特定個人情報保護評価書（基礎項目評価書）

評価書番号	評価書名
38	重度障がい者医療費助成事務

個人のプライバシー等の権利利益の保護の宣言

吹田市は、重度障がい者医療費助成事務において特定個人情報ファイルを取り扱うにあたり、その取扱いが個人のプライバシー等の権利利益に影響を及ぼしうることを認識し、特定個人情報の漏えいその他の事態が発生するリスクを軽減させるため、番号法及び個人情報保護に関する法令を遵守するとともに、特定個人情報ファイルの保護と安全な利用について適切な措置を実施することで、個人のプライバシー等の権利利益の保護に取り組んでいることを宣言する。

特記事項	

評価実施機関名

大阪府吹田市長

公表日

令和6年12月20日

［令和6年10月　様式2］

Ⅰ　関連情報

1. 特定個人情報ファイルを取り扱う事務	
①事務の名称	重度障がい者医療費助成事務
②事務の概要	吹田市重度障がい者の医療費の助成に関する条例に基づき、重度障がい者医療証交付申請書の受付、重度障がい者医療証の交付、医療費の助成及び受給者台帳の管理等を行う。特定個人情報ファイルは、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。）の規定により、次の事務において使用する。 ・重度障がい者医療証交付申請者に係る所得判定事務 ・医療費助成対象者に係る所得判定事務 ・重度障がい者医療証交付申請者に係る健康保険情報の取得事務 ・医療費助成対象者に係る健康保険情報の取得事務
③システムの名称	①医療費助成システム　②団体内統合宛名システム　③中間サーバー　④住登外システム

2. 特定個人情報ファイル名
重度障がい者医療費助成台帳ファイル

3. 個人番号の利用	
法令上の根拠	番号法第9条第2項

4. 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	〔情報提供の根拠〕 なし 〔情報照会の根拠〕 番号法第19条第9号	

5. 評価実施機関における担当部署	
①部署	福祉部障がい福祉室
②所属長の役職名	室長

6. 他の評価実施機関

7. 特定個人情報の開示・訂正・利用停止請求	
請求先	吹田市市民部市民総務室　住所：吹田市泉町1丁目3番40号　電話：06-6384-1456

8. 特定個人情報ファイルの取扱いに関する問合せ	
連絡先	吹田市福祉部障がい福祉室　住所：吹田市泉町1丁目3番40号　電話：06-6384-1347

9. 規則第9条第2項の適用	[　]適用した
適用した理由	

Ⅱ　しきい値判断項目

1. 対象人数			
評価対象の事務の対象人数は何人か		[　1,000人以上1万人未満　]	＜選択肢＞ 1) 1,000人未満（任意実施） 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
	いつ時点の計数か	令和6年4月1日 時点	
2. 取扱者数			
特定個人情報ファイル取扱者数は500人以上か		[　500人未満　]	＜選択肢＞ 1) 500人以上　2) 500人未満
	いつ時点の計数か	令和6年4月1日 時点	
3. 重大事故			
過去１年以内に、評価実施機関において特定個人情報に関する重大事故が発生したか		[　発生なし　]	＜選択肢＞ 1) 発生あり　2) 発生なし

Ⅲ　しきい値判断結果

しきい値判断結果
基礎項目評価の実施が義務付けられる

Ⅳ リスク対策

1. 提出する特定個人情報保護評価書の種類		
	[基礎項目評価書]	<選択肢> 1) 基礎項目評価書 2) 基礎項目評価書及び重点項目評価書 3) 基礎項目評価書及び全項目評価書
2)又は3)を選択した評価実施機関については、それぞれ重点項目評価書又は全項目評価書において、リスク対策の詳細が記載されている。		

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。）		
目的外の入手が行われ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

3. 特定個人情報の使用		
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
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

4. 特定個人情報ファイルの取扱いの委託		[ ]委託しない
委託先における不正な使用等の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

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
不正な提供・移転が行われるリスクへの対策は十分か	[ ]	<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

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）
目的外の入手が行われ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	
不正な提供が行われるリスクへの対策は十分か	[ ]	<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	

7. 特定個人情報の保管・消去		
特定個人情報の漏えい・滅失・毀損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

8. 人手を介在させる作業		[　]人手を介在させる作業はない
人為的ミスが発生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
判断の根拠	・特定個人情報を含む書類や電子媒体は、施錠可能なキャビネット等に適切に保管している。 ・出張等によりマイナンバー記載書類等の持出しがある場合は、庁外持出管理簿を用いて持出から返却に至るまで上司が徹底管理している。 ・マイナンバー関連の書類を送付する際は、複数の職員が相互にチェックを行う等、誤送付のないよう対策を講じている。	

9. 監査		
実施の有無	［ ○ ］ 自己点検　［　 ］ 内部監査　［　 ］ 外部監査	
10. 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
11. 最も優先度が高いと考えられる対策	**［　］全項目評価又は重点項目評価を実施する**	
最も優先度が高いと考えられる対策	［ 3) 権限のない者によって不正に使用されるリスクへの対策 ］ ＜選択肢＞ 1) 目的外の入手が行われるリスクへの対策 2) 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への対策 3) 権限のない者によって不正に使用されるリスクへの対策 4) 委託先における不正な使用等のリスクへの対策 5) 不正な提供・移転が行われるリスクへの対策(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。) 6) 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への対策 7) 情報提供ネットワークシステムを通じて不正な提供が行われるリスクへの対策 8) 特定個人情報の漏えい・滅失・毀損リスクへの対策 9) 従業者に対する教育・啓発	
当該対策は十分か【再掲】	［　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
判断の根拠	・システムマネージャは、年度当初など職員の異動等に応じて設定したアクセス権を一覧表にまとめ、不必要な権限が放置されていないか適宜点検を行っている。 ・管理責任者は、職員に対して業務上必要な範囲を超えたアクセス権を付与することなく、情報セキュリティの確保に必要な記録を一定期間保存する等、不正なログインやアクセスについて常に監視し、必要に応じてアクセスログの分析等を行っている。	

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6年12月20日	【Ⅰ　関連情報】 3. 個人番号の利用 法令上の根拠	番号法第9条第2項	番号法第9条第2項	事後	
令和6年12月20日	【Ⅰ　関連情報】 4. 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	番号法第19条第15号	〔情報提供の根拠〕 　なし 〔情報照会の根拠〕 　番号法第19条第9号	事後	
令和6年12月20日	Ⅳ　リスク対策 8. 人手を介在させる作業 人為的ミスが発生するリスクへの対策は十分か 判断の根拠	ー	・特定個人情報を含む書類や電子媒体は、施錠可能なキャビネット等に適切に保管している。 ・出張等によりマイナンバー記載書類等の持出しがある場合は、庁外持出管理簿を用いて持出から返却に至るまで上司が徹底管理している。 ・マイナンバー関連の書類を送付する際は、複数の職員が相互にチェックを行う等、誤送付のないよう対策を講じている。	事後	様式変更による項目追加
令和6年12月20日	Ⅳ　リスク対策 11. 最も優先度が高いと考えられる対策 当該対策は十分か【再掲】 判断の根拠	ー	・システムマネージャは、年度当初など職員の異動等に応じて設定したアクセス権を一覧表にまとめ、不必要な権限が放置されていないか適宜点検を行っている。 ・管理責任者は、職員に対して業務上必要な範囲を超えたアクセス権を付与することなく、情報セキュリティの確保に必要な記録を一定期間保存する等、不正なログインやアクセスについて常に監視し、必要に応じてアクセスログの分析等を行っている。	事後	様式変更による項目追加