資料１－２

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及び保険給付に関する事務

評価実施機関名
全国健康保険協会

提出日
平成29年7月28日

概要説明日
平成29年8月7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。	—	—	—	—	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及び保険給付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個人番号管理システム等の開発は、平成29年7月にシステムの要件定義が終了し、平成29年9月上旬以降からプログラミングの開始を予定しており、実施時期については委員会と協議の上、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及び保険給付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。

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)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及び保険給付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。
(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.1 ～ P.2	Ⅰ 1. ②	問題は認められない	健康保険の資格適用及び保険給付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図ら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.2	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.2	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.5	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.5	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.6 ～ P.8	Ⅰ (別添1)	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
(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.21 ～ P.38	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。
(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.38	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し、当該計画に基づいて、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、新規職員採用時に研修を実施すること、また、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.38	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.38	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.40	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及び保険給付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ることをもって、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。

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.9	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、個人番号を既存システムの識別番号と紐付けて都道府県民税又は市区町村民税の情報を個人番号管理情報ファイルから検索・参照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）書など帳票類は保管庫等に保管・管理し、個人番号管理システム及び適用等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.9	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.11	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.11	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.11	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.11	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.11	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.11	Ⅱ 3. ⑧	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
		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.12 ～ P.16	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.12 ～ P.16	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.12 ～ P.16	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.17	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.17	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.19	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.19	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.19	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.21	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、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、電子記録媒体により入手する場合は、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には、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。 入手の際の特定個人情報の漏えい・紛失を防止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、日本年金機構との通信は、専用回線で行う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.21	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.22	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.22	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.22	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.23	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.23	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.23	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.24	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.24	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.24	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.25	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.25	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.25	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.26	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.26	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.26	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.27	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をしている等、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、システムの操作におけるログを記録し、一定期間保管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.27	Ⅲ 4. 閲覧者の制限	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.27	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.28	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.29	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.29	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.29	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.29	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.30	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.30	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.30	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.30	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.30	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.31	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特定個人情報の入手を防止す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等が具体的に記載されている。 入手の際の特定個人情報の漏えい・紛失を防止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.31	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.31	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.32	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.32	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.33	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.33	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.34	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.35	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等が具体的に記載されている。 また、中間サーバー等は、データセンターに設置し、設置場所への入退室記録管理、監視カメラによる監視及び施錠管理を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、適用等システム及び個人番号管理システムにおいては、適用等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、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。 また、中間サーバー等においては、保有する特定個人情報が、端末等を通じてインターネットに流出することを防止するため、インターネットには接続できないようシステム面の措置を講じていること、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、アクセス制御、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.36	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.36	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.36	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.36	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.37	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.37	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.37	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. 特定個人情報の使用の記録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.22	Ⅲ 3. リスク2	問題は認められない	①個人番号の登録や更新、情報検索、個人番号を含むデータ表示機能等の使用、及び特定個人情報ファイルへのアクセスなどについて、システム操作ログを自動的に記録すること、②システム管理者は定期的にシステム操作ログを確認し、不正な運用が行われていないか確認すること等が具体的に記載されている。 操作ログの確認について、当委員会から、今後操作が増大した場合においても効果的・効率的な確認を行えるよう、更なる対応策を確認した結果、システム化による自動点検等を検討するとの報告を受けた。

【総評】

(1) 健康保険の資格適用及び保険給付に関する事務においては、適用等システム、個人番号管理システム及び中間サーバー等を使用し、特定個人情報ファイルである健保特定個人情報ファイルを適切に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健保特定個人情報ファイルについて、特定個人情報ファイルの内容、特定個人情報の流れ、使用するシステムの機能並びに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) 操作ログの確認について、当委員会から、今後操作が増大した場合においても効果的・効率的な確認を行えるよう、更なる対応策を確認した結果、システム化による自動点検等を検討するとの報告を受けた。

【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及び保険給付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) 特定個人情報の取扱いについては厳格な対応が求められるため、職員への教育・研修を実務に即して実施するとともに、実効性のある自己点検・監査を実施することが重要である。

(4) 情報漏えい等に対するリスク対策については、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とともに、不断の見直し・検討を行うことが重要である。特に操作ログの確認は、非常に重要なリスク対策であるとの認識のもと、将来的な情報照会の増加も踏まえて、実効性のある対策を講じることが重要である。