資料２－２

特定個人情報保護評価書の特定個人情報保護評価指針への適合性・妥当性の審査

評価書名
全国健康保険協会における健康保険の資格適用・保険給付・保健事業・相談・問い合わせに関する事務　全項目評価書

評価実施機関名
全国健康保険協会

提出日
令和６年２月20日

概要説明日
令和６年２月21日

（目次）

全体的な事項

※ 評価実施手続に関する事項及び特定個人情報ファイルに共通する事項

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
(1)しきい値判断に誤りはないか。	—	—	—	—	問題は認められない	対象人数が30万人以上に該当するため、全項目評価を実施することは、指針に適合している。
(2)適切な実施主体が実施しているか。	—	1. 評価実施機関が複数存在し、取りまとめの評価実施機関が評価書を作成・提出する場合に、取りまとめ以外の全ての評価実施機関について記載しているか。	—	—	問題は認められない	特定個人情報ファイルは、全国健康保険協会（以下「協会」という。）が健康保険の資格適用・保険給付・保健事業・相談・問い合わせに関する事務において保有するものであることから、実施主体は適切である。
(3)公表しない部分は適切な範囲か。	—	—	—	—	問題は認められない	評価書の内容は全て公表することとしている。
(4)適切な時期に実施しているか。	—	—	—	—	問題は認められない	特定個人情報ファイルを取り扱うシステムの改修に伴うプログラミングの開始を、令和6年3月に予定しており、プログラミング開始前の適切な時期に評価を実施している。
(5)適切な方法で広く国民の意見を求め、得られた意見を十分考慮した上で必要な見直しを行っているか。	—	—	—	—	問題は認められない	国民への意見募集については、協会のホームページにて、30日間実施した。 なお、寄せられた意見はなかった。
(6)特定個人情報保護評価の対象となる事務の実態に基づき、特定個人情報保護評価書様式で求められる全ての項目について検討し、記載しているか。	—	—	—	—	問題は認められない	健康保険の資格適用・保険給付・保健事業・相談・問い合わせに関する事務について、求められる事項が具体的に記載されている。 なお、再実施の理由となる重要な変更については、電子申請、個人番号をキーとした被保険者検索の実施及び公金受取口座の利用が可能となることによるものであるが、当該重要な変更についても求められる事項が具体的に記載されている。
(7)記載された特定個人情報保護評価の実施を担当する部署は、特定個人情報保護評価の対象となる事務を担当し、リスクを軽減させるための措置の実施に責任を負うことができるか。	—	—	—	—	問題は認められない	健康保険の資格適用・保険給付・保健事業・相談・問い合わせに関する事務における番号制度への対応は協会本部企画部企画グループが行っており、特定個人情報保護評価の対象となる事務の実施に当たって、リスクを軽減させるための措置の実施等については、責任を負うことができる部署である。

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
(8)特定個人情報保護評価の対象となる事務の内容の記載は具体的か。当該事務における特定個人情報の流れを併せて記載しているか。	①特定個人情報ファイルを取り扱う事務やその事務において使用するシステムについて、基本情報を具体的に分かりやすく記載しているか。	2. 評価対象の事務全体の概要及びその中で特定個人情報ファイルを使用して実施する事務の内容を具体的に記載しているか。	P.3 ～ P.4	Ⅰ 1. ②	問題は認められない	健康保険の資格適用・保険給付・保健事業・相談・問い合わせに関する事務において、それぞれ特定個人情報ファイルを使用することが事務の流れに即し具体的に記載されている。 また、別添1の事務の内容において、一般被保険者等及び事業主から提出される各種届出書により個人番号を入手し、識別番号と紐付けた上で個人番号管理情報ファイルに登録すること、識別番号が記載されていない申出書を受け付けた場合は、個人番号を基に個人番号管理システムに識別番号等の資格情報を検索・照会すること等、事務において取り扱う特定個人情報の流れが事務の内容に即して具体的に記載されているほか、加入者において、課税証明書等の添付の省略が可能となる等、実現が期待されるメリット等についても具体的に記載されている。
		3. 当該システムが実現する機能の名称とその概要を具体的に記載しているか。	P.5 ～ P.7	Ⅰ 2. ②	問題は認められない	
		4. 当該システムと情報をやり取りするシステムを全て記載しているか。	P.5 ～ P.7	Ⅰ 2. ③	問題は認められない	
		5. 特定個人情報ファイルを取り扱うことが評価対象の事務を実施する上で必要であることを、事務の流れに即して具体的に説明しているか。	P.8	Ⅰ 4. ①	問題は認められない	
		6. 評価対象の事務において特定個人情報ファイルを取り扱うことにより、期待されるメリットについて幅広く具体的に記載しているか。	P.8	Ⅰ 4. ②	問題は認められない	
		7. 事務に関わる者、事務において使用するシステム、事務において取り扱う情報の流れを具体的に記載しているか。	P.9 ～ P.11	Ⅰ (別添1)	問題は認められない	
(9)特定個人情報ファイルを取り扱うプロセスにおいて特定個人情報の漏えいその他の事態を発生させるリスクを、特定個人情報保護評価の対象となる事務の実態に基づき、特定しているか。	―	―	P.36 ～ P.57	Ⅲ、Ⅳ	問題は認められない	全項目評価書に例示されている各リスクにどのように対応しているかが具体的に記載されている。

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
(10)特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 (11)記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	⑨特定個人情報ファイルの取扱いについて自己点検・監査や従業者に対する教育・啓発を行っているか。	70. 評価書に記載したとおりに運用がなされていること等について、評価の実施を担当する部署自らが、どのように自己点検するか具体的に記載しているか。	P.57	Ⅳ 1. ①	問題は認められない	自己点検については、協会の情報セキュリティ規程の対策推進計画に基づき、情報セキュリティ統括管理者が年度自己点検計画を策定するとともに、当該計画に基づき、役職員等が自己点検を実施すること、また、監査については、定期的に監査部門により、自己点検の結果を確認するとともに、指摘事項が発生した場合は、次回監査時に改善状況を確認すること等が具体的に記載されている。 従業者に対する教育・啓発については、協会の個人情報管理規程、特定個人情報管理規程及び情報セキュリティ規程に基づき、職員に対し個人情報の管理・保護及び情報セキュリティ対策に関する研修を義務付けており、新規職員採用時等に研修を実施すること、個人情報に係る情報漏えい事例について、イントラネットの掲示板を利用した情報提供を行い、同一事案の再発防止に役立てていること、また、委託業者については、外部委託契約の締結に当たり個人情報の漏えいの防止等の適切な管理のための必要な措置を講じることを義務付けていること等が具体的に記載されている。
		71. 評価書に記載したとおりに運用がなされていること等について、どのように監査するか具体的に記載しているか。	P.57	Ⅳ1. ②	問題は認められない	
		72. 特定個人情報を取り扱う従業者等に対しての教育・啓発や違反行為をした従業者等に対する措置について具体的に記載しているか。	P.57	Ⅳ 2.	問題は認められない	
		73. 国民・住民等からの意見聴取により得られた意見を踏まえて評価書のどの箇所をどのように修正したかを具体的に記載しているか。	P.59	Ⅵ 2. ⑤	問題は認められない	寄せられた意見がなかったことが記載されている。
(12)個人のプライバシー等の権利利益の保護の宣言は、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	―	―	P.1	表紙	問題は認められない	協会は、健康保険の資格適用・保険給付・保健事業・相談・問い合わせ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当たり、その取扱いが個人のプライバシー等の権利利益に影響を及ぼしかねないことを認識し、特定個人情報の漏えいその他の事態が発生す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している。

特定個人情報ファイル
（健保特定個人情報ファイル）

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
(8)特定個人情報保護評価の対象となる事務の内容の記載は具体的か。当該事務における特定個人情報の流れを併せて記載しているか。	②特定個人情報ファイルの取扱いプロセスの概要(特定個人情報の入手・使用、特定個人情報ファイルの取扱いの委託、特定個人情報の提供・移転、特定個人情報の保管・消去)について、具体的に分かりやすく記載しているか。	8. 対象となる国民・住民の特定個人情報を特定個人情報ファイルにおいて保有することが事務を実施する上で必要な理由を具体的に記載しているか。	P.12	Ⅱ 2. ③	問題は認められない	特定個人情報の使用目的として、個人番号を用いて都道府県民税又は市区町村民税の情報、収入等の情報及び公金受取口座情報を個人番号管理システム経由で情報提供ネットワークシステムに照会すること、個人番号を既存システムの識別番号と紐付けて特定個人情報ファイルから資格関係情報を検索することが具体的に記載されている。 また、特定個人情報ファイルはデータセンター内のサーバに保管・管理、申請(届)書など帳票類及び特定個人情報ファイルが収録された電子媒体は保管庫等に保管・管理し、個人番号管理システム・適用等システム及び保健事業システムに接続していない事務用PC、個人ロッカー・事務デスク内には一切保管しないよう規制していること等、特定個人情報ファイルの取扱いプロセスの概要(入手・使用、委託、提供、保管・消去)について具体的に記載されている。
		9. 主な記録項目について、保有する理由をそれぞれ具体的に記載しているか。	P.12	Ⅱ 2. ④	問題は認められない	
		10. 特定個人情報の入手に係る妥当性を具体的に記載しているか。	P.15	Ⅱ 3. ④	問題は認められない	
		11. 特定個人情報の入手の事実及び使用目的が本人に示されていることを具体的に記載しているか。	P.16	Ⅱ 3. ⑤	問題は認められない	
		12. 特定個人情報を使用する理由を具体的に記載しているか。	P.16	Ⅱ 3. ⑥	問題は認められない	
		13. 特定個人情報ファイルに記録される情報を他から入手する際の突合の内容、特定個人情報ファイルに記録された情報と他の情報との突合の方法や突合の理由を具体的に記載しているか。	P.16	Ⅱ 3. ⑧	問題は認められない	
		14. 特定個人情報を用いた統計分析を行う場合は、その内容を具体的に記載しているか。	P.16	Ⅱ 3. ⑧	該当なし	
		15. 特定個人情報を使用することにより国民の権利利益に影響を与え得る決定を行う場合は、その内容を具体的に記載しているか。	P.16	Ⅱ 3. ⑧	問題は認められない	
		16. 委託先に当該特定個人情報ファイルを取り扱わせることが必要な理由を具体的に記載しているか。	P.17～P.24	Ⅱ 4. ②	問題は認められない	
		17. 委託先を国民・住民等が確認できるか否か、確認できる場合はどのように確認できるか、確認できない場合はそのような取扱いが評価対象の事務を実施する上で必要な理由を具体的に記載しているか。	P.17～P.24	Ⅱ 4. ⑤	問題は認められない	
		18. 特定個人情報ファイルの取扱いを再委託するに当たって、どのような手続・方法によるかを具体的に記載しているか。	P.17～P.24	Ⅱ 4. ⑧	問題は認められない	
		19. 提供した特定個人情報が、提供先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.25 P.28～P.29	Ⅱ 5. ②	問題は認められない	
		20. 移転した特定個人情報が、移転先において、いかなる目的で、どのように使用されることになるかを具体的に記載しているか。	P.25	Ⅱ 5. ②	該当なし	
		21. 特定個人情報の保管場所の態様及び保管場所への立入り制限・アクセス制限について具体的に記載しているか。	P.26	Ⅱ 6. ①	問題は認められない	
		22. 特定個人情報の保管期間は妥当であるか。また、その理由を具体的に記載しているか。	P.26	Ⅱ 6. ②	問題は認められない	
		23. 保管期間を経過した特定個人情報を消去する方法を具体的に記載しているか。	P.26	Ⅱ 6. ③	問題は認められない	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
(10)特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 (11)記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	③特定個人情報の入手について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	24. 評価対象の事務を遂行する上で必要な者以外の者の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.36	Ⅲ 2. リスク1:	問題は認められない	対象者以外の情報の入手を防止するリスク対策として、本人等から特定個人情報を入手する場合は、番号法第16条(本人確認の措置)に則り本人確認を行い、本人確認後の加入者の個人番号の提供を受けること、本人がマイナポータルの自己情報取得APIを利用し、自身の健康保険の資格情報を取得し、協会の資格情報が取得できた場合に限り電子申請を可能とすること、地方公共団体情報システム機構から特定個人情報を入手する場合は、協会の照会要求に該当した機構保存本人確認情報のみ入手すること、日本年金機構から入手する場合は、協会の対象者以外の情報は提供されないこと等が具体的に記載されている。 必要な情報以外の入手を防止するリスク対策として、電子申請システムにて個人番号を含む情報を入手する場合には、Webフォームまたは指定の様式に必要事項を記載・提出いただく形とすることに加え、ホームページや記入の手引き等により不必要な情報を入力することがないよう案内すること、電子記録媒体により入手する場合には、あらかじめ定められたフォーマットを用いること、日本年金機構との専用回線による通信は、あらかじめ定めたインターフェース仕様に沿って行うこと等が具体的に記載されている。 入手した特定個人情報が不正確であるリスク対策として、被扶養者の個人番号を電子申請システム上で入力するとき、その本人確認は被保険者が行うが、被扶養者の個人番号が提供された場合は、地方公共団体情報システム機構に情報照会を行うこと、相談・問い合わせ対応のために電話により個人番号を聞き取る際は、氏名・住所・生年月日等の情報を聴取して本人確認を行うこと等が具体的に記載されている。 入手の際に特定個人情報が漏えい・紛失するリスク対策として、中間サーバー等との通信は、VPN等の技術を用いた専用線等を使用すること、電子記録媒体は暗号化し、施錠した搬送容器にて持ち運ぶこと、日本年金機構から電子記録媒体で入手する場合は、機構職員及び協会職員が、施錠した搬送容器にて複数名で運搬を行い、受取書を取り交わすこと、日本年金機構との通信は、専用回線で行うこと、電子申請システムにて個人番号を含む情報を入手する際は、TSL/SSLにより暗号化されたインターネット回線を使用すること、電子申請システムから適用等システムに、個人番号を含む申請情報を転送する際には、ウイルスチェック等の処理を行った上で、申請情報を暗号化すること等が具体的に記載されている。
		25. 事務を遂行する上で必要な情報以外の特定個人情報を入手しないよう講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.37	Ⅲ 2. リスク1:	問題は認められない	
		26. 特定個人情報の入手に際して、適切な方法で入手するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.38	Ⅲ 2. リスク2:	問題は認められない	
		27. 特定個人情報を入手する際に、その特定個人情報が本人の情報であることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.39	Ⅲ 2. リスク3:	問題は認められない	
		28. 入手した個人番号が本人の個人番号で間違いないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.39	Ⅲ 2. リスク3:	問題は認められない	
		29. 特定個人情報を入手した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.39	Ⅲ 2. リスク3:	問題は認められない	
		30. 特定個人情報を入手する際に、情報の安全確保の観点から講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.40 ～ P.41	Ⅲ 2. リスク4:	問題は認められない	
		31. 特定個人情報の入手において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.41	Ⅲ 2. その他のリスク	問題は認められない	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
	④特定個人情報の使用について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	32. 宛名システム等において、特定個人情報が、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要のない情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.42	Ⅲ 3. リスク1：	問題は認められない	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対策として、適用等システム、保健事業システム及び個人番号管理システムについては、全てのシステム利用者にユーザID、パスワードを発行してログイン認証を行うこと、共有のユーザIDは使用しないこととすること、パスワードを定期的に変更することをルール化すること、アクセス権限が付与された担当者以外は個人番号を取り扱えないようシステム的に制御すること、アクセス権限を付与する担当者は最小限とすること、入手した公金受取口座情報については、情報項目に不必要な情報が紐づけられないようシステムにおいて制御すること等が具体的に記載されている。 不正に複製されるリスク対策として、適用等システム、保健事業システム及び個人番号管理システムについては、特定個人情報を含んだ電子記録媒体は暗号化し、施錠できる保管庫等で管理すること、個人番号管理システム専用端末は、統合専用端末との情報の授受を行うため、隔離した専用の室内に設置し、同室内への入退室はセキュリティカードにより管理すること、統合専用端末は、隔離した専用の室内に設置し、同室内への入退室はセキュリティカードにより管理すること、職員はシンクライアント端末を使用し、特定個人情報をダウンロードすることはできないこと、統合専用端末、シンクライアント端末及び個人番号管理システム専用端末のいずれの端末も、インターネットからは分離されていること等が具体的に記載されている。
		33. 事務で使用するその他のシステムにおいて、特定個人情報が、使用目的を超えて取り扱われないよう、また、評価対象の事務に必要のない情報と併せて取り扱われないよう、講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.42	Ⅲ 3. リスク1：	問題は認められない	
		34. 特定個人情報にアクセスする際の認証を行う場合は、特定個人情報にアクセスするユーザの認証方法、なりすましが行われないために講じている対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.42	Ⅲ 3. リスク2：	問題は認められない	
		35. 特定個人情報ファイルを取り扱う者が正当なユーザであることを確認するための情報の発効・失効の管理について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.42	Ⅲ 3. リスク2：	問題は認められない	
		36. アクセス権限の発効・失効の管理を行う者による当該管理の適正性についてチェックをしている内容を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.43	Ⅲ 3. リスク2：	問題は認められない	
		37. 特定個人情報の入手から消去までの各過程において、特定個人情報ファイルの取扱い記録やアクセスの失敗の記録等を残していることを具体的に記載しているか。記録を残していない場合は、残していなくても権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.43	Ⅲ 3. リスク2：	問題は認められない	
		38. 従業者が特定個人情報ファイルを事務外で使用しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.44	Ⅲ 3. リスク3：	問題は認められない	
		39. 特定個人情報ファイルを取り扱う者が特定個人情報ファイルを不正に複製しないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.44	Ⅲ 3. リスク4：	問題は認められない	
		40. 特定個人情報の使用において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.44	Ⅲ 3. その他のリスク	該当なし	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
	⑤特定個人情報の委託について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	41. 委託先を決定する際に特定個人情報ファイルを適切に取り扱う委託先であることを確認する手続等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.45	Ⅲ 4. 情報管理体制	問題は認められない	個人番号管理システムの導入や保守・点検等を委託することとしているが、委託先は認証資格を取得している等、情報保護管理について十分な体制である者を選定すること等が具体的に記載されている。 委託先においては、特定個人情報を取り扱う事務を行わせる従業者を必要最小限とし、協会職員と同様に取り扱う事務の範囲や特定個人情報ファイルへのアクセス権限をシステム的に制限すること、システム操作におけるログを記録し、一定期間保管すること、特定個人情報を取り扱う端末は、作業後、特定個人情報を保存せず、速やかに消去すること等が具体的に記載されている。
		42. 委託先において特定個人情報ファイルの閲覧者・更新者を必要最小限に制限していることを具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.45	Ⅲ 4. 閲覧者・更新者の制限	問題は認められない	
		43. 委託先における特定個人情報ファイルの取扱いについて記録を残している場合は、その方法や保存期間等を具体的に記載しているか。また、記録を残していない場合は権限のない者による不正な使用を防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.45	Ⅲ 4. 記録	問題は認められない	
		44. 委託に伴う特定個人情報の提供に関するルールを定めている場合、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託先から他者への提供を認めていない場合、提供されていないことを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.45 ～ P.46	Ⅲ 4. 提供ルール	問題は認められない	
		45. 委託先における特定個人情報の消去のルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。また、委託契約終了後に消去されていることを確認する方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.46	Ⅲ 4. 消去ルール	問題は認められない	
		46. 委託先と締結する委託契約における特定個人情報ファイルの取扱いに関する規定について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.46	Ⅲ 4. 委託契約書中の規定	問題は認められない	
		47. 特定個人情報ファイルの取扱いを再委託している場合、再委託先での適正な取扱いの確保のために行っている措置について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.47	Ⅲ 4. 再委託	問題は認められない	
		48. 特定個人情報ファイルの取扱いの委託において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.47	Ⅲ 4. その他のリスク	該当なし	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
	⑥特定個人情報の提供・移転について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	49. 特定個人情報の提供又は移転の記録を残している場合は、その記録の内容や記録方法、保存期間等を具体的に記載しているか。また、記録を残していない場合は特定個人情報が不正に提供又は移転されることを防止できる理由を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.48	Ⅲ 5. リスク1：	該当なし	―
		50. 特定個人情報の提供・移転に関するルールを定めている場合は、ルールの内容やルール遵守の確認方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.48	Ⅲ 5. リスク1：	該当なし	
		51. 特定個人情報を提供・移転する際に、情報漏えいや紛失のリスクを軽減するための措置や提供先・移転先における特定個人情報の使途が法令に基づく適切なものであることを確認するための措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.48	Ⅲ 5. リスク2：	該当なし	
		52. 誤った特定個人情報を提供・移転することや誤った相手に提供・移転することを防止する措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.48	Ⅲ 5. リスク3：	該当なし	
		53. 特定個人情報の提供・移転において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.48	Ⅲ 5. その他のリスク	該当なし	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
	⑦情報提供ネットワークシステムとの接続について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	54. 情報提供ネットワークシステムを通じて特定個人情報を入手する際に、目的外の入手が行われないために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.49	Ⅲ 6. リスク1:	問題は認められない	情報提供ネットワークシステムを通じて目的外の入手が行われるリスク対策として、中間サーバー等に接続する端末(統合専用端末、個人番号管理システム専用端末、シンクライアント端末)を用いた情報提供・照会の操作は、適切な権限を保有する協会職員のみが実施すること、保健事業システムにおける加入者情報照会をする画面機能は、中間サーバー等へ接続できないこと、給付金の請求をする申請書に、登録されている公金受取口座情報の利用希望の有無を確認するチェック欄を設け、当該チェック欄にて利用希望が確認された場合に限り、公金受取口座情報を照会する仕組みとすること等が具体的に記載されている。 入手の際に特定個人情報が漏えい・紛失するリスク対策として、中間サーバー等と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厚生労働省統合ネットワーク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こと、中間サーバー等と医療保険者等の通信は、VPN等の技術を用いた専用線等を使用することで、データ転送時の通信内容秘匿、盗聴防止の対応をすること等が具体的に記載されている。
		55. 情報提供ネットワークシステムを通じて特定個人情報を入手する際に、特定個人情報の安全が保たれない不適切な方法で特定個人情報を入手しないために講じている対策を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.49	Ⅲ 6. リスク2:	問題は認められない	
		56. 情報提供ネットワークシステムを通じて特定個人情報を入手した後、その情報の正確性を保つために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.49	Ⅲ 6. リスク3:	問題は認められない	
		57. 情報提供ネットワークシステムを通じて特定個人情報を入手する際に、情報漏えいや紛失のリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.50	Ⅲ 6. リスク4:	問題は認められない	
		58. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の不正な提供が行われるリスクを軽減するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.50	Ⅲ 6. リスク5:	問題は認められない	
		59. 情報提供ネットワークシステムを通じて提供する際に、特定個人情報の提供方法が不適切とならないよう講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.51	Ⅲ 6. リスク6:	問題は認められない	
		60. 情報提供ネットワークシステムを通じて提供する際に、誤った特定個人情報を提供することや、誤った相手に提供することを防止するために講じている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.51	Ⅲ 6. リスク7:	問題は認められない	
		61. 情報提供ネットワークシステムとの接続に伴うリスクについて、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.52	Ⅲ 6. その他のリスク	問題は認められない	

審査の観点 （指針第10(2)）	主な考慮事項	主な考慮事項(細目)	該当箇所		審査結果	所見
	⑧特定個人情報の保管・消去について、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	62. 特定個人情報の漏えい・滅失・毀損を防ぐために行っている物理的な対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.53	Ⅲ 7. リスク1: ⑤	問題は認められない	物理的対策として、サーバ室、運用保守エリアは、IDカード・パスワード認証による立入の制限や入退室記録の管理をすること、監視カメラを設置すること、サーバ、個人番号管理システム専用端末、統合専用端末及びシンクライアント端末をインターネット等外部ネットワークと隔離すること、中間サーバー等は、セキュリティを確保したサーバー室に設置し、許可された者のみが入退室できる管理対象区域にて設置すること、入手した電子記録媒体は、パスワードを設定し、媒体管理簿の記載を行い、施錠可能な保管庫等にて厳重に保管すること、保管の必要がない使用済みの電子記録媒体等はシュレッダー等にて破棄すること等が具体的に記載されている。 技術的対策として、適用等システム、保健事業システムに接続して事務を行う端末をシンクライアント化し、ローカル環境への保存ができないよう制御すること、適用等システムにおいては、個人番号を暗号化して保有すること、支部と本部の間の通信に専用回線を用いること、日本年金機構との通信に専用回線を用いること等が具体的に記載されている。 特定個人情報が古い情報のまま保管され続けるリスク対策として、給付金申請の際に公金受取口座の利用希望があった場合は、その都度情報照会をして更新するため、常に最新の情報連携で取得した情報のみ保管すること等が記載されている。 特定個人情報が消去されずいつまでも存在するリスク対策として、電子申請システムから適用等システムに個人番号を含む申請情報を転送後、電子申請システムから個人番号を含む申請情報はシステム処理により自動で削除されること、適用等ファイルにおいて保有する暗号化した個人番号は、決裁後システム処理により自動で削除されること等が具体的に記載されている。
		63. 特定個人情報の漏えい・滅失・毀損を防ぐために行っている技術的な対策について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.54	Ⅲ 7. リスク1: ⑥	問題は認められない	
		64. 過去3年以内に発生した全ての重大事故の内容、原因、影響、重大事故発生時への対応等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.54	Ⅲ 7. リスク1: ⑨	該当なし	
		65. 重大事故を受けて策定・実施した再発防止策の内容について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.54	Ⅲ 7. リスク1: ⑨	該当なし	
		66. 死者の個人番号を保管している場合は保管方法を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.54	Ⅲ 7. リスク1: ⑩	問題は認められない	
		67. 特定個人情報を最新の状態で保管するために行っている措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.55	Ⅲ 7. リスク2:	問題は認められない	
		68. 保管期間を経過した特定個人情報を適切な時に安全かつ確実に消去できる手続・体制・手法になっているか等について具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし、妥当なものか。	P.56	Ⅲ 7. リスク3:	問題は認められない	
		69. 特定個人情報の保管・消去において、その他のリスク及びそれらのリスクへの対策についての記載はあるか。	P.56	Ⅲ 7. その他のリスク	問題は認められない	

評価実施機関に特有の問題に対するリスク対策

審査の観点（指針第10(2)）	主な考慮事項	主な考慮事項（細目）	該当箇所		審査結果	所見
(10)特定されたリスクを軽減するために講ずべき措置についての記載は具体的か。 (11)記載されたリスクを軽減させるための措置は、個人のプライバシー等の権利利益の侵害の未然防止、国民・住民の信頼の確保という特定個人情報保護評価の目的に照らし、妥当なものか。	⑩その他、評価実施機関に特有な問題や懸念に対し、特定されたリスクを軽減するために講ずべき措置を具体的に記載しているか。記載された対策は、特定個人情報保護評価の目的に照らし妥当なものか。	74. 電子申請システムにより特定個人情報を入手するが、その際の取扱いに係るリスク対策を具体的に記載しているか。記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P.36等	Ⅲ 2. リスク1等	問題は認められない	・本人がマイナポータルの自己情報取得APIを利用し、自身の健康保険の資格情報を取得し、協会の資格情報が取得できた場合に限り電子申請を可能とすること ・電子申請システムにて個人番号を含む情報を入手する場合には、Webフォームまたは指定の様式に必要事項を記載・提出いただく形とすることに加え、ホームページや記入の手引き等により不必要な情報を入力することがないよう案内すること ・被扶養者の個人番号を電子申請システム上で入力するとき、その本人確認は被保険者が行うが、被扶養者の個人番号が提供された場合は、地方公共団体情報システム機構に情報照会を行うこと ・電子申請システムにて個人番号を含む情報を入手する際は、TSL/SSLにより暗号化されたインターネット回線を使用すること ・電子申請システムから適用等システムに、個人番号を含む申請情報を転送する際には、ウイルスチェック等の処理を行った上で、申請情報を暗号化すること ・電子申請システムから適用等システムに個人番号を含む申請情報を転送後、電子申請システムから個人番号を含む申請情報はシステム処理により自動で削除されること 等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。
		75. 個人番号をキーとして被保険者検索を実施するが、その際の取扱いに係るリスク対策を具体的に記載しているか。記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P.36等	Ⅲ 2. リスク1等	問題は認められない	・番号法第16条（本人確認の措置）に則り本人確認を行い、本人確認後の加入者の個人番号の提供を受けること ・職員はシンクライアント端末を使用し、特定個人情報をダウンロードすることはできないこと ・シンクライアント端末はインターネットからは分離されていること ・アクセス権限が付与された担当者以外は個人番号を取り扱えないこと ・適用等システムにおいては、個人番号を暗号化して保有すること ・適用等ファイルにおいて保有する暗号化した個人番号は、決裁後システム処理により自動で削除されること 等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。
		76. 給付金の支給に当たり、情報提供ネットワークシステムを介して公金受取口座情報を入手し、使用するが、その際の取扱いに係るリスク対策を具体的に記載しているか。記載された対策は特定個人情報保護評価の目的に照らし、妥当なものか。	P.43等	Ⅲ 3. リスク2等	問題は認められない	・入手した公金受取口座情報については、情報項目に不必要な情報が紐づけられないようシステムにおいて制御すること ・給付金の請求をする申請書に、登録されている公金受取口座情報の利用希望の有無を確認するチェック欄を設け、当該チェック欄にて利用希望が確認された場合に限り、公金受取口座情報を照会する仕組みとすること ・給付金申請の際に公金受取口座の利用希望があった場合は、その都度情報照会をして更新するため、常に最新の情報連携で取得した情報のみ保管すること 等が具体的に記載されており、特定個人情報保護評価の目的に照らし、妥当である。

【総評】

(1)　健康保険の資格適用・保険給付・保健事業・相談・問い合わせに関する事務においては、特定個人情報ファイルを取り扱うことについて、一連の事務の内容や流れが具体的に記載されており、特段の問題は認められないものと考えられる。

(2)　事務で取り扱われる特定個人情報ファイルの取扱いについてのリスク及びリスク対策が具体的に記載されており、特段の問題は認められないものと考えられる。

(3)　電子申請による入手に係るリスク対策、個人番号をキーとした被保険者情報の検索に係るリスク対策、公金受取口座情報の入手等に係るリスク対策等、本評価対象事務において懸念されるリスク及びリスク対策についても具体的に記載されており、特段の問題は認められないものと考えられる。

【個人情報保護委員会による審査記載事項】

（Ⅵ　評価実施手続　4. 個人情報保護委員会の承認）

(1)　健康保険の資格適用・保険給付・保健事業・相談・問い合わせに関する事務の内容、特定個人情報ファイルの内容、特定個人情報の流れ並びにリスク及びリスク対策が具体的に記載されており、特段の問題は認められないと考えられるが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。

(2)　特定個人情報のインターネットへの流出を防止する対策については、インターネット接続端末と特定個人情報を取り扱う端末とはネットワークが分離されていること等の措置が記載されているが、特定個人情報保護評価書に記載されているとおり確実に実行する必要がある。

(3)　組織的及び人的安全管理措置については、適切な組織体制の整備、職員への必要な教育・研修、実効性のある自己点検・監査等を実施し、実務に即して適切に運用・見直しを行い、今後リスクを相当程度変動させ得る事実関係の変更が生じ、当該変更に応じたリスク対策を講ずる際などには、必要な特定個人情報保護評価を適切に実施する体制を、有効に機能させることが重要である。

(4)　自身の記号・番号を把握していない加入者から申請や問い合わせがあった場合、個人番号による被保険者情報の検索を実施することとなるが、特定個人情報ファイルにアクセスする者の増加に伴い、悪意をもった従業者が、事務外で不正に特定個人情報を使用することがないよう、定期的なログの分析や監査等を通じて確認を徹底するとともに、当該取組を通じて不正行為への牽制を図ることが重要である。

(5)　上記について、不断の見直し・検討を行うことに加え、事務フローの変更や新たなリスク対策が生ずることとなった場合は、必要に応じて評価の再実施を行うことが重要である。