従来の紙の予診票に代えて、タブレットに搭載された医療機関用アプリ等においてマイナンバーカードを用いることにより、医療機関は住民が事前に入力した予診票情報、接種記録の取得/閲覧/入力が可能となる。 本市は、医療機関から入力された予診票情報、接種記録の取得及び住民への通知が可能となる。
	Ⅰ基本情報 2．特定個人情報ファイルを取り扱う事務において使用するシステム5	①システムの名称 ワクチン接種記録システム（VRS） ②システムの機能 ・令和６年９月３０日時点における新型コロナワクチン臨時接種記録等の個人情報の保管	①システムの名称 予診情報・予防接種記録管理／請求支払システム ②システムの機能 ①予防接種関連データの登録機能 本市区町村は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診票項目、接種勧奨における通知文言等の予防接種関連データを予診情報・予防接種記録管理／請求支払システムへ登録する。 ②情報登録機能及びPMHキー採番依頼機能等 予診情報・予防接種記録管理／請求支払システムは、本市区町村で管理している個人番号、対象者情報、予診票情報及び接種記録を予診情報・予防接種記録管理／請求支払システムに登録する。また、Public Medical Hubを経由して医療情報基盤・診療報酬審査支払機構（以下、「DX審査支払機構」という。）の医療保険者等向け中間サーバーと連動し、PMHキーを自動採番する。すでにPMHキーが採番済みの個人番号であれば、採番は行わずに既存のPMHキーを利用する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 予診情報・予防接種記録管理／請求支払システムは、マイナポータルからの予診情報・予防接種記録管理／請求支払システム初回利用時に、マイナポータル上で生成されたPMH仮名識別子をPMHキーと紐付けて予診情報・予防接種記録管理／請求支払システムに格納して保管する。 ・仮名識別子を利用した情報入力/提供機能 予防接種の対象者は、マイナポータルへログインしてマイナンバーカードの電子証明書のシリアル番号に紐付くPMH仮名識別子を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く接種記録・通知をマイナポータルへ提供する。また、マイナポータルへログインして予診票の入力画面から情報を入力することにより、予診情報・予防接種記録管理／請求支払システムはPMH仮名識別子からPMHキーを特定し、PMHキーに紐付く予診票情報を登録する。 ④情報連携機能（医療機関用アプリ等） ・本人確認情報の格納機能 予防接種対象者が、顔認証端末又はマイナ資格確認アプリを利用してマイナンバーカードで認証及び同意することにより、オンライン資格確認等システムを経由してPublic Medical Hubに本人確認情報が格納される。 ・本人確認情報を利用した情報入力/提供機能 医療機関用アプリ等は、予診情報・予防接種記録管理／請求支払システムへ本人確認情報を利用した照会を行う。予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubから本人確認情報を取得し、本人確認情報に紐付く予防接種対象者番号をキーに予診票情報を医療機関用アプリ等に提供する。また、医療機関が接種記録の入力画面から情報を入力することにより、予診情報・予防接種記録管理／請求支払システムは予防接種対象者番号からPMHキーを特定し、PMHキーに紐付く接種記録を登録する。 ⑤情報連携機能（履歴照会回答システム） ・識別子の格納機能 予診情報・予防接種記録管理／請求支払システムは接種記録等の情報を予防接種DBに連携し、予防接種DBにおいて予防接種の有効性・安全性等の調査・研究を行う。予診情報・予防接種記録管理／請求支払システムから履歴照会回答システムにPMHキーを連携し、履歴照会回答システムはオ

			ンライン資格確認等システムから被保険者番号等を取得し、履歴照会回答システム上で生成したID5をPMHキーと紐づけて予診情報・予防接種記録管理／請求支払システムに連携する。
	（別添1）事務内容 （備考）	追加	①特定個人情報の登録・管理 ・本市区町村は、健康管理システムからの情報連携又は予診情報・予防接種記録管理／請求支払システム画面への直接入力により、予診情報・予防接種記録管理／請求支払システムにおいて対象者の個人番号を含む対象者情報の登録を行う。（LGWAN回線等経由） ・本市区町村は予診情報・予防接種記録管理／請求支払システムから接種記録等、必要な情報を自動連携またはダウンロードし、健康管理システム等への取込を行う。 ・予診情報・予防接種記録管理／請求支払システムへ登録された個人情報へのアクセスは適切に制御される。 ②PMHキー採番 ・予診情報・予防接種記録管理／請求支払システムは、Public Medical Hubに対して個人番号を連携することで、オンライン資格確認等システムと予診情報・予防接種記録管理／請求支払システムが連動するためのPMHキーの採番処理を依頼する。 ・Public Medical Hubは、医療保険者等向け中間サーバーを経由しPMHキーを採番して予診情報・予防接種記録管理／請求支払システムに回答する。 ・医療保険者等向け中間サーバーは、PMHキーと個人番号を紐付けて、PMHキーと紐付番号をオンライン資格確認等システムへ連携する。 ・オンライン資格確認等システムは、紐付番号をキーに仮名識別子とPMHキーを紐付けて、マイナポータルに連携する。 ・マイナポータルは、新たにPMH用の仮名識別子（PMH仮名識別子）を生成し、シリアル番号、仮名識別子、PMHキーと紐付けて、予診情報・予防接種記録管理／請求支払システムに連携する。 （連携後、マイナポータル上からPMHキーは削除される。）以降、③④⑤⑥が可能となる。 ③マイナポータルへの通知 ・予診情報・予防接種記録管理／請求支払システムからマイナポータル経由で住民向けの通知を行うため、本市区町村は予診情報・予防接種記録管理／請求支払システムを利用してマイナポータルに識別子（PMH仮名識別子）と通知情報を登録する。 ④マイナポータルからの入力・取得（予診票・接種記録） ・住民は、マイナポータル経由で予診情報・予防接種記録管理／請求支払システムへの予診票の事前入力や、予診情報・予防接種記録管理／請求支払システムから接種記録や通知情報を閲覧/取得する。 ⑤医療機関用アプリ等からの入力・取得（予診票・接種記録） ・医療機関が医療機関用アプリ等を利用し、接種時に住民からマイナンバーカードによる本人確認を経て、事前入力された予診票及び接種記録の閲覧/取得/入力を行う。 ⑥ID5取得 ・予防接種DBへの接種記録等の連携時に個人を特定する識別子情報として、予診情報・予防接種記録管理／請求支払システムが履歴照会回答システム経由でID5を取得する。
	Ⅱ特定個人情報ファイルの概要 6．特定個人情報の保管・削除 ①保管場所	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜自治体中間サーバー・プラットフォームにおける措置＞ ①自治体中間サーバー・プラットフォームはデータセンターに設置している。データセンターへの入館，及びサーバー室への入室を行う際は，警備員などにより顔写真入りの身分証明書と事前申請との照合を行う。 ②特定個人情報は，サーバー室に設置されたクラウドサービス事業者が保有・管理する環境に構築する自治体中間サーバーのデータベース内に保存され，バックアップもデータベース上に保存される。 ＜ワクチン接種記録システム（ＶＲＳ）における追加措置＞ 　ワクチン接種記録システム(VRS)は，特定個人情報の適切な取扱いに関するガイドライン，政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており，情報セキュリティの国際規格を取得しているクラウドサービスを利用している。なお，以下のとおりのセキュリティ対策を講じている。 　・論理的に区分された当市区町村の領域にデータを保管する。 　・当該領域のデータは，暗号化処理をする。 　・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 　・国、都道府県からは特定個人情報にアクセスできないように制御している。 　・日本国内にデータセンターが存在するクラウドサービスを利用している。	＜ガバメントクラウドにおける措置＞ ①サーバ等はクラウド事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウド事業者が実施する。なお、クラウド事業者はISMAPのリストに登録されたクラウドサービス事業者であり、セキュリティ管理策が適切に実施されているほか、次を満たすものとする。 ・ISO/IEC27017、ISO/IEC27018 の認証を受けていること。 ・日本国内でのデータ保管を条件としていること。 ②特定個人情報は、クラウド事業者が管理するデータセンター内のデータベースに保存され、バックアップも日本国内に設置された複数のデータセンターのうち本番環境とは別のデータセンター内に保存される。 ＜自治体中間サーバー・プラットフォームにおける措置＞ ①自治体中間サーバー・プラットフォームは政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 　・　ISO/IEC27017、ISO/IEC27018 の認証を受けている。 　・　日本国内でデータを保管している。 ②特定個人情報は，クラウドサービス事業者が保有・管理する環境に構築する自治体中間サーバーのデータベース内に保存され，バックアップもデータベース上に保存される。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用している。なお、以下のとおりセキュリティ対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・日本国内にデータセンターが存在するクラウドサービスを利用している。

	Ⅱ特定個人情報ファイルの概要 6．特定個人情報の保管・削除 ③消去方法	＜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。 ＜ワクチン接種記録システム（ＶＲＳ）における追加措置＞ ・自機関の領域に保管されたデータは，他機関から消去できない。 ※クラウドサービスは，IaaSを利用し，クラウドサービス事業者からはデータにアクセスできないため， 消去することができない。	＜ガバメントクラウドにおける措置＞ ①特定個人情報の消去は地方公共団体からの操作によって実施される。地方公共団体の業務データは国及びガバメントクラウドのクラウド事業者にはアクセスが制御されているため特定個人情報を消去することはない。 ②クラウド事業者がHDDやSSDなどの記録装置等を障害やメンテナンス等により交換する際にデータの復元がなされないよう、クラウド事業者において、NIST 800-88、ISO/IEC27001等にしたがって確実にデータを消去する。 ③既存システムについては、地方公共団体が委託した開発事業者が既存の環境からガバメントクラウドへ移行することになるが、移行に際しては、データ抽出及びクラウド環境へのデータ投入、並びに利用しなくなった環境の破棄等を実施する。 ＜中間サーバ・プラットフォームにおける措置＞ ・　特定個人情報の消去は地方公共団体からの操作によって実施されるため，通常，中間サーバ・プラットフォームの保守・運用を行う事業者が特定個人情報を消去することはない。 ・　クラウドサービス事業者が保有・管理する環境において、障害やメンテナンス等によりディスクやハード等を交換する際は、クラウドサービス事業者において、政府情報システムのためのセキュリティ評価制度（ISMAP）に準拠したデータの暗号化消去及び物理的破壊を行う。さらに、第三者の監査機関が定期的に発行するレポートにより、クラウドサービス事業者において、確実にデータの暗号化消去及び物理的破壊が行われていることを確認する。 ・中間サーバー・プラットフォームの移行の際は、地方公共団体情報システム機構及び中間サーバー・プラットフォームの事業者において、保存された情報が読み出しできないよう、データセンターに設置しているディスクやハード等を物理的破壊により完全に消去する。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務> ・本市の領域に保管されたデータのみ、予診情報・予防接種記録管理／請求支払システムを用いて消去することができる。 ・本市区町村の領域に保管されたデータは、他機関から消去できない。 ※クラウドサービスは、IaaSを利用し、クラウドサービス事業者からはデータにアクセスできないため、 消去することができない。 ・不要となった特定個人情報は、削除用データの連携又は運用保守事業者に依頼して消去する。 ・不要となったバックアップファイルは、ストレージに適用されたライフサイクルルールに基づき、保管されたログ情報については、各オブジェクトの保管日（作成日）を起点として3年が経過した時点で、自動的に削除される。
	（別添2）特定個人情報ファイル記録項目 （備考）	予防接種情報ファイル 項目名 1　対象者 2　対象者宛名番号 3　対象者個人番号（※１） 4　対象者情報 5　氏名 6　住所 7　電話番号 8　生年月日 9　性別 10　続柄 11　受診日（接種日） 12　受診年度（接種年度） 13　接種種別 14　接種回数 15　接種判定 16　接種日年齢 17　年度末年齢 18　基準日年齢 19　実施医療機関 20　問診医 21　接種医 22　接種番号 23　実施場所 24　メーカー 25　ロットナンバー 26　接種量 27　未接種理由 28　特記事項 29　予診フラグ 30　更新日 31　更新時刻 32　更新者職員番号 ※　個人番号は，宛名番号と紐づけて共通管理システムの情報から参照する。	予防接種情報ファイル 項目名 1　対象者 2　対象者宛名番号 3　対象者個人番号（※１） 4　対象者情報 5　氏名 6　住所 7　電話番号 8　生年月日 9　性別 10　続柄 11　受診日（接種日） 12　受診年度（接種年度） 13　接種種別 14　接種回数 15　接種判定 16　接種日年齢 17　年度末年齢 18　基準日年齢 19　実施医療機関 20　問診医 21　接種医 22　接種番号 23　実施場所 24　メーカー 25　ロットナンバー 26　接種量 27　未接種理由 28　特記事項 29　予診フラグ 30　更新日 31　更新時刻 32　更新者職員番号 ※　個人番号は，宛名番号と紐づけて共通管理システムの情報から参照する。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加の記録項目> (1)対象者情報 ・個人番号 ・PMHキー ・PMH仮名識別子 ・基本５情報（カナ・氏名・住所・生年月日・性別） ・保護者氏名 ・自治体コード ・自治体業務ID ・連携ファイル名

			・連携日時 ・連携処理ステータス/エラー内容 ・制御フラグ（リカバリー/不開示/閲覧停止） ・変更区分 ・消除の異動日 ・その他管理番号・ID等（予防接種対象者番号） ・その他区分等（接種対象者区分/減免区分） (2)ユーザー情報 ・機関マスタID ・機関ユーザーID ・メールアドレス ・ユーザー氏名 ・ユーザー区分 ・ユーザー権限ID ・個人番号閲覧可能フラグ ・ユーザー削除フラグ (3)予診票情報 ・項目ID ・管理ID ・更新日時 ・回答ID ・回答内容 ・回答処理ステータス ・回答日時 ・接種不可フラグ ・予防接種設定ID ・予防接種管理ID ・組み合わせ番号 ・強制失効日 ・勧奨情報（ルールID、勧奨日） (4)予防接種記録情報 ・予防接種記録ID ・予防接種管理ID ・接種日 ・接種同意フラグ ・医療機関コード ・医師名 ・実施場所 ・実施区分 ・接種区分 ・GTINコード ・ワクチンメーカー名 ・ワクチン名（ワクチン一般名/ワクチン通称/ワクチン販売名） ・ロット番号 ・接種量 ・接種部位 ・接種方法 ・ワクチン有効期限 ・要注意接種フラグ ・特別の事情 ・海外接種フラグ ・更新日時
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 3.特定個人情報の使用 リスク2：権限のない者（元職員，アクセス権限のない職員等）によって不正に使用されるリスク ユーザー認証の管理 具体的な管理方法	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 1　ユーザーの認証方法 ・　業務端末から保健情報管理システムを利用する際，ユーザーＩＤ（職員番号）と生体認証（指静脈）による二要素認証を行い，認証後は利用機能の認可機能により，システム上で利用可能な機能を制限することで，利用を許可された者以外の不正利用が行えないよう制限している。 ・　システムの利用できる端末を管理・制御することにより，不要な端末からの利用ができないような制限を実施している。 2　なりすましが行われないための対策 生体認証（指静脈）によりシステムへログインすることで，なりすましによる利用を完全に排除している。	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 1　ユーザーの認証方法 ・　業務端末から保健情報管理システムを利用する際，ユーザーＩＤ（職員番号）と生体認証（指静脈）による二要素認証を行い，認証後は利用機能の認可機能により，システム上で利用可能な機能を制限することで，利用を許可された者以外の不正利用が行えないよう制限している。 ・　システムの利用できる端末を管理・制御することにより，不要な端末からの利用ができないような制限を実施している。 2　なりすましが行われないための対策 生体認証（指静脈）によりシステムへログインすることで，なりすましによる利用を完全に排除している。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ 権限のない者に不正使用されないよう、以下の対策を講じている。 ・本市は、予診情報・予防接種記録管理／請求支払システムのアクセス権限を管理する管理者を定める。 ・予診情報・予防接種記録管理／請求支払システムのログインはユーザID・パスワードで行う。 ・予診情報・予防接種記録管理／請求支払システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・端末は、限定された者しかログインできない。 ・予診情報・予防接種記録管理／請求支払システムにおける特定個人情報へのアクセスは、LGWAN回線又はその他の閉域網回線経由の接続のみ認められるよう制御している。 ・既存システム（各業務システム）から予診情報・予防接種記録管理／請求支払システムへの連携は、アクセス権限を持つ者のみ実施が可能となっている。
	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	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 1　発効管理 所属長の許可を得た上で経営管理課に依頼を行い、経営管	宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 1　発効管理 所属長の許可を得た上で経営管理課にてその必要性を十分確認した上で必要なアクセス権限を個人単位で付与している。

	リスク対策 3.特定個人情報の使用 リスク2：権限のない者（元職員，アクセス権限のない職員等）によって不正に使用されるリスク アクセス権限の発行・失効の管理 具体的な管理方法	所属長の許可を得た上で経営管理課に依頼を行い，経営管理課にてその必要性を十分確認した 上で必要なアクセス権限を個人単位で付与している。 やむを得ず、複数の職員が共有するID（以下「共用ID」という。）を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、所属長が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動／退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。 2　失効管理 ・　職員等は，業務上必要がなくなった場合は，ユーザー登録を抹消するようにしている。 ・　利用者抹消（異動，退職等）に伴うユーザーIDの取扱いについて，人事課から随時情報提供を 受けて，確実な失効を行っている。 ・　大量異動が行われる年度初めに，全てのユーザーIDのチェックを行い，不要なユーザーIDの失効を行っている。	上で必要なアクセス権限を個人単位で付与している。 やむを得ず、複数の職員が共有するID（以下「共用ID」という。）を発行する必要がある場合は、当該IDを使用する職員・端末を特定し、所属長が把握した上で、パスワードを厳重に管理する運用を徹底し、必要最小限に発行する。なお、共用IDを使用する職員及び端末について、異動／退職等のイベントが発生したタイミングで確認し、当該事由が生じた際は速やかに把握している内容を更新する。 2　失効管理 ・　職員等は，業務上必要がなくなった場合は，ユーザー登録を抹消するようにしている。 ・　利用者抹消（異動，退職等）に伴うユーザーIDの取扱いについて，人事課から随時情報提供を 受けて，確実な失効を行っている。 ・　大量異動が行われる年度初めに，全てのユーザーIDのチェックを行い，不要なユーザーIDの失効を行っている。 ＜予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置＞ ・予診情報・予防接種記録管理／請求支払システムへのログイン用のユーザIDは、管理者に対してユーザ登録を事前申請した者に限定して発行される。 ・管理者は、アクセス権限の管理表を作成し、申請者に対して管理表に基づき適切なアクセス権限を付与する。 ・本市において、人事異動や退職等があった際は、異動情報に基づき、不要となったアクセス権限を管理し、失効させる。
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 4.特定個人情報ファイルの取扱いの委託 委託契約書中の特定個人情報ファイルの取り扱いに関する規定 既定の内容	個人情報の取扱いについては，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。 ①　契約終了又は解除された後においても秘密保持すること。 ②　従事者に対して宇都宮市個人情報保護条例で定める罰則の教示を行うこと。 ③　個人情報の収集の制限と適正管理を行うこと。 ④　本市の許可なき個人情報の複写及び持ち出しの禁止 ⑤　目的外の使用と第三者への提供の禁止 ⑥　個人情報の返還と廃棄に関すること。 ⑦　事故発生時の速やかな報告 ⑧　契約事項の違反による損害賠償の担保	個人情報の取扱いについては，宇都宮市個人情報保護条例に則り，個人情報の保護の重要性を認識し，個人の権利利益を侵害することのないよう適正に取り扱うように委託契約書において特記事項として定めている。 ①　契約終了又は解除された後においても秘密保持すること。 ②　従事者に対して宇都宮市個人情報保護条例で定める罰則の教示を行うこと。 ③　個人情報の収集の制限と適正管理を行うこと。 ④　本市の許可なき個人情報の複写及び持ち出しの禁止 ⑤　目的外の使用と第三者への提供の禁止 ⑥　個人情報の返還と廃棄に関すること。 ⑦　事故発生時の速やかな報告 ⑧　契約事項の違反による損害賠償の担保 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 栃木県国保連合会及び国保中央会は特定個人情報の適正な取扱いに関するガイドライン（行政機関等編）を遵守し、委託契約書に以下の規定を設ける。 ・秘密保持義務 ・事業所内からの特定個人情報の持ち出しの禁止 ・特定個人情報の目的外利用の禁止 ・特定個人情報ファイルの閲覧者・更新者の制限 ・特定個人情報ファイルの取扱いの記録 ・特定個人情報の提供ルール/消去ルール ・再委託における条件 ・再委託先による特定個人情報ファイルの適切な取扱いの確保 ・漏えい等事案が発生した場合の委託先の責任 ・委託契約終了後の特定個人情報の消去 ・特定個人情報を取り扱う従業者の明確化 ・従業者に対する監督・教育 ・契約内容の遵守状況についての報告 ・実地の監査、調査等に関する事項
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去 リスク1：特定個人情報の漏洩・滅失・毀損リスク ⑤物理的リスク 具体的な対策の内容	1　本市における措置 宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 サーバー設置場所 サーバーを設置する情報システム室から外部に通ずるドアは最小限とし，ICカードと生体認証等にて立入を制限の上，入退室管理システムにより24時間入退室を監視している。 端末設置場所 ①　職員等は，パソコン等の端末について，第三者に使用されること又は情報システム管理者の許可なく情報を閲覧されることがないように，離席時の端末のロック等，適切な措置を講じている。 ②　業務終了後は，パソコン等の端末を施錠できる場所へ保管し又は事務所を施錠することで，盗難を防止している。 記録媒体・紙媒体の保管場所 ①　情報を記録した記録媒体や情報が印刷された文書等について，第三者に使用されること又は情報システム管理者の許可なく情報を閲覧されることがないように容易に閲覧されない場所（施錠可能な事務所内倉庫や保管庫）へ保管している。 ②　遠隔地保管を行うバックアップ用ＬＴＯメディアは，経営管理課が一括管理しており，所管課との受渡しは記録簿にて管理を行っている。 2　中間サーバー・プラットフォームにおける措置 中間サーバー・プラットフォーム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	1　本市における措置 宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 サーバー設置場所 サーバーを設置する情報システム室から外部に通ずるドアは最小限とし，ICカードと生体認証等にて立入を制限の上，入退室管理システムにより24時間入退室を監視している。 端末設置場所 ①　職員等は，パソコン等の端末について，第三者に使用されること又は情報システム管理者の許可なく情報を閲覧されることがないように，離席時の端末のロック等，適切な措置を講じている。 ②　業務終了後は，パソコン等の端末を施錠できる場所へ保管し又は事務所を施錠することで，盗難を防止している。 記録媒体・紙媒体の保管場所 ①　情報を記録した記録媒体や情報が印刷された文書等について，第三者に使用されること又は情報システム管理者の許可なく情報を閲覧されることがないように容易に閲覧されない場所（施錠可能な事務所内倉庫や保管庫）へ保管している。 ②　遠隔地保管を行うバックアップ用ＬＴＯメディアは，経営管理課が一括管理しており，所管課との受渡しは記録簿にて管理を行っている。 2　中間サーバー・プラットフォームにおける措置 中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、設置場所のセキュリティ対策はクラウドサービス事業者が実施する。なお、クラウドサービス事業者は、セキュリティ管理策が適切に実施されているほか、次を満たしている。 ・　ISO/IEC27017、ISO/IEC27018 の認証を受けている。 ・　日本国内でデータを保管している。 ＜ガバメントクラウドにおける措置＞

		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している。 ＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 ＜ワクチン接種記録システム(VRS)における措置＞ ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための 統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウド サービスを利用しているため、特定個人情報の適切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。 ・サーバー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。	＜ガバメントクラウドにおける措置＞ ①ガバメントクラウドについては政府情報システムのセキュリティ制度（ISMAP）のリストに登録されたクラウドサービスから調達することとしており、システムのサーバー等は、クラウド事業者が保有・管理する環境に構築し、その環境には認可された者だけがアクセスできるよう適切な入退室管理策を行っている。 ②事前に許可されていない装置等に関しては、外部に持出できないこととしている。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置> 予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める物理的対策を満たしている。 主に以下の物理的対策を講じている。 ・サーバ設置場所等への入退室記録管理、施錠管理 ・日本国内にデータセンターが存在するクラウドサービスの利用
	Ⅲ　特定個人情報ファイルの取扱いプロセスにおけるリスク対策 7.特定個人情報の保管・消去 リスク1：特定個人情報の漏洩・滅失・毀損リスク ⑥技術的リスク 具体的な対策の内容	1　本市における措置 宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ウイルス対策 ①　職員等は記録媒体を使う場合，コンピューターウイルス等の感染を防止するために，本市が管理している記録媒体のみを利用している。 ②　サーバー及びパソコン等の端末に，コンピューターウイルス等の不正プログラム対策ソフトウェアを常駐させている。 ③　不正プログラム対策ソフトウェアを導入し，定期的に当該ソフトウェア及びパターンファイルの更新を実施し，常に最新の状態を保っている。 不正アクセス対策 ①　保健情報管理システムは，外部のインターネットと物理的に接続していない。 ②　情報システム管理者はセキュリティに関する事案を検知するため，情報システムを常時監視し，障害が起きた際にも速やかに対応できるようにしている。 2　中間サーバー・プラットフォームにおける措置 ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネット ワークを効率的かつ包括的に保護する装置）等を導入し，アクセス制限，侵入検知及び侵入防止を行うとともに，ログの解析を行っている。 ②中間サーバー・プラットフォームでは，ウイルス対策ソフトを導入し，パターンファイルの更新を行っている。 ③導入しているＯＳ及びミドルウェアについて，必要に応じてセキュリティパッチの適用を行っている。 3　ワクチン接種記録システム(VRS)における措置 ワクチン接種記録システム(VRS)は、特定個人情報の適切な取扱いに関するガイドライン、政府機関等の情報セキュリティ対策のための統一基準群に準拠した開発・運用がされており、情報セキュリティの国際規格を取得しているクラウドサービスを利用しているため、特定個人情報の適切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の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国、都道府県からは特定個人情報にアクセスできないように制御している。 ・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。 ・LG-WAN端末とワクチン接種記録システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ＜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	1　本市における措置 宇都宮市情報セキュリティ対策基準に基づき，以下の対策を行っている。 ウイルス対策 ①　職員等は記録媒体を使う場合，コンピューターウイルス等の感染を防止するために，本市が管理している記録媒体のみを利用している。 ②　サーバー及びパソコン等の端末に，コンピューターウイルス等の不正プログラム対策ソフトウェアを常駐させている。 ③　不正プログラム対策ソフトウェアを導入し，定期的に当該ソフトウェア及びパターンファイルの更新を実施し，常に最新の状態を保っている。 不正アクセス対策 ①　保健情報管理システムは，外部のインターネットと物理的に接続していない。 ②　情報システム管理者はセキュリティに関する事案を検知するため，情報システムを常時監視し，障害が起きた際にも速やかに対応できるようにしている。 2　中間サーバー・プラットフォームにおける措置 ①中間サーバー・プラットフォームではUTM（コンピュータウイルスやハッキングなどの脅威からネット ワークを効率的かつ包括的に保護する装置）等を導入し，アクセス制限，侵入検知及び侵入防止を行うとともに，ログの解析を行っている。 ②中間サーバー・プラットフォームでは，ウイルス対策ソフトを導入し，パターンファイルの更新を行っている。 ③導入しているＯＳ及びミドルウェアについて，必要に応じてセキュリティパッチの適用を行っている。 ④　中間サーバー・プラットフォームは、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されたクラウドサービス事業者が保有・管理する環境に設置し、インターネットとは切り離された閉域ネットワーク環境に構築する。 ⑤　中間サーバーのデータベースに保存される特定個人情報は、中間サーバー・プラットフォームの事業者及びクラウドサービス事業者がアクセスできないよう制御を講じる。 ⑥　中間サーバーと団体についてはVPN等の技術を利用し、団体ごとに通信回線を分離するとともに、通信を暗号化することで安全性を確保している。 ⑦　中間サーバー・プラットフォームの移行の際は、中間サーバー・プラットフォームの事業者において、移行するデータを暗号化した上で、インターネットを経由しない専用回線を使用し、VPN等の技術を利用して通信を暗号化することでデータ移行を行う。 ＜ガバメントクラウドにおける措置＞ ①国及びクラウド事業者は利用者のデータにアクセスしない契約等となっている。 ②地方公共団体が委託したASP(「地方公共団体情報システムのガバメントクラウドの利用に関する基準【第1.0版】」（令和４年１０月　デジタル庁。以下「利用基準」という。）に規定する「ASP」をいう。以下同じ。)又はガバメントクラウド運用管理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。 <予診情報・予防接種記録管理／請求支払システムを活用した情報連携に係る予防接種事務における追加措置>

		理補助者（利用基準に規定する「ガバメントクラウド運用管理補助者」をいう。以下同じ。）は、ガバメントクラウドが提供するマネージドサービスにより、ネットワークアクティビティ、データアクセスパターン、アカウント動作等について継続的にモニタリングを行うとともに、ログ管理を行う。 ③クラウド事業者は、ガバメントクラウドに対するセキュリティの脅威に対し、脅威検出やDDos対策を24時間365日講じる。 ④クラウド事業者は、ガバメントクラウドに対し、ウイルス対策ソフトを導入し、パターンファイルの更新を行う。 ⑤地方公共団体が委託したASP又はガバメントクラウド運用管理補助者は、導入しているOS及びミドルウエアについて、必要に応じてセキュリティパッチの適用を行う。 ⑥ガバメントクラウドの特定個人情報を保有するシステムを構築する環境は、インターネットとは切り離された閉域ネットワークで構成する。 ⑦地方公共団体やASP又はガバメントクラウド運用管理補助者の運用保守地点からガバメントクラウドへの接続については、閉域ネットワークで構成する。 ⑧地方公共団体が管理する業務データは、国及びクラウド事業者がアクセスできないよう制御を講じる。	予診情報・予防接種記録管理／請求支払システムは、特定個人情報の適正な取扱いに関するガイドライン、政府機関等のサイバーセキュリティ対策のための統一基準群に準拠した開発・運用がされており、政府情報システムのためのセキュリティ評価制度（ISMAP）において登録されたサービスか、ISO/IEC27017:2015又はCSマーク・ゴールドの認証を取得している者で、かつ、「政府情報システムにおけるクラウドサービスの利用に係る基本方針」等による各種条件を満たすクラウドサービスを利用しているため、特定個人情報の適正な取扱いに関するガイドラインで求める技術的対策を満たしている。 主に以下の技術的対策を講じている。 ・予診情報・予防接種記録管理／請求支払システムは論理的に区分された当市区町村の領域にデータを保管する。 ・当該領域のデータは、暗号化処理をする。 ・個人番号が含まれる領域はインターネットからアクセスできないように制御している。 ・国保中央会や医療機関及び住民からは特定個人情報にアクセスできないように制御している。 ・当該システムへの不正アクセスの防止のため、予診情報・予防接種記録管理／請求支払システムは外部からの侵入検知・通知機能を備えている。 ・本市の端末と予診情報・予防接種記録管理／請求支払システムとの通信は暗号化を行うことにより、通信内容の秘匿及び盗聴防止の対応をしている。 ・本市の端末と予診情報・予防接種記録管理／請求支払システムとの通信はLGWAN回線又は閉域網VPN等に限定されている。 ・クラウドマネージドサービスを利用する場合においても、パブリッククラウド事業者は特定個人情報にはアクセスできない。 ・バックアップは地理的に十分に離れた拠点に保管することで、大規模なシステム障害や震災などの 発生によりデータが破損・消失しても、バックアップからデータを復元できるようにする。