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
6	自立支援医療受給者証（精神通院）の交付に関する事務に係る全項目評価書【法定・都単独事業】

個人のプライバシー等の権利利益の保護の宣言

東京都知事は個人番号を利用するにあたり、特定個人情報の不適正な取り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を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むことを宣言する。

特記事項	本件評価は、しきい値判断においては、重点項目評価に該当するが、より適切な特定個人情報の保護を確保するため、全項目評価として実施するものである。

評価実施機関名

東京都知事

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5月　様式4］

項目一覧

Ⅰ　基本情報
（別添1）事務の内容
Ⅱ　特定個人情報ファイルの概要
（別添2）特定個人情報ファイル記録項目
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
Ⅳ　その他のリスク対策
Ⅴ　開示請求、問合せ
Ⅵ　評価実施手続
（別添3）　変更箇所

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	自立支援医療受給者証（精神通院）の交付に関する事務
②事務の内容　※	・障害者総合支援法及び障害者総合支援法施行細則に基づき、精神疾患のために継続的に通院による治療を受ける必要がある者を対象に医療費の助成を行う。申請者から申請があった場合、区市町村及び都で資格審査の上、受給者証を申請者に交付し台帳管理を行っている。 ・区市町村からの進達で保険情報が確認できない場合等に、都において保険情報照会を行っている。 ・特定個人情報ファイルは、障害者総合支援法及びその他法令の規定に従い、次の事務に使用している。 ア　所得区分及び自己負担上限額の決定、都への進達（区市町村） イ　保険情報の照会（都） ウ　支給認定審査 エ　受給者証の発行、交付 オ　台帳管理 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・情報連携のため、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む対象者情報、公費資格情報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、自身の本事務に係る公費医療費助成の資格情報の取得/閲覧が可能となる。 ・住民が、医療機関受診時に公費医療費助成の給付を受ける際に、従来の紙の受給者証に代えて、マイナンバーカードをオンライン資格確認端末で用いることにより、資格情報を医療機関が取得/閲覧することが可能となる。
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	医療費助成事務システム（精神通院）
②システムの機能	・受給者認定登録 ・受給者情報管理
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　（ PMH、団体内統合利用番号連携サーバー　）
システム2～5	
システム2	
①システムの名称	住民基本台帳ネットワークシステム（東京都サーバ）
②システムの機能	・本人確認情報の更新・管理・全国サーバに対する更新通知 ・本人確認の情報抽出・出力 ・全国サーバへの情報照会
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　（ 中間サーバー　）

システム3	
①システムの名称	団体内統合利用番号連携サーバー（以下「連携サーバ」という。）
②システムの機能	・中間サーバーへの符号取得要求の仲介 ・団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号、個別業務システム利用番号の紐付管理 ・副本登録における、個別業務システムからの中間サーバーへの登録要求の仲介 ・情報照会における、個別業務システムからの照会要求の受付及び中間サーバーと個別業務システムとの情報授受の仲介
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　（ 中間サーバー、医療費助成事務システム（精神通院）　）
システム4	
①システムの名称	中間サーバ
②システムの機能	・符号及び団体内統合利用番号の取得、管理 ・符号、団体内統合利用番号の紐付管理 ・副本管理 ・情報照会の受付及び管理 ・情報提供管理
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　（ 連携サーバ　）
システム5	
①システムの名称	Public Medical Hub　（PMH）
②システムの機能	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ①情報登録機能及びPMHキー採番依頼機能等 東京都立中部総合精神保健福祉センター（以下、「センター」という。）で管理している個人番号及び公費医療費助成の資格情報等をPublic Medical Hub（PMH）に登録し、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。 ②情報連携機能（医療機関システム） ・PMH連携キーを利用した情報提供機能 医療機関からの問い合わせに対し、公費医療費助成の資格情報を連携する。 医療機関のオンライン資格確認端末で、患者（利用者）が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上で都度、PMH連携キーが生成され、公費医療費助成の資格情報の照会が行われる。Public Medical Hub（PMH）は、PMH連携キーからPMHキーを復号し、PMHキーに紐付けられた公費医療費助成の資格情報を医療機関システムへ提供する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 マイナポータルからのPublic Medical Hub（PMH）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Public Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報提供機能 公費医療費助成の対象者は、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。Public Medical Hub（PMH）は、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く公費医療費助成の資格情報をマイナポータルへ提供する。
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　（ 東京都医療費助成事務システム　）
システム6～10	

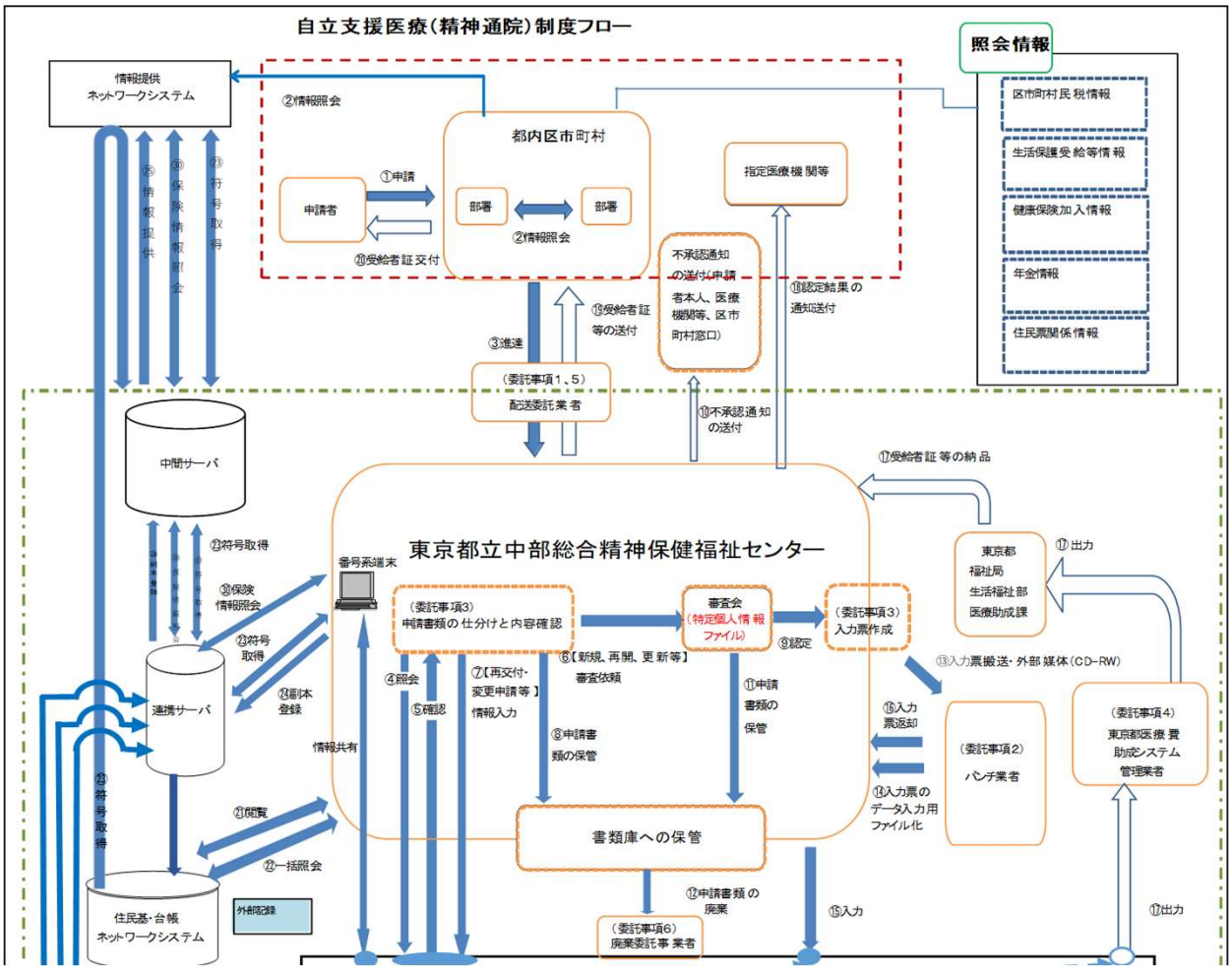
システム11～15	
システム16～20	
3. 特定個人情報ファイル名	
自立支援医療費（精神通院）認定事務ファイル	
4. 特定個人情報ファイルを取り扱う理由	
①事務実施上の必要性	自立支援医療受給者証（精神通院）の交付に関する事務を適切に行うために、最新かつ正確な生活保護関係情報、区市町村民税情報を把握する必要がある。
②実現が期待されるメリット	より正確な自立支援医療受給者証（精神通院）の交付に関する事務を行うことができるとともに、申請者からの添付書類の提出を削減できる。
5. 個人番号の利用　※	
法令上の根拠	【法定】 番号法第9条第1項　別表　第117の項　内閣府総務省令第5号第60条 【都単独事業】 番号法第9条第2項 番号法に基づく個人番号の利用及び特定個人情報の提供に関する条例第4条　別表第一第4項 番号法に基づく個人番号の利用及び特定個人情報の提供に関する条例施行規則第4条 【区市町村】 特別区における東京都の事務処理の特例に関する条例 特別区における東京都の事務処理の特例に関する条例に基づき特別区が処理する事務の範囲等を定める規則 市町村における東京都の事務処理の特例に関する条例 市町村における東京都の事務処理の特例に関する条例に基づき市町村が処理する事務の範囲等を定める規則 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞における追加措置＞ 番号法第19条6号
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	【法定】 番号法第19条8号に基づく主務省令第2条の表144の項 内閣府総務省令第7号第19条、第30条第12号、第44条、第55条第6号、第55条第7号、第55条の2、第55条の3 【都単独事業】 番号法第19条第16号 番号法第19条第15号に基づき同条第7号に準ずるものとして定める特定個人情報の提供に関する規則第3条 番号法に基づく個人番号の利用及び特定個人情報の提供に関する条例第4条　別表第一第4項 番号法に基づく個人番号の利用及び特定個人情報の提供に関する条例施行規則第4条 【区市町村】 特別区における東京都の事務処理の特例に関する条例 特別区における東京都の事務処理の特例に関する条例に基づき特別区が処理する事務の範囲等を定める規則 市町村における東京都の事務処理の特例に関する条例 市町村における東京都の事務処理の特例に関する条例に基づき市町村が処理する事務の範囲等を定める規則
7. 評価実施機関における担当部署	
①部署	東京都立中部総合精神保健福祉センター
②所属長の役職名	所長
8. 他の評価実施機関	
東京都内各区市町村長、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。）	

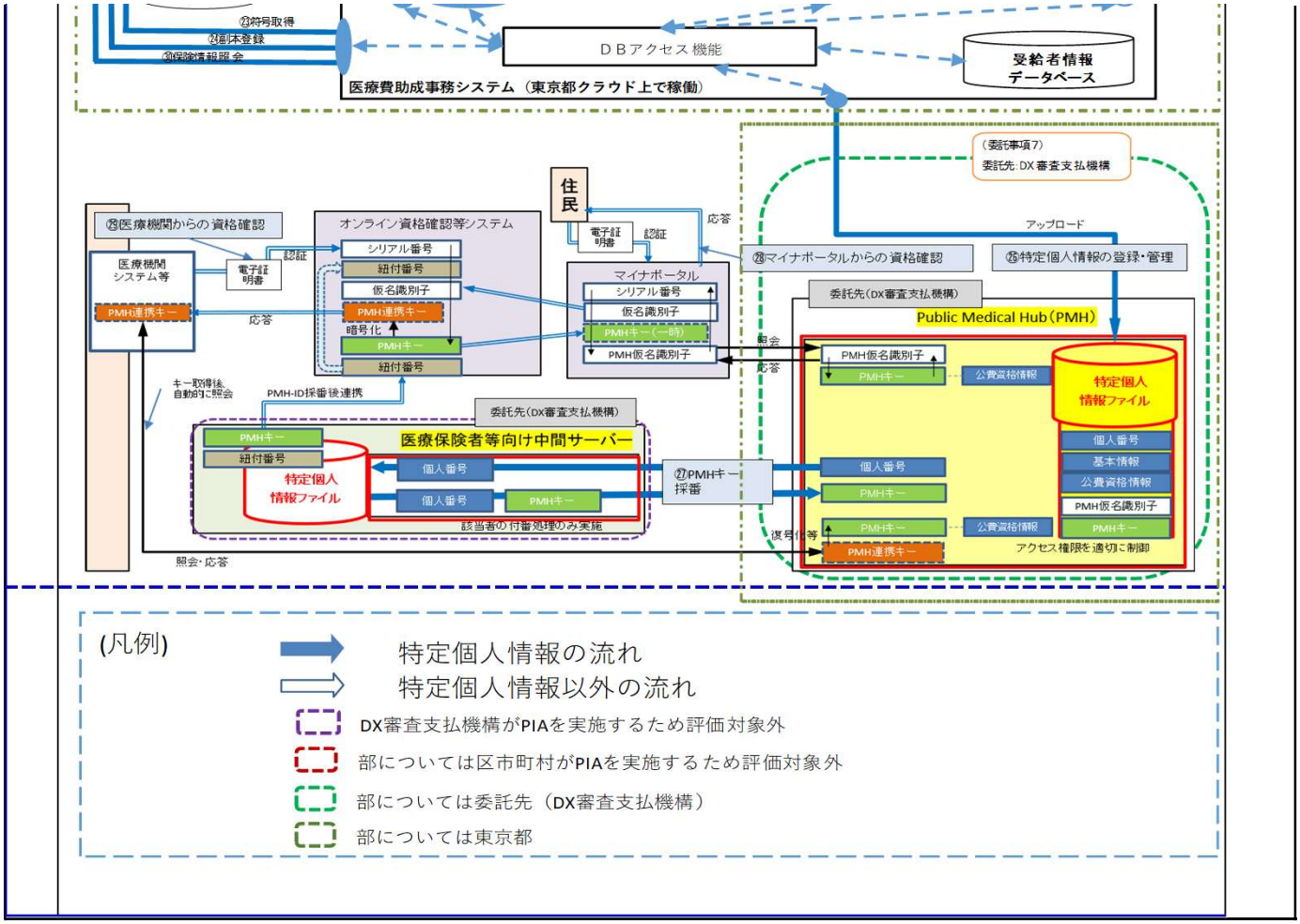
（別添1）事務の内容

実施マニュアル_様式
［都様式

事務・システムフロー図

評価書番号	6	担当部署	東京都立中部総合精神保健福祉センター
事務の名称	自立支援医療受給者証（精神通院）の交付に関する事務		
システムの名称	医療費助成事務システム		





(凡例)

特定個人情報の流れ

特定個人情報以外の流れ

DX審査支払機構がPIAを実施するため評価対象外

部については区市町村がPIAを実施するため評価対象外

部については委託先（DX審査支払機構）

部については東京都

（備考）

1.取得
①申請者が居住地である区市町村窓口に申請を行う。
②区市町村窓口で申請書類を収受し、区市町村は区市町村民税情報等の必要な情報照会を行う。
③区市町村はセンターに進達を行う。
（搬送委託（委託事項5）または郵送（委託事項1））
2. 認定
④受給状況の確認を行うために、東京都医療費助成システム（以下、「システム」という。）で照会を行う。（委託事項3）
⑤システムで受給内容の把握を行う。（委託事項3）
⑥審査会の審査が必要な申請書類（新規、再開、更新等）は審査にかける。（職員）
⑦審査不要な申請書類（再交付・変更申請等）の個人情報をシステムへ入力する。（委託事項3）
⑧審査不要の申請書類は入力終了後、書類庫へ保管する。（職員）
⑨審査会で認定された申請書類について入力票の作成を行う。（委託事項3）
⑩審査会で不承認とされた場合には、不承認通知を申請者本人、医療機関等、区市町村窓口へ送付する。（職員）
⑪審査が終了した申請書類は、センター書類庫へ保管する。（職員）
⑫保存期間満了後、申請書類を廃棄する。（委託事項6）
⑬作成した入力票を取りまとめて、入力票をパンチ業者へ搬送する。また、空の外部記録媒体（CD-RW）を搬送する。（委託事項2）
⑭パンチ業者にて入力票の個人情報をシステムで処理可能なデータ入力用ファイルとして作成し、センターに外部記録媒体（CD-RW）で返送する。（委託事項2）
⑮センターがシステムに入力する。（職員）
⑯パンチ業者から入力票が返却される。（委託事項2）
⑰システム管理業者が個人情報を出力し、東京都福祉局生活福祉部医療助成課（以下、「医療助成課」という。）が受給者証等の印刷契約を締結した事業者から受給者証等をセンターへ納品する。
⑱センターから医療機関等へ認定結果の通知を送付する。（委託事項1（郵便局への搬送））
3. 受給者証交付
⑲受給者証等を申請者の居住地の区市町村窓口へ送付する。（搬送委託（委託事項5）または郵送（委託事項1））
⑳区市町村窓口より受給者証を申請者に交付する。
4. 副本登録（職員のみ）
㉑住基への照会件数が少ない場合は、センターが都庁にある住民基本台帳ネットワークシステムを閲覧し、本人確認情報を取得する。
㉒住基への照会件数が多い場合は、センターが外部記録媒体（CD-RW）を持参し、都庁（総務局行政部）にて住民基本台帳ネットワークシステムから一括照会し、本人確認情報を取得する。取得した情報をシステムに取り込む.。
㉓符号取得する
㉔副本登録を行う。
㉕情報提供を行う。
5. PMHを利用した情報連携
㉖・特定個人情報の登録・管理　情報連携のため、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む対象者情報、公費医療資格情報等の紐付け及び登録を行う。（LGWAN回線等経由）
・PMH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
㉗PMHHD採番　・PMHは、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、PMHキーを採番してPMHに回答する。医療保険者等向け中間サーバーは、PMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。
㉘マイナポータルからの資格確認　・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、PMH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、マイナポータルからの資格確認が可能となる。
・住民がマイナポータル経由で、自身の公費医療資格情報を確認する。
㉙医療機関からの資格確認　・オンライン資格確認等システムは、紐付番号をキーにマイナンバーカードの電子証明書のシリアル番号とPMHキーを紐付けて、一時的に利用するためのPMH連携キーを暗号化して生成する。オンライン資格確認等システムは、PMHにPMH連携キーで公費医療費助成の資格情報を照会し、照会元となる医療機関システム等に同資格情報を応答する。（PMH連携キーは都度作成され、利用後に削除される。）医療機関システム等を利用して受診者が、マイナンバーカードで認証し、同意する都度、資格確認が可能となる。
6. 保険情報の情報提供ネットワークシステムへの情報照会
㉚医療費助成システムから連携サーバ及び中間サーバを経由し情報提供ネットワークシステムへ保険情報の情報照会を行う。

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

自立支援医療費（精神通院）認定事務ファイル

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 ※		自立支援医療受給者証（精神通院）の発行を受けたもの
	その必要性	適正に自立支援医療費（精神通院）の支給認定を行い受給者証を発行するため
④記録される項目		［　10項目以上50項目未満　］　＜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 ［ ○ ］5情報（氏名、氏名の振り仮名、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　（　医療費資格情報　）
	その妥当性	・個人番号及びその他識別情報：対象者を正確に特定するために保有 ・4情報及び連絡先：①受給者証に記載して発行するため、②本人への連絡等のために保有 ・生活保護・社会福祉関係・年金関係情報：受給者の所得区分及び自己負担限度額を決定するために保有 ・障害者福祉関係情報：精神障害者保健福祉手帳との同時申請の場合に手帳に基づき支給認定するために保有 ・健康・医療関係情報：医療費助成の対象となる精神疾患を有しているか確認するために保有 ・医療保険関係情報：所得区分の決定及び支給認定にあたり、医療保険による世帯所得を確認する必要があるため保有 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ○・識別情報（その他識別情報） PMHキー、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 自治体業務ID…PMH内で公費医療の種類を区別するために必要となる。 ・業務関係情報（その他） 医療助成資格情報…（医療費助成事務の適切な実施にあたり必要となる情報を管理し、）PMHが、外部と情報連携するために必要となる。
	全ての記録項目	別添2を参照。
⑤保有開始日		平成28年1月1日
⑥事務担当部署		東京都立中部総合精神保健福祉センター

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 （ ） [ ] 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 （ ） [ ] 民間事業者 （ ） [○] その他 （ 日本年金機構、医療保険者等向け中間サーバー、医療機関用アプリ マイナポータル ）
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 （ 住民基本台帳ネットワークシステム ）
③入手の時期・頻度		都においては、区市町村が個人番号及び所得区分の確認ができず進達した場合等必要に応じて、入手する。 区市町村においては、本人又は本人の代理人が申請した場合に、その都度入手する。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・PMHキーの採番処理依頼時に都度、医療保険者等向け中間サーバーから特定個人情報を入手する。
④入手に係る妥当性		・申請書類：「障害者の日常生活及び社会生活を総合的に支援するための法律」、「障害者の日常生活及び社会生活を総合的に支援するための法律施行細則」、「特別区における東京都の事務処理の特例に関する条例」、「特別区における東京都の事務処理の特例に関する条例に基づき特別区が処理する事務の範囲等を定める規則」、「市町村における東京都の事務処理の特例に関する条例」、「市町村における東京都の事務処理の特例に関する条例に基づき市町村が処理する事務の範囲等を定める規則」に基づき、入手する。 ・区市町村民税情報・生活保護受給等情報・健康保険加入情報・年金情報・住民票関係情報：番号法に基づき、入手する。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・外部との情報連携のため、PMHキーの採番処理依頼時に医療保険者等向け中間サーバーから自動的に入手される。
⑤本人への明示		【法定】 障害者の日常生活及び社会生活を総合的に支援するための法律第53条第1項及び障害者の日常生活及び社会生活を総合的に支援するための法律施行規則第35条に、特定個人情報を入手することが明示されている。 【都単独事業】 障害者の日常生活及び社会生活を総合的に支援するための法律施行細則第15条に、特定個人情報を入手することが明示されている。 【区市町村】 特別区における東京都の事務処理の特例に関する条例 特別区における東京都の事務処理の特例に関する条例に基づき特別区が処理する事務の範囲等を定める規則 市町村における東京都の事務処理の特例に関する条例 市町村における東京都の事務処理の特例に関する条例に基づき市町村が処理する事務の範囲等を定める規則
⑥使用目的 ※		自立支援医療費（精神通院）受給資格の審査及び受給者証の交付
	変更の妥当性	―
⑦使用の主体	使用部署 ※	東京都立中部総合精神保健福祉センター事務室自立支援医療担当 東京都福祉局生活福祉部医療助成課医療調整担当 東京都福祉局障害者施策推進部精神保健医療課生活支援担当
	使用者数	[50人以上100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 ※		Ⅰ　支給認定に関する事務 ・　医療関係情報から支給資格を審査し、支給認定を行う。 ・　医療保険情報、生活保護・社会福祉関係情報から所得区分及び自己負担限度額を決定する。なおこの際、区市町村からの進達で保険情報が確認できない場合等に、都において保険情報照会を行う。 ・　精神障害者保健福祉手帳と同時申請の場合に、障害者福祉関係情報から支給資格を審査し、支給認定を行う。 ・　支給認定結果を指定医療機関等に通知する。 Ⅱ　受給者証交付に関する事務 ・　4情報を受給者証に記載して交付（再交付）する。 Ⅲ　台帳管理に関する事務 ・　支給認定に係る情報を、システムに登録する。 ・　変更申請に基づき、登録情報を変更する。 ・　捜査事項照会等、法令に基づく開示請求に対する回答を行う。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・情報連携のため、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む対象者情報、公費資格情報の紐付け及び登録を行う。 ・登録後、Public Medical Hub（PMH）は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub（PMH）が連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hub（PMH）に応答する。なお、採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金が医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルとPublic Medical Hub（PMH）で共有されることでマイナポータルや医療機関システムから公費資格情報の取得/閲覧を行うといった情報連携が可能となる。
	情報の突合 ※	生活保護・社会福祉関係情報と申告情報を突合して、所得区分を確認する。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・PMHキーの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。
	情報の統計分析 ※	特定個人情報を使用した分析は行わない。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・特定の個人を判別するような情報の統計や分析は行わない。
	権利利益に影響を与え得る決定 ※	自立支援医療受給者証（精神通院）の交付
⑨使用開始日		平成28年1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 （　　7　）件
委託事項1		東京都立中部総合精神保健福祉センター交換便業務等委託
①委託内容		交換便業務（東京都立中部総合精神保健福祉センターと指定場所（原則として都庁）で、個人情報を含む文書等の収集、整理、搬送等の業務を行う。
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 ※	自立支援医療費（精神通院）の申請をした者
	その妥当性	東京都立中部総合精神保健福祉センターから都庁の指定場所まで運ぶために、取扱う必要がある。
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　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		ビーエスロジスティクス株式会社
再委託	⑦再委託の有無 ※	[　再委託しない　] ＜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	
	⑨再委託事項	
委託事項2～5		
委託事項2		医療費助成事務システム入力データファイル作成処理委託
①委託内容		自立支援医療（精神通院）受給者証交付申請に関する申請情報を、システムで処理可能なデータ入力用ファイルとして作成し、提供する。
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一部] ＜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 ※	自立支援医療費（精神通院）の申請をした者
	その妥当性	自立支援医療（精神通院）受給者証を交付するために必要な情報を入力するため、取扱う必要がある。
③委託先における取扱者数		[　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
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　（　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		株式会社PROGRESS
再委託	⑦再委託の有無 ※	[　再委託しない　] ＜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	
	⑨再委託事項	
委託事項3		東京都立中部総合精神保健福祉センター自立支援医療（精神通院）受給者証の交付等業務委託
①委託内容		自立支援医療（精神通院）受給者証の交付のため、申請書の仕分け、データ入力、受給者証の仕分け、発送等を行う。

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 ※	自立支援医療費（精神通院）の申請をした者
	その妥当性	自立支援医療（精神通院）受給者証を交付するために必要な情報を入力や仕分けをするため、取扱う必要がある。
③委託先における取扱者数		［ 50人以上100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　（　　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		東武トップツアーズ株式会社
再委託	⑦再委託の有無 ※	［ 再委託しない ］ ＜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	
	⑨再委託事項	
委託事項4		医療費助成事務の電算処理委託（受給者証作成）
①委託内容		医療費助成事務システムの運用・保守および、受給者証印刷データの作成を行う。
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 ※	自立支援医療費（精神通院）の申請をした者
	その妥当性	自立支援医療（精神通院）受給者証を交付するため、取扱う必要がある。
③委託先における取扱者数		［ 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
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　（　　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		システム開発終了後に保守委託契約を締結する。

再委託	⑦再委託の有無 ※	[　　] ＜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	
	⑨再委託事項	
委託事項5		東京都立中部総合精神保健福祉センター搬送業務委託
①委託内容		搬送業務（東京都立中部総合精神保健福祉センターと指定場所（各区市町村（保健センター等含む）窓口）で、個人情報を含む文書等の収集、整理、搬送等の業務を行う。
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 ※	自立支援医療費（精神通院）の申請をした者
	その妥当性	東京都立中部総合精神保健福祉センターと各区市町村の指定場所との間での搬送のために、取扱う必要がある。
③委託先における取扱者数		[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
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　（　　）
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		ビーエスロジスティクス株式会社
再委託	⑦再委託の有無 ※	[再委託しない] ＜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	
	⑨再委託事項	
委託事項6～10		
委託事項6		機密文書の収集・運搬及び処分を行う。
①委託内容		保管期間満了の申請書等個人番号を含む文書の廃棄を行う。
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 ※	自立支援医療費（精神通院）の申請をした者
	その妥当性	保管期間を満了した個人番号を含む申請書類等の廃棄を適切に行う必要があるため。
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　(　　)
⑤委託先名の確認方法		ホームページ「東京都入札情報サービス」にて公表している。
⑥委託先名		株式会社エコ・エイト
再委託	⑦再委託の有無 ※	[　　再委託しない　　]　＜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	
	⑨再委託事項	
委託事項7		Public Medical Hub(PMH)を活用した情報連携に係る各事務における特定個人情報ファイルの一部の取扱
①委託内容		Public Medical Hub(PMH)の利用・情報連携業務及び運用保守業務
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一部]　＜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 ※	自立支援医療費(精神通院)の申請をした者
	その妥当性	Public Medical Hub(PMH)はDX審査支払機構が運用し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。 ただし、PMHに格納された特定個人情報は、自動処理により再委託先に情報連携されるため、国(デジタル庁)は特定個人情報にアクセスすることはない。
③委託先における取扱者数		[　　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
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　(LGWAN又は閉域網回線を用いた提供　　)
⑤委託先名の確認方法		下記、「⑥委託先名」の項の記載より確認できる。
⑥委託先名		DX審査支払機構
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	書面又は電磁的方法による承諾
	⑨再委託事項	〔※既存又は新規の評価書に以下事項の追記・記載〕 ＜Public Medical Hub(PMH)を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・Public Medical Hub(PMH)の運用保守 ・PMHキーの採番 ・PMHキーを介した医療機関システム・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。
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 （ 3 ）件 [○] 移転を行っている （ 1 ）件 [ ] 行っていない
提供先1	区市町村長
①法令上の根拠	番号法第19条第8号
②提供先における用途	災害対策基本法による被災者台帳の作成に関する事務
③提供する情報	被災者に係る障害者の日常生活及び社会生活を総合的に支援するための法律第六条の自立支援給付の支給に関する情報
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	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ
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	区市町村長が災害対策基本法による被災者台帳を作成するに当たり、情報提供ネットワークシステムを通じて特定個人情報の照会があった都度
提供先2～5	
提供先2	道府県知事等
①法令上の根拠	番号法第19条第8号
②提供先における用途	生活保護法による保護の決定及び実施又は徴収金の徴収に関する事務
③提供する情報	要保護者等に係る障害者の日常生活及び社会生活を総合的に支援するための法律第六条の自立支援給付の支給に関する情報
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	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ
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	都道府県知事等が生活保護法による保護の決定及び実施又は徴収金の徴収に当たり、情報提供ネットワークシステムを通じて特定個人情報の照会があった都度
提供先3	道府県知事等
①法令上の根拠	番号法第19条第8号
②提供先における用途	中国残留邦人等支援給付等の支給に関する事務
③提供する情報	要支援者等に係る障害者の日常生活及び社会生活を総合的に支援するための法律第六条の自立支援給付の支給に関する情報
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	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ
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	中国残留邦人等支援給付等の支給に当たり、情報提供ネットワークシステムを通じて特定個人情報の照会があった都度
提供先6～10	
提供先11～15	
提供先16～20	
移転先1	西多摩福祉事務所・島しょ支庁
①法令上の根拠	番号法第19条第8号
②移転先における用途	生活保護法による保護の決定及び実施又は徴収金の徴収に関する事務
③移転する情報	要保護者等に係る障害者の日常生活及び社会生活を総合的に支援するための法律第六条の自立支援給付の支給に関する情報
④移転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移転する情報の対象となる本人の範囲	「Ⅱ　特定個人情報ファイルの概要　2. 基本情報　③対象となる本人の範囲」と同じ
⑥移転方法	[○] 庁内連携システム　　[　　] 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	生活保護法による保護の決定及び実施又は徴収金の徴収に当たり、情報提供ネットワークシステムを通じて特定個人情報の照会があった都度
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 ※		【医療費助成事務システム】 医療費助成事務システムは、CSPが提供するクラウドサービスに東京都クラウドインフラとして必要と考えられる統制機能やセキュリティ設定を適用した「クラウドインフラサービス」基盤上に構築される。 採用するCSPは、AWSとなり、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となる。このため、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おり、主に以下の物理的対策を講じている。 ・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。 ・許可されたアカウント以外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。 ・特定個人情報は、CSP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に保存される。 【申請書類】 申請書類は、収受情報を台帳で管理している。また、キャビネットにて、施錠・保管を行っている。 ＜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】 ①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。 【連携サーバー】 ① 連携サーバーは、サーバー等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバー専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ② 当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。 【媒体】 ・媒体（CD-RW）は施錠できるロッカー等に保存している。 【Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務】 Public Medical Hub（PMH）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または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。 ・DX審査支払機構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。
②保管期間	期間	[5年] ＜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	ー

③消去方法	【医療費助成事務システム】 ・5年間異動のないデータは定期処理により削除することとしている。 ・外部記録媒体内のデータは、職員が消去している。 ・特定個人情報の消去は管理組織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東京都クラウドインフラ管理者及び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。 ・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は、クラウド事業者はNIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄する。 ・既存システムについては、管理組織が委託した開発事業者が既存の環境から東京都クラウドインフラ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。 【申請書類】 ・保存期間を満了した申請書類については、溶解処理により廃棄を行う。 ・なお、廃棄に当たっては、搬送から溶解処理に至るまでの間、職員が立ち会う。 【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・運用を行う事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②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。③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。 【連携サーバー】 ・個別業務システム（事務）及び中間サーバとの間で授受されるデータは、所要の処理完了後又は一定時間経過後に削除される。 ・機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、物理的破壊により、当該データを復元不可能な状態とする。 【＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞】 ・センターに保管されたデータのみ、Public Medical Hub（PMH）を用いて消去することができる。 ・センター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、古いものから順に自動削除される。

7. 備考

―

（別添2）特定個人情報ファイル記録項目

〇精神通院照会　受給者明細
・受給者番号
・入力日
・受給者氏名（カナ）
・受給者氏名（漢字）（氏名履歴）
・受給者性別
・受給者生年月日
・受給者住所（住所履歴）
・受給者電話番号
・保険者（保険履歴）　※要配慮個人情報
・保険種別　※要配慮個人情報
・被保険者証（記号・番号）　※要配慮個人情報
・保健所・申請区分
・公費負担期間（公費負担履歴）
・担当医療機関（適用日）
・交付日
・受給者証出力
・手帳番号
・添付書類
・所得区分
・運用開始日
・重度かつ継続
・患者自己負担限度額
・非課税区分
・医療費助成期間
・障害区分（ICDコード）　※要配慮個人情報
・認定回数
・初回開始日
・資格喪失日
・資格喪失理由
・個人番号
・団体内統合利用

＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務追加の記録項目＞
(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）
　・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（不開示/閲覧停止）
　・その他管理番号・ID等（履歴ID、属性ID）
(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)医療助成資格情報
　・受給者証種別ID
　・受給者証名
　・受給者証ID
　・受給者証券面情報
　・受給者証項目情報
　・表示順番号
　・公費ID
　・区分
　・公費負担者番号
　・公費受給者番号
　・自己負担上限情報（自己負担上限額ID、自己負担上限額種別、負担定義、負担率、金額、回数）
　・有効期間
　・強制失効日
　・医療機関コード
　・指定医療機関情報

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	
自立支援医療費(精神通院)認定事務ファイル	
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	【申請書】 ・障害者総合支援法施行細則に定められた様式を使用している。 ・申請書は、本人以外の申請を認めない形式となっており、本人情報以外の情報の入手を防止している。 【本人確認情報】 ・住民基本台帳ネットワークシステムに提供依頼する対象者データは対象者について使用簿を作成し、内部承認を経た上で、番号系端末を使用して照会を行う。 【庁内連携】 (連携サーバー) ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 (福祉局) ・庁内連携により生活保護関係情報等を取得する際は、対象者について使用簿を作成し、内部承認を経た上で、番号系端末を使用して照会を行う。 【＜Public Medical Hub(PMH)を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置】 ・PMHキーの採番処理時には、Public Medical Hub(PMH)が保有する個人番号及び基本情報(カナ、氏名、生年月日、性別、住所)と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで対象者以外の情報の入手を防止する。(当該機能は、R6年度中に実装予定) ・既存事務において本人確認を行った個人番号を既存システム(各業務システム)からPublic Medical Hub(PMH)に連携し、その本人確認済みの個人番号を医療保険者等向け中間サーバーに連携するが、提供した個人番号は加工することなく返却されるため、対象者以外の情報を入手することはない。
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	【申請書】 ・障害者総合支援法施行細則に定められた様式を使用している。 ・記入要領を充実し、必要最小限の情報の記載となるようにする。 ・マニュアルを整備し、窓口である区市町村に対し周知している。 【本人確認情報】 ・住民基本台帳ネットワークシステムは、本人確認情報のみを保有している。 【庁内連携】 (連携サーバー) ・連携サーバーシステムでは、照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められたものだけについて連携を行う。なお、チェック項目は、番号法等の改正に応じて、更新する。 (福祉局) ・庁内連携により生活保護関係情報等を取得する際は、対象者に係る必要な情報について使用簿を作成し、内部承認を経た上で、番号系端末を使用して照会を行う。 【＜Public Medical Hub(PMH)を活用した情報連携に係る自立支援医療受給者証交付事務＞における追加措置】 ・医療保険者等向け中間サーバーからPublic Medical Hub(PMH)へは、定められたインターフェース仕様に沿って決められたデータ項目(PMHキーと個人番号)のみが返却されるようシステム的に制御している。
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】 ・他県からの転入者の診断書の情報を入手する際には、本人の同意書を取得し行っている。 ・マニュアルを整備し、窓口である区市町村に対し周知している。 【本人確認情報】 ・住民基本台帳ネットワークシステムを所管する総務局が定める利用届により、住民基本台帳法により本人確認情報の利用が認められている旨を申請し、総務局の許可を事前に受けた上で入手を行う。 ・住民基本台帳ネットワークシステムを所管する総務局が定める様式及び方法により、入手を行う。 ・住民基本台帳ネットワークシステムから入手する本人確認情報の対象者については、責任者の承認手続きを経た上で入手する。 【庁内連携】 （連携サーバー） ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 （福祉局） ・.庁内連携により生活保護関係情報等を取得する際は、対象者に係る必要な情報ついて使用簿を作成し、内部承認を経た上で、番号系端末を使用して照会を行う。 ・医療費助成事務システムの操作については、ID単位でアクセス制御を行い、アクセスログを取得し、不正操作を監視する。 【＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞における追加措置】 ・医療保険者等向け中間サーバーからPublic Medical Hub（PMH）へは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステム的に制御している。 ・Public Medical Hub（PMH）のデータベースは、市区町村ごとに論理的に区分されており、他市区町村の領域からは、特定個人情報の入手ができないようにアクセス制御している。
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	
入手の際の本人確認の措置の内容	【申請書】 ・区市町村担当者が、番号法第16条、番号法政令第12条第1項、番号法施行規則第1条等の規定に基づき、個人番号カード等にて本人確認することをマニュアルに掲載し、窓口である区市町村に対し周知している。 【本人確認情報】 ・住民基本台帳を所管する各自治体で本人確認済み。 【庁内連携】 （連携サーバー） ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、団体内統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報照会が可能となるよう制御されている。 （福祉局） ・生活保護関係情報等を取得する際には、対象者の本人確認情報及び個人番号について住民基本台帳ネットワークシステムによる確認の上、番号系端末を使用して照会を行う。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・Public Medical Hub（PMH）が提供した個人番号を加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。

個人番号の真正性確認の措置の内容	【申請書】 ・番号法第16条、番号法政令第12条第1項、番号法施行規則第1条等の規定に基づき、個人番号カード等にて真正性を確認することをマニュアルに掲載し、窓口である区市町村に対し、周知している。 【本人確認情報】 ・住民基本台帳を所管する各自治体で真正性確認済み。 【庁内連携】 （連携サーバー） ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、団体内統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報照会が可能となるよう制御されている。 （福祉局） 生活保護関係情報等を取得する際には、対象者の本人確認情報及び個人番号について住民基本台帳ネットワークシステムによる確認の上、番号系端末を使用して照会を行う。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・Public Medical Hub（PMH）が提供した個人番号を加工することなく返却されるため、本人のものではない誤った個人番号を入手することはない。
特定個人情報の正確性確保の措置の内容	【申請書】 ・都は、医師の記載した診断書の内容と申請内容とが相違ないか確認する。 【本人確認情報】 ・正確性は、住民基本台帳を所管する各自治体が適切に対応している。 【庁内連携】 （連携サーバー） ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報照会が可能となるようアクセス制御されている。 ・情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 （福祉局） ・生活保護関係情報等を取得後、使用簿によって照会結果の確認を行う。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・PMHキーの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで正確性を担保する。（当該機能は、R6年度中に実装予定） ※チェック機能は補助的な機能であり、機能実装までの間においても既に既存事務において、個人番号及び基本情報の正確性は、住基システムとの連携等により担保されている。
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】 ・区市町村からの進達の際に漏えい・紛失しないよう、区市町村の責任において都に受け渡している。 ・マニュアルを整備し、窓口である区市町村に対し台帳管理を行うよう周知する。 ・センター内で受付簿を作成し、地区別保管庫により施錠保管している。 【本人確認情報】 ・入手に係る外部記録媒体は、住民基本台帳ネットワークシステムを所管する総務局が貸し出す物を使用する。 ・対象者に係る照会データを格納した外部記録媒体については、総務局が定める住民基本台帳ネットワークシステムに係る運用規程に基づき暗号化し、安全管理基準に基づき職員が総務局に持ち込む。 ・総務局から入手する本人確認情報を格納した外部記録媒体については、暗号化されている。 【庁内連携】 （連携サーバー） ・ログイン時に利用者の認証を実施する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 ・照会側と提供（回答）側の間で行われる特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・情報連携に用いる機器は、USB機器等に対する制御を行い、外部記録媒体の利用を制限する。 （福祉局） ・番号系端末は執務室内に設置し、操作画面が部外者の目に触れないように配置する。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・Public Medical Hub（PMH）と支払基金の医療保険者等向け中間サーバーは、暗号化された閉域網で接続される。
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

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
【区市町村】 ・「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）」にのっとり、適切に安全管理措置を講じる。 ・申請書類は、「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）」にのっとり、適切に保管する。また、保存期間を経過した場合は速やかに廃棄又は削除する。 ・都に進達する際は、厳重な送付体制のもと、指定された袋を使用し、指定された方法で行う。

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	【連携サーバー】 個人番号に係る共通基盤である連携サーバーは、ユーザIDにより利用者・個別業務システム（事務）等の単位でアクセス可能な範囲を限定し、正当な権限のない利用者・個別業務システム（事務）等からは個人番号を利用できないようアクセス制御を行っている。
事務で使用するその他のシステムにおける措置の内容	・医療費助成事務システムでは、利用者IDによりアクセス可能な業務範囲を限定し、正当な権限のない利用者からは個人番号を利用できないようアクセス制御を行っている。加えて、医療費助成事務システムでは、情報連携のため、個人情報を外部記録媒体に書き出す場合は、二要素認証機能付きの専用端末のみで行えるよう制限する。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・Public Medical Hub（PMH）にアクセスする本市区町村の職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。 ・Public Medical Hub（PMH）では、権限のある者しか個人番号にはアクセスできないように制御している。 ・医療機関システムからは既存の閉域網経由でPublic Medical Hub（PMH）に接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないよう制御している。 ・住民からはインターネットからマイナポータルAPI経由でPublic Medical Hub（PMH）に接続するが、必要な情報のみアクセスでき、個人番号にはアクセスできないように制御している。
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	【医療費助成事務システム】 ・システムセキュリティに係る内規により端末起動時にID・パスワードでのユーザ認証を行うこととしている。 ・IDの有効期限は1年未満で設定することとし、パスワードについては必要に応じて変更するほか、3回以上誤ったパスワードを入力すると該当IDはロックされることとしている。 ・アクセスログが一定期間保管され、誰がいつどの情報を参照・変更等の操作を行ったか把握でき、IDの不適正利用が確認された場合は、当該IDの利用を制限する。 ・ID管理に係る内規に基づき、利用者ID管理簿の定期的な棚卸を実施し、必要最低限の利用者ID付与を行っている。 ・二要素認証情報を用いた管理を行う。 【東京都クラウド】 ・AWS IAMによる個別アカウント管理を実施している。 ・管理者アカウント（特権ユーザー）及び特権ユーザが作成したすべてのユーザに対し、多要素認証（MFA）及び接続元IPアドレス制限している。 ・管理対象サーバへの接続は東京都クラウドが提供する踏み台サーバを経由する。 ・AWS CloudTrailによりAWS API操作を記録するとともに、踏み台サーバのログイン履歴及び操作履歴を記録。なお、東京都クラウドインフラ利用者及び受託者はこれらの設定を変更すること及び収集されたログを変更・削除することはできない。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付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。 ・本市区町村は、Public Medical Hub（PMH）のアクセス権限を管理する管理者を定める。 ・Public Medical Hub（PMH）のログインはユーザID・パスワードで行う。 ・Public Medical Hub（PMH）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。 ・Public Medical Hub（PMH）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Public Medical Hub（PMH）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。

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	【医療費助成事務システム】 ・ID管理に係る内規に基づき、管理を行っている。 ・情報セキュリティ責任者（統括）が年度当初にシステム利用所管にあてた調査を実施し、利用者の異動情報を把握した上で、情報セキュリティ責任者（統括）が権限の付与・削除をID管理簿の加除訂正を行いながら一元管理する。 ・IDは年度末に失権するよう設定しており、調査時に連絡が漏れたり、遅れた場合、IDは失効するよう設定されている。 ・年度途中の権限付与管理は、職員については異動情報、委託先従事者については申請に基づき行っている。 【東京都クラウド】 ・CSPの特権ユーザーは、CSP環境の払出し時に東京都クラウドインフラ管理者が発行する。利用者によるCSPの特権ユーザーの作成・削除・更新は不可。また、CSPの特権ユーザーの削除は、利用者からの東京都クラウドインフラ利用終了の申請（利用終了申請書）に基づき東京都クラウドインフラ管理者が実施する。 ・ 踏み台サーバーのログインユーザーは、東京都クラウドインフラ管理者より、踏み台サーバーの払出し時に提供する。以後の追加・削除・パスワードリセットは、利用者の申請（ユーザー申請（踏み台OS））に基づき東京都クラウドインフラ管理者が実施する。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・Public Medical Hub（PMH）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。 ・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。
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	【医療費助成事務システム】 ・アクセス権限については、情報セキュリティ責任者（統括）が全ての権限を一元的に管理しており、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定している。 ・ID管理簿の定期的な棚卸により、付与する権限に過不足が生じないようにし、どのIDにどのような権限が設定されているのかを把握できるようにしている。 ・IDの不適正利用が確認された場合は、システムセキュリティに係る内規により、当該IDの利用を制限する。 ・IDの一覧表は内部認証手続により、権限設定が適正であることを確認している。 ・IDにより管理に加え、二要素認証を用い、アクセス権限管理を行う。 【東京都クラウド】 ・AWS IAMにより職務に応じた最小権限の原則に基づくアクセス制御を実施している。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・共用IDは発行せず、必ず個人に対し、ユーザーIDを発行する。 ・パスワードの有効期限を設定する。 ・管理者が定期的に管理表を確認し、必要に応じて見直しを行う。
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	【医療費助成事務システム】 ・「医療費助成事務システム情報セキュリティ実施手順」により、アクセスログは一定期間保管することとしている。 ・不正操作の監視を行うとともに、ログ分析についてシステム運用管理業者より月次報告を受け、情報システム管理者が確認している。 ・記録については、改ざん、窃取又は不正な削除の防止のために必要な措置を講じていることを確認している。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・システム上の操作のログを取得し、操作ログを定期的に確認する。

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	・情報資産の取扱いに関する内規において、情報資産の外部持ち出しは禁止している。 ・個人情報の保護に関する法律第69条により、事務外での利用を制限されている。 ・番号法第29条で特定個人情報ファイルの作成が制限されている。また、福祉局特定個人情報等安全管理基準により、事務の遂行上必要な場合を除き、特定個人情報等を複製することを禁止している。 ・これらを担保する手段として、端末での外部記憶媒体の使用を制限すること等により、容易に情報資産の持ち出しができないようにしている。さらにアクセスログによる不正操作の監視を行っている。 ・eーラーニングによる年1回の悉皆研修（福祉局研修「情報セキュリティ・個人情報保護」）を実施している。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・特定個人情報を取り扱う職員に対して、セキュリティに関する研修を行い、個人情報保護の重要性について教育するとともに、業務外での特定個人情報の取扱いの禁止等の指導を徹底することで、事務外の使用を防止している。 ・委託業務については、委託先との契約により、委託業者が従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。本市区町村は、当該教育の実施について履行確認を行う。 ・操作ログの追跡により不正アクセス者の特定が可能であることを周知徹底することで、コンプライアンスの意識を高め、事務外での使用を防止する。
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	・端末からの情報資産の複製・持ち出しは外部媒体の接続を制限している。また、医療費助成事務システムでは、二要素認証機能付きの専用端末においてのみ情報の書き出しを行う。 ・システムセキュリティに係る内規により外部記録媒体に保有情報を書き出す場合は、必ずデータの暗号化又は記録媒体のパスワード設定を行っている。 ・ハードコピー等の紙資料については、取扱いに細心の注意を払うよう、研修等により注意喚起している。 ・アクセスログによる不正操作の監視も行っている。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・既存システム（各業務システム）から特定個人情報を抽出したCSVファイルをPublic Medical Hub（PMH）へ登録する際は、作業を行う職員及び端末を必要最小限に限定する。 ・本市区町村の既存システム（各業務システム）からPublic Medical Hub（PMH）への特定個人情報の連携は、情報漏えいを防止するために暗号化された通信回線（LGWAN又はその他の閉域網回線）を利用した接続のみが認められる。 ・Public Medical Hub（PMH）では、権限のある者しか個人番号にはアクセスできないように制御している。 ・システムにアクセスする職員について、当該職員が所掌する事務以外の情報は閲覧できない仕組みとしている。
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
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	
・個人情報をシステム外に持ち出す場合は、局の内規により、その都度、事前に情報セキュリティ責任者の許可を得ている。また用務終了の都度、速やかに消去している。 ・システム入力データファイル作成処理委託では、入力は検孔含めた二度打ちを行い、正確性を確保している。 ・業務上の必要なく、医療費助成事務システム端末以外のインターネットと接続している端末上に、特定個人情報ファイルを作成・保存することを禁止しており、特定個人情報ファイルは出力の際、全て暗号化している。	

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		【委託事項1、5】 ・従事者名簿、計画書、業務報告書を提出させている。 【委託事項2、4】 ・ともにプライバシーマーク取得事業者である。また、システム運用管理業者はシステムセキュリティに関する内規によりISMS認証取得事業者としている。 【委託事項2～4】 ・契約時に取り交わす仕様書で、責任者、作業体制、連絡体制及び作業場所を書面にして提出、業務従事者への遵守事項の周知、再委託の承諾申請の提出、作業担当者の名簿の提出等を委託先に求めている。 ・委託元が委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認する。 【委託業務2】 媒体を授受する際の双方確認、保管中の確実な施錠、速やかなデータ削除等、実施手順を遵守することを受託者に教育する。 【委託業務6】 ・溶解処理施設への運搬と機密文書の計量は委託者立ち合いの元で行い、溶解処分の証明書類として情報抹消証明書、再生資源管理伝票及び適正に処分した現場写真を提出させている。 ・廃棄委託における都職員の立会いの実施か、立会いに代えて受託者に証明書や写真等を提出させる場合は、写真を撮るポイントを具体的に指定する。 【委託事項7】 Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務における特定個人情報の取扱いをDX審査支払機構に委託することとする。 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）に基づき、委託先の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。
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	【委託事項1～5】 ・作業者を限定するために、委託業務従事者名を書面により提出させている ・開封を禁止する取り決めを業者と交わしている。 【委託事項3、4】 ・委託先が使用するユーザIDは、ID管理に係る内規に基づき、割り当てを行っている。ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。 【委託事項2～4】 ・秘密の保持、目的外使用の禁止、複写及び複製の禁止、作業場所以外への持ち出し禁止、情報の保管及び管理等を規定した仕様書を取り交わし、委託処理に係る必要事項を定めている。 【委託事項6】 機密文書を保管している段ボール箱を開封することなく溶解させている。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・センターではアクセス権限の管理状況を確認できる。 ・アクセス権限を付与する者を必要最小限に限定する。 ・アクセス権限を付与する範囲を必要最小限に限定する。 ・アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再委託先（PMHキー採番や運用保守）のみに付与される。

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	【委託事項1、5】 ・日報にて取扱件数を管理している。 【委託事項2～4】 ・委託先との契約に際して、施錠できる保管庫等での管理、管理状況の記録、管理記録の報告等を規定した仕様書を取り交わし、委託処理に係る必要事項を定めている。 【委託事項4】 ・システム運用管理委託では、システムセキュリティに関する内規によりアクセスログを記録し、一定期間保存しており、誰がデータベース上のどの情報をアクセスし、抽出したかが記録され、不正アクセスを監視している。 ・システム運用管理業者は管理記録を3年間保存し、毎月個人情報の取扱い状況の報告を行うとともに、作業を行った場合は、作業案件・懸案課題管理表により週次で報告を行っている。 【委託事項6】 ・委託者は「委託完了届」、溶解処分に係る証明書類として「情報抹消証明書」、「再生資源管理伝票」(別紙1)及び適正に処分した現場写真等を提出させている。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・特定個人情報の取り扱いのログを保存し、提供を求めることができる。 ※再委託先（PMHキー採番や運用保守）に係る特定個人情報の取扱いログに限られる。
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	【委託事項1～6】 ・委託先から他者への外部提供なし。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・委託先（再委託も含む。）から他者への提供は行わない。 ・センターでは委託契約に基づき、委託先（再委託先も含む。）から他者への提供が行われていないことを確認できる。
	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	【委託事項2～4】 ・受託者は、仕様書により、その内容を遵守する旨記載した誓約書を都に提出することになっている。また、都による監査、点検及び検査に協力している。 【委託事項2】 ・帳票原票の受け渡しは施錠できる専用トランクをセンターから貸与し、運搬することとし、授受の際はセンターから送付書を渡し、納品時は納品書を受領し確認する。 ・帳票の保管は施錠管理とし、複写禁止している。 【委託事項4】 ・オンライン入力若しくはバッチ入力で受け渡された申請データが格納されるDBへのアクセス権限は都から付与されるIDにより設定され、必要最小限に制限されている。 ・本番データの参照・修正は都の指示に基づき行っている。 ・作業状況については週次の定例会で報告を行い確認している。 ・作業は保守拠点に設置する都が貸与した専用端末により実施しており、専用端末が設置された部屋への立ち入りはICカード所持者に限定している。 ・委託先には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記す予定。 【委託事項3】 ・貸与時と納入時に職員が件数をチェックしている。 【委託事項6】 業務の履行に際して取り扱う特定個人情報について、都の特定個人情報保護条例を遵守して取り扱う義務を課し、その秘密保持に厳重な注意を払う旨を仕様書に記載する。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・委託先には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する。 ・センターでは委託契約に基づき、委託先（再委託先も含む。）から契約書で定められた範囲の特定個人情報しか提供されていないことを確認できる。

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	【委託事項1、3、5、6】 ・業務上、消去する事務が発生しない。 【委託事項2】 ・仕様書により、入力に使用した書類の速やかな返却及びデータ消去を求めており、契約仕様書により複写を禁止している。また、データ消去の報告も求めている。 【委託事項4】 ・仕様書により、用務完了後に記録媒体上に含まれる当該委託業務に係る情報を全て消去することが規定されており、担当者・管理者の確認・承認の上作業を行っている。 ・消去した情報項目、数量、消去方法及び消去日等を明示した書面の報告を求めている。 ・消去方法については委託仕様書により定めている。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・委託契約終了後は保管していた全ての特定個人情報を消去する。 ・特定個人情報を紙媒体で保管しない。 ・委託契約書に基づき、消去について、センターは報告を受けることができ、それにより消去状況について確認が可能となる。
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	【委託事項1～6】 ・委託契約書において、「個人情報の保護に関する法律」の規定を遵守し、個人情報の漏洩防止等適正な管理のために必要な体制の確保に万全の措置を講じることが規定されている。 【委託事項2～4】 ・目的外使用の禁止、情報の保管及び管理、再委託の取扱い、実地調査及び指導等について仕様書で規定している。 【委託事項2】 ・契約仕様書にて、作成データの暗号化、物件授受時の送付書・受領書の取交し、センターの貸与する専用トランクでの運搬、複写の禁止等を規定している。 【委託事項4】 委託仕様書にて、オペレーターID管理など適切なアクセス権限管理、データ授受時の送付書・受領書の取交し、都の文書の施錠保管、ウィルス対策、セキュリティ監査協力等を定めている。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ 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

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る　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	【委託事項1、5】 ・契約の中で再委託を禁止している。 【委託事項2～4】 ・再委託は原則として行わない。 ・再委託をする場合は、仕様書により、あらかじめ選定理由、業務管理方法、セキュリティ管理体制等を記載した書面で承諾を得ることになっている。 ・委託先と同様に本特記仕様書の遵守する旨の誓約書を提出させる。 【委託事項6】 ・委託契約時に取り交わす「特定個人情報の取扱いに関する特記事項」により、受託者は、特定個人情報の適正な安全管理が図られていることを都が確認し、都の許諾を得た場合に限り、再委託をすることができることになっている。 【委託事項7】 ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるDX審査支払機構が、再委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、必要であると認めるときには、DX審査支払機構に報告を求めることができる。
その他の措置の内容		【委託事項4】 ・委託業務で使用する電子媒体等の扱いについても都から貸与した媒体を使用することなど委託仕様書により定めている。 【委託事項7】 <Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置> ・PMHキーの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。（当該機能は、R6年度中に実装予定） ・委託契約書に以下の規定を設ける。 委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。 ・委託先からの情報提供を十分に受けられるよう、Teamsによりコミュニケーションを行い、同システムを利用する他の部署とも連携して最新の情報を収集・共有する。
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		
【委託事項2、4】 ・システム入力データファイル作成受託業者、システム運用管理業者ともにプライバシーマーク取得事業者である。 【委託事項4】 ・システム運用管理業者はシステムセキュリティに関する内規によりISMS認証取得事業者としている。 ・本番データの参照・修正は都庁内に設置されている専用の端末により実施している。 ・保守運用で利用する居室への立ち入りはICカード所持者に限定しており、入室に当たり、ICカードに加え、カメラによる監視等、厳重なセキュリティ対策を行っている。 ・年1回の実地確認を実施している。		

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
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	【庁内連携】 （連携サーバー） 全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 （福祉局） ・医療費助成事務システムではアクセスログが一定期間保管され、誰がいつどの情報を参照・変更等の操作を行ったか記録している。
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	【庁内連携】 （連携サーバー） 全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 （福祉局） ・医療費助成事務システムではアクセスログが一定期間保管され、誰がいつどの情報を参照・変更等の操作を行ったか記録している。
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	【庁内連携】 （連携サーバー） ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・全ての照会及び回答について、特定個人情報の照会者、移転者、日時等をシステム上でアクセスログとして記録し、7年間保存する。 （福祉局） ・受給者情報は、番号法に基づき、連携サーバーを経由してのみ中間サーバに副本登録する。
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	【庁内連携】 （連携サーバー） ・照会者、事務、移転者、特定個人情報の項目等のチェック項目に基づき、システムでチェックを行い、正当であると認められ、かつ移転者が明示的に回答を承認した場合に限り、連携を行う。照会に対しては、照会条件として指定された対象者に関する情報だけを回答する。なお、チェック項目は、番号法等の改正に応じて、更新する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバーからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 （医療費助成事務システム） ・受給者証の発行時期に合せ、特定個人情報を提供する仕組みとなっており、システム内で提供状況管理を行い、チェックリストを定期的に出力する。所管課において、チェックリストに基づき、提供情報の適切な反映時期について確認を行う。 ・システムの情報（正本）の正確性確保措置については、システム内でエラーチェックを行い、定期的にエラーチェックリストを出力する。所管課において、エラーチェックリストを確認することにより、提供情報の正確性を確保する。
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	＜中間サーバー・ソフトウェアにおける措置＞ 【中間サーバー・ソフトウェア】 ・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。 ・中間サーバの職員認証・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）番号法の規定によ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に係る情報照会者、情報提供者、事務及び特定個人情報を一覧化し、情報照会の可否を判断するために使用するもの。 （※3）中間サーバ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 【連携サーバー】 ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報照会が可能となるようアクセス制御されている。 ・符号取得においては、あらかじめ各事務のシステムにて登録され、個別業務システム利用番号が割り当てられた状態の対象者のみを受付けるよう制御されている。 ・符号取得に対する回答及び情報照会に対する回答は、当該照会を行った事務に対してのみ返却するよう制御されている。 ・各事務所管部署が個々の照会データを一意に識別できるよう付与した識別子を、連携サーバからの回答データに付記して返却することで、どの照会に対する回答かを各事務所管部署で正確に突合できるようにしている。 【福祉局】 ・情報提供ネットワークにより特定個人情報を取得する際は、対象者について使用簿を作成し、内部承認を経たうえで番号系端末を使用して照会を行う。 【区市町村】 ・「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）」に従って、区市町村が適切に安全管理措置を講じている。
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	＜中間サーバー・ソフトウェアにおける措置＞ 【中間サーバー・ソフトウェア】 ・中間サーバは、特定個人情報保護委員会との協議を経て、内閣総理大臣が設置・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･プラットフォームにおける措置】 ・中間サーバと既存システム、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。 ・中間サーバと団体については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。 【連携サーバー】 ・ログイン時に利用者の認証を実施する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【福祉局】 ・情報提供ネットワークにより特定個人情報を取得する際は、対象者について使用簿を作成し、内部承認を経たうえで、番号系端末を使用して照会を行う。 【区市町村】 ・「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）」に従って、区市町村が適切に安全管理措置を講じている。
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	＜中間サーバー・ソフトウェアにおける措置＞ 【中間サーバー・ソフトウェア】 ・中間サーバは、特定個人情報保護委員会との協議を経て、内閣総理大臣が設置・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。 【連携サーバー】 ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、個別業務システム利用番号が割り当てられていることを前提として、当該人に対する符号取得が可能となるよう制御されている。 ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、団体内統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報照会が可能となるよう制御されている。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【福祉局】 ・特定個人情報を取得する際には、対象者の本人確認情報及び個人番号について住民基本台帳ネットワークシステムによる確認の上、照会を行う。 ・特定個人情報を取得後、使用簿によって照会結果の確認を行う。 【区市町村】 ・「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）」ガイドラインに従って、区市町村が適切に安全管理措置を講じている。
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	＜中間サーバー・ソフトウェアにおける措置＞ 【中間サーバー・ソフトウェア】 ・中間サーバは、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（※）。 ・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。 ・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。 ・中間サーバの職員認証・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・プラットフォーム】 ・中間サーバと既存システム、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。 ・中間サーバと団体については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。 ・中間サーバ・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。 【連携サーバー】 ・ログイン時に利用者の認証を実施する。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 ・システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 【福祉局】 ・番号系端末は執務室内に設置し、操作画面が部外者の目に触れないように配置する。 【区市町村】 ・「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）」に従って、区市町村が適切に安全管理措置を講じている。 ＜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、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。
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	【中間サーバー・ソフトウェア】 ・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。 ・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。 ・機微情報については、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。 ・中間サーバの職員認証・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。 【連携サーバー】 ・ログイン時に利用者の認証を実施する。 ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報提供が可能となるようアクセス制御されている。 ・システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【福祉局】 ・受給者情報は、番号法に基づき、連携サーバーを経由してのみ中間サーバーに副本登録する。 エラー発生時は、エラーデータを修正し、再度登録を行う。 【区市町村】 ・区市町村では提供を行わない。 ＜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。 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機微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。
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	【中間サーバー・ソフトウェア】 ・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。 ・中間サーバの職員認証・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】 ・中間サーバと既存システム、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。 ・中間サーバと団体については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。 ・中間サーバ・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。 【連携サーバー】 ・ログイン時に利用者の認証を実施する。 ・各事務所管部署からの申請に基づき、利用者とその所掌事務の紐付けが連携サーバ上であらかじめ定義され、その範囲においてのみ情報提供が可能となるようアクセス制御されている。 ・システムの利用者、日時等をシステム上でログとして記録し、7年間保存する。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【福祉局】 ・受給者情報は、番号法に基づき、連携サーバーを経由してのみ中間サーバーに副本登録する。 【区市町村】 ・区市町村では提供を行わない。 ＜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事業者及びクラウドサービス事業者においては、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。
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	【中間サーバー・ソフトウェア】 ・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。 ・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。 ・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。 【連携サーバー】 ・各事務所管部署で本人確認及び真正性確認を行った個人番号に基づき、団体内統合利用番号及び個別業務システム利用番号が紐付けられていることを前提として、当該人に対する情報提供が可能となるよう制御されている。 ・個別業務システム（事務）と中間サーバとの間における特定個人情報の授受に当たっては、その中継のみを行い、システム内に特定個人情報（副本相当）は保有しない。 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で、暗号化を行う。 ・中間サーバとの間は、行政情報ネットワーク上で他とは分離された通信を用いるとともに、暗号化を行う。 ・サーバ認証により真正性が担保された中間サーバに接続する。 【福祉局】 （医療費助成事務システム） ・受給者証の発行時期に合せ、特定個人情報を提供する仕組みとなっており、システム内で提供状況管理を行い、チェックリストを定期的に出力する。所管課において、チェックリストに基づき、中間サーバへの提供情報の適切な反映時期について確認を行う。 ・システムの情報（正本）の正確性確保措置については、システム内でエラーチェックを行い、定期的にエラーチェックリストを出力する。所管課において、エラーチェックリストを確認することにより、提供情報の正確性を確保する。 【区市町村】 ・区市町村では提供を行わない。 ＜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、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。 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
【中間サーバー・ソフトウェア】 ・中間サーバの職員認証・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・プラットフォーム】 ・中間サーバと既存システム、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。 ・中間サーバと団体については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。 ・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。 ・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・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事業者及びクラウドサービス事業者における情報漏えい等のリスクを極小化する。

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･プラットフォーム】 ･中間サーバ･プラットフォームをデータセンタに構築し、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。 ･事前に申請し承認されていない物品、記憶媒体、通信機器などを不正に所持し、持出持込することがないよう、警備員などにより確認している。 【連携サーバー】 ･サーバ等を設置するための専用施設内に他のシステムとは分離した区画を設け、当該サーバ専用のラックに施錠して収容する。当該施設では、入退室者管理、区画ごとの施錠管理、監視カメラによる録画、有人監視等を実施する。 ･当該施設の煙感知装置、ガス系消火設備、耐震対応等により、火災や地震に起因する滅失等のリスクを低減する。 ･機器のうち、特定個人情報等のデータが記録されうるものの廃棄等に当たっては、磁気的消去又は物理的破壊等により、当該データを復元不可能な状態とする。 【東京都クラウド】 　医療費助成事務システムは、CSPが提供するクラウドサービスに東京都クラウドインフラとして必要と考えられる統制機能やセキュリティ設定を適用した「クラウドインフラサービス」基盤上に構築される。 　　採用するCSPは、AWSとなり、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となる。このため、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おり、主に以下の物理的対策を講じている。 　　･CSPが管理する物理的に保護されたデータセンター環境（ISMAP登録クラウドサービス）において、論理的に区分された領域にデータを保管する。なお、データセンターにおけるフェンス、監視カメラ、警備員等の物理的セキュリティ対策はCSPの責任範囲で実施する。 　　･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。 【医療費助成事務システム】 執務室及び端末は、以下の対応をしている。 ･執務室いずれも媒体及び紙資料は施錠保管している。 ･端末設置場所は施錠管理するとともに、端末はセキュリティワイヤにより固定し、ワイヤ錠は情報セキュリティ責任者（統括）が一元管理し、施錠保管している。 【申請書類】 ･申請書類は、収受情報を台帳で管理している。また、キャビネットにおいて施錠保管している。 【区市町村】 ･「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）」にのっとり、区市町村の安全管理措置で適切に対応している。 【媒体】 ･媒体（CD-RW）は施錠できるロッカー等に保存している。 ＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ Public Medical Hub（PMH）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または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を利用している。 ＜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

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･プラットフォーム】 ・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。 ・中間サーバー・プラットフォームでは、ウィ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。 ・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。 【連携サーバー】 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントとそれ以外のセグメントの境界にファイアーウォールを導入するとともに、ログを取得する。 ・ウィルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア（OS）及びミドルウェアは、必要に応じてセキュリティパッチを適用する。 ・データベースにデータを暗号化して保存する。 ・データベースに対する操作権限を細分化し、連携サーバ管理者であっても真に必要な場合を除いてはデータにアクセスできないよう制御する。 ・データベースに対するアクセスログを取得する。 ・データベースのバックアップを取得する。 ・あらかじめ登録された機器だけがネットワークに接続できるよう制御する。 ・サーバ及びその管理に用いる機器は、書き出し可能な外部記録媒体を内蔵せず、かつUSB機器等に対する制御を行い、外部記録媒体の利用を制限する。 【医療費助成事務システム】 ・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。 ・許可されたアカウント以外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。 ・入手した特定個人情報を取り込むこととなる医療費助成システムは、専用回線又は閉塞ネットワークとし、外部ネットワークから第三者によるアクセスは不可能である。 ・ファイアーウォールを設置し、許可していない端末やポート番号の通信遮断を行っている。 ・唯一の外部との接触点である外部記録媒体からのウィルス感染に備え、ウィルス対策ソフトを導入している。 ・業務継続及び災害復旧に備えバックアップを取得している。バックアップデータについてもアクセス制御及び暗号化を実施する 【東京都クラウド】 ・個人番号が含まれる領域は独立しており、他のネットワーク系統からアクセスできないように制御している。 ・許可されたアカウント以外は東京都クラウドの基盤制御に関わる機能にアクセスできないように制御している。 ・ファイアウォール、IAM、多要素認証、CloudTrail等によるセキュリティ対策を実施している。 【区市町村】 ・「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）」にのっとり、区市町村の安全管理措置で適切に対応している。 <Public Medic＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ Public Medical Hub（PMH）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または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。 ・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。	

		・論理的に区分された当該団体専用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。 ・DX審査支払機構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、外部からの侵入検知・通知機能を備えている。 ・センターの端末とPublic Medical Hub（PMH）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。 ・センターの端末とPublic Medical Hub（PMH）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。 ＜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。 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。

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	①令和4年5月、東京都現代美術館において、ミュージアムショップ運営の受託事業者スタッフが、展覧会図録を予約した顧客へ一斉に案内メールを送信する際、メールアドレスをBCC欄ではなく、宛先欄に入力して発信した。 ②令和4年5月、技能検定試験に関する通知を外国人技能実習の複数の監理団体に対しメールで送付する際、誤ってメールアドレスをBCC欄ではなく、CC欄に入力し、一斉送信した。 ③令和4年5月、就学支援金事務において、就学支援金の基礎データをCD-Rに情報を保存し、対象高等学校等宛て一斉に送付したところ、そのうち1校に、他校の受給者に関する情報が含まれていることが判明した。 ④令和4年5月、受託事業者が、事業に関するイベントを案内するメールマガジンを送付する際、配信プログラム改修ミスにより、宛先欄に複数のメールアドレスが入力され、送信された。 ⑤令和4年10月、東京都陽性者登録センターの運営受託事業者が、医療機関で新型コロナウイルス陽性の診断を受け、センターに登録申請を行った複数の患者への登録完了メールを、送付先アドレスが全て入れ替わったまま送信した。 ⑥令和4年12月、労働力調査の統計調査員に対して連絡事項をメールした際、BCC欄に入力して送るべきところを宛先欄に入力し、一斉送信した。 ⑦令和5年4月、再委託先の派遣会社職員が、業務で使用するシステムを不適切に使用し、個人情報を閲覧、メモにとり自宅に持ち出した。 ⑧令和5年5月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑨令和5年6月、施設から転院する患者に診断資料を渡した際、別の患者の検査資料を含めて交付した。 ⑩令和5年7月、施設を退所する患者に関して、退所先候補の施設と受入調整を行うため、診療関係書類をFAX送信した際、誤って別のFAX番号宛てに送信した。 ⑪令和5年8月、申請により受け付けた申請書が紛失していることが発覚した。 ⑫令和5年9月、関係施設宛に都民情報をFAX送信した際、誤って別の事業者宛てに送信した。 ⑬令和5年9月、事業の対象者に案内チラシを郵送した際、送付対象者の抽出ツールのプログラム仕様の不備により、誤って事業対象外の方に送付したことで、旧住所宛てに送付し返戻されなかったものが誤送付となった。 ⑭令和5年9月、決定通知書に公印を押印する目的で本庁に出張し、押印後持ち帰ったが、発送の準備をしていた際に、通知書1枚が紛失していることが発覚した。 ⑮令和6年1月、患者A宛てに送付すべき利用者情報を、誤ってB宛てに送付した。 ⑯令和6年1月、入所者の診療関係ファイルが紛失していることが発覚し、その後、退所者の荷物の中に当該ファイルが混入していたことが発覚した。 ⑰令和6年2月、児童相談所の職員が、出張中に個人情報が記載されている手帳を紛失し、あわせて手帳に収納されていた、当該職員の証票及び所内職員の緊急連絡網を紛失した。 ⑱令和6年2月、施設を退所した患者Aに関する薬剤情報等を記載した書類を、誤って別の患者の退院時の荷物に混入させ交付した。 ⑲令和6年2月、オンライン研修で使用した映像において、患者の情報をマスキング処理していたところ、当該映像をスマートフォンで視聴した場合に、マスキングが外れ、個人が特定できる状態になっていたことが判明した。 ⑳令和6年4月、受け付けた申請書を紛失していることが発覚した。 ㉑令和6年4月、施設職員が、利用者の通院付添の際、処方箋を紛失した。 ㉒令和6年4月、指定管理者が、事業者に対してExcel資料をメールで送信した際、本来削除すべきだった個人情報の入力されたシートを削除しなかった。 ㉓令和6年7月、受託事業者が、都へ交付すべき納入済通知書を、誤って他の事業者宛てに交付したことが発覚した。 ㉔令和6年7月、受託事業者がイベントを行った際の申込時の個人情報が掲載されたウェブページが、一時外部からアクセス可能な状態となっていたことが発覚した。 ㉕令和6年7月、職員が、説明会の資料の中に個人情報が含まれていることに気が付かずに、各自治体にデータを配布した。 ㉖令和6年7月、職員が、A宛てに送付すべき個人情報を、誤ってB宛てに送付していたことが発覚した。 ㉗令和6年7月、受託事業者から送付した個人情報を含む資料が、紛失していることが発覚した。 ㉘令和6年7月、受け付けた申請書を紛失していることが発覚した。 ㉙令和6年8月、受託事業者が配付した資料の中に、個人情報等が含まれる資料が混入していたことが発覚した。 ㉚令和6年10月、職員が、受託者に資料をメールで送信した際、誤って個人情報が記載された別のファイルを添付した。 ㉛令和6年10月、受託事業者が、A宛てに送付すべき電話記録を、誤ってB宛てにFAXで送信した。 ㉜令和6年11月、受け付けた申請書を紛失していることが発覚した（後日発見）。 ㉝令和6年11月、令和3年頃に個人情報が記載された資料を紛失していたことが発覚した。 ㉞令和6年12月、受託事業者が、個人情報が記載された資料を、誤って外部へ送信した。 ㉟令和7年1月、受託事業者が、個人情報が記載された資料を、誤って期限前に廃棄した。 ㊱令和7年1月、受け付けた届出書が、誤って机ごと廃棄されていることが発覚した。	

		①（1）ミュージアムショップにおいて、本社セキュリティインシデント統括部と連携して、個人情報取り扱い、情報管理体制の改善を行う。 （2）特に複数人へのメール送信に際してはダブルチェックを徹底する。 （3）現代美術館全委託業者に、適切な個人情報等の取扱い及び情報管理を徹底するよう指示する。 （4）財団が管理運営する各施設にも本事案を共有し、個人情報を含む情報の適切な管理を徹底する。 ②（1）個人情報の取扱い及び情報管理の徹底等について周知するとともに、職員全員に臨時研修を速やかに実施 （2）誤送信防止に向けたシステムの導入（ダイアログの自動表示など） （3）複数人チェックなど基本的対策の徹底 ③チェック機能を再検証し、全日制等と同様の仕組みを通信制にも直ちに導入するほか、事務フローの再構築を行い、再発防止に努める。そのうえで、本件を財団内で広く共有させ、個人情報の取扱い全般についてハード・ソフトの両面から厳しく見直すとともに、職員の意識向上を図っていく。また、都の実施機関においても個人情報の適正管理とサイバーセキュリティー対策について改めて確認を行う。 ④（1）システムの改善 メールマガジンの配信は、これまで「TO」により自動で1件ずつ送信がされる仕組みであったが、一括メール送信においては送信者アドレスを全て「BCC」に入れるようシステム改修を行う。 （2）システム会社における確認体制の強化 開発前にシステム会社が実施する、影響調査・テスト内容等について、これまでの2名体制によるダブルチェックから、システム会社のプロジェクトマネージャーも加えることとし、確認した内容を報告させて承認する運用へ見直す。 （3）受託事業者における確認体制の強化 システム会社のテスト結果の確認にあたっては、テストの証跡情報の提出を求め、内容の確認を行うとともに、受託事業者での運用テストでは要件定義とも照らした確認を担当だけでなく管理職も実施することにより徹底する。 ⑤受託事業者に対して厳正に指導し、登録完了メール送信作業のチェック体制を強化させる。 ⑥（1）部コンプライアンス推進委員会の臨時開催 ・メール送信時のダブルチェックを徹底させるため、個人情報等の取扱いに係るチェックリストの全職員での点検により注意を喚起、情報管理を再徹底する。 ・あわせて、最近の事故事案の事例を周知するなど、事故の再発予防を進める。 （2）定期的な事故防止意識の醸成 統計調査員を含む全職員を対象に、各所属長や指導員から情報セキュリティや感染拡大防止等に関する指導を定期・継続的に行い、危機意識の醸成等を図る。 ⑦委託先における個人情報の閲覧・使用に当たっての権限の設定や、不適切な閲覧・使用・持ち出しを防止するための体制についてあらためて確認し、適切な運用を徹底させる。 ⑧（1）情報共有をしているホワイトボードの位置、記入欄が分かりにくいとの意見が出 ため、位置、記入方法について変更した。 （2）書類封入時のチェック手順中に、患者氏名の確認を明示した。 （3）2者確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし

	再発防止策の内容	(3)と看確認を徹底するため、事務員のみでなく看護職員もチェックを行うこととし、 2者チェックが終わった段階で封書のチェックボックスに記載する。 (4)責任の所在を明確にするため「転院時退所セット確認書」を新たに作成し、チェックを行った職員が記名する。 ⑨(1)チェックリストを活用し、複数人、複数回のチェックを行うとともに、最終チェック者を統括責任者とすることで、誤封入等を防ぐ体制を整える。 (2)都職員が施設へ直接出向き、個人情報管理の実態確認を実施するとともに、対応が不十分な場合は是正指導を行う。 (3)個人情報保護の研修を実施し、施設全体で個人情報保護の取り組み状況を共有した上で、改善を徹底する。 ⑩(1)委託先に対し、個人情報に関する業務手順を見直し及び徹底を図ることや、全従事者に対する個人情報保護研修を行うことを指導した。また、改善策の確認のため、都が施設へ出向き、個人情報管理の実態を確認した。 (2)再委託先において、送付の際は、まずFAX以外の手段を調整し、止むを得ずFAXを使用する際には、FAX番号の聞き取りの際の復唱や、FAX送信前の送信先への番号の再確認、複数人で複数回のチェックを必ず行うこととした。また、全従業者に対する個人情報保護研修を行った。 ⑪(1)作業環境等を見直し、書類の混入等が起きにくい環境を整備 ①執務室内の作業スペースの確保及び活用 ②引き出し付きの棚をキャビネット内に新設し、書類の分類をよりしやすくした。 (2)委託業者との書類の受け渡し方法の変更(送付する判定機関ごとに数を確認しながら受け渡す)。 ⑫個人情報をFAX送信することを禁止するよう各施設に通知した。 ⑬抽出ツールのプログラム確認は、委託先事業者の運用チームのみが行っていたが、抽出ツールを作成・利用する際には、運用チームに加えて、開発チームと委託元である都の3者で抽出ツールのプログラムの仕様・設定を確認することとした。 ⑭個人情報の持出、返却確認及び受け渡しの際の確認の徹底を行う。また、作業工程等を点検し、作業方法やチェック方法等ミスが起きにくい方法を検討、実施する。 ⑮郵便の発送作業は複数職員でチェックすることを再徹底。また、特に慎重を要する個人情報を取り扱う施設における個人情報の事故の重大性について改めて周知するとともに、書類の発送、保管、業務の進行管理等について、注意喚起や指導を行った。 ⑯(1)ファイルが他の物に紛れてしまわないよう、目立つ色に変更する。 (2)作業スペースに仕切りを立てて、使用スペースを物理的に限定する。 (3)ファイルに記載する名前をイニシャルに表記変更する等、使用する情報から個人情報を削除する。 (4)決まった時間に決まった人員が所在を確認する。 (5)チェックの時間を定刻とし、声をかけ合う。 (6)出したらしまうといった基本的事項を、改めて徹底するよう、注意喚起する。 (7)急いでいたり、忙しい時間帯でも、ダブルチェックをするよう、改めて徹底する。また、退所時にも荷物を確認してから渡すようにする ⑰(個人情報の管理について)

		⑰（個人情報の管理について） （1）相談援助業務上の記録をノート等に記載する場合は、イニシャルを使用するなど個人情報を特定されないようにすること。また、私物のノートや手帳に個人情報を記載しないこと。 （2）庁舎外での会議等に出席した際には、個人端末を活用して記録の作成を行うとともに、作成した文書は暗号化し保存すること。 （3）業務上やむを得ず個人情報が記録された書類を庁舎外に持ち出す場合は、局の保有個人情報安全管理基準に基づき管理職の許可を得ること。 （4）個人情報を含む書類を持ち出すにあたっては、盗難や紛失を防止できる形状・機能を持つ鞄に収納し、肌身離さず持ち運ぶなど十分に注意すること。 （5）その他個人情報の取り扱いについては、局の保有個人情報安全管理基準等を遵守し、適正に行うこと。 （職員の証票の管理について） （1）月1回、各職員の保有状況を点検すること （2）携行する際には、ストラップ付きのケースに収納するなど、常に身体から離さずに携行することを徹底すること （職員の緊急連絡網の管理について） （1）必要な連絡先は公用携帯に保存し、連絡網を記載した紙は庁舎外に持ち出さないこと。 ⑱（1）入所時や退所時の手順確認のチェックリスト様式を変更し、入所時の写真撮影やリストへの正確な情報記載、退所時の荷物確認の手順など守るべきルールを追記するとともに、実施者を記載する欄を追加。 （2）個人情報紛失判明時の、本部への速やかな報告や具体的な捜索の手順などを、チェックリストに追記。 （3）毎朝のミーティングにてリーダー看護師等に個人情報保護の重要性やルールの順守を徹底。勤務者には、業務実施前に最新のマニュアルを確認するよう指導。 ⑲（1）発表資料の事前確認の徹底について幹部会で決定し、各部署に注意喚起 （2）録画や写真撮影をして保管していない旨を書面で確認 （3）画像等の個人情報の収集・利用に関する同意手続きの見直し ⑳（1）電子申請を推奨して紙文書の紛失リスクを軽減 （2）個人情報の適切な管理を職員に改めて周知徹底 ㉑（1）病院へ持ち運ぶファイルに、処方箋を収納する専用スペースを作る （2）医療機関受診時に係るマニュアルを作成 （3）帰園後は可能な限り速やかに所管部署に処方箋等を提出する （4）重要な個人情報を預かっている状況での裁断作業を避ける （5）上記対応について、ミーティング等で周知徹底、注意喚起 ㉒（1）必要なデータファイルのみを送信用データとしてPDF化し、送信前に、PDFに不要な箇所が入っていないことを確認の上、送信することを徹底 （2）メールシステム上、外部送信時に必須である上長の承認の際、個人情報が含まれていないか等の確認を徹底
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	生存者のデータと同様に保管している。
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： 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	受給者証の更新は1年毎であり、年度途中の変更申請であっても、申請書へのマイナンバー記載が必要であるため情報は常に更新されている。	
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	申請書類等が、文書管理に関する規程等によって定められている保管期間を経過した場合には、特定個人情報の適正な取扱いに関するガイドライン等の関係法令に則った安全措置を講じ溶解処理により廃棄する。	
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		

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	【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。 【医療費助成事務システム】 個人情報保護については、全職員が職員向けの自己点検表を用いてチェックを実施。情報セキュリティについては、情報セキュリティ責任者（統括）が点検表を用いてチェックを実施。評価書の記載内容どおりの運用ができているか、年1回担当部署でチェックを実施。	
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	【医療費助成事務システム】 ・外部監査：外部専門機関による医療費助成事務システムの情報セキュリティ監査を実施。監査対象は運用受託業者、管理担当職員、入力担当職員とし、物理的、人的、技術的の各方向からシステムの情報セキュリティについて網羅的な監査を行っている。直近実施時に指摘されたリスク（いずれも軽微なリスク）について、すべてシステムのセキュリティ対策に反映している。今後も定期的に監査を行っていく。また、内部監査人による監査を4年に一度実施している。 【東京都クラウド】 デジタルサービス局が定める監査要綱に基づき、セキュリティ監査を実施しています。 実施サイクルは、内部監査を2年に1回、外部監査を5年に1回として計画しています。 【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・プラットフォームについて、定期的に監査を行うこととしている。 ②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	【職員（非常勤含む。）】 全職員を対象に情報セキュリティ・特定個人情報保護の研修（特定個人情報含む）を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない）年1回 ・新規採用職員や他局転入職員等を対象とした研修 ・未受講者が出ないように端末のない職員に紙でeラーニング研修の実施を行い、結果の報告を受けることとしている。 ・具体的な手順や体制について、都職員へ周知徹底する。 【委託事業者】 ・業務開始に当たり、個人情報の取扱いルールを順守することを確認させている。 【中間サーバー･プラットフォームにおける措置】 IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、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、運用規則（接続運用規定等）や、情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。	

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管理（入退室管理等）、ITリテラシ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。

【特定個人情報の適切な取扱いについて、継続的な改善を実施するための仕組み】
【評価対象の事務における事務責任者等の関与の仕組み】
【特定個人情報保護評価を適切医実施するために整備している体制】
【特定個人情報の漏えい事案等が発生した場合の対応】

＜Public Medical Hub（PMH）を活用した情報連携に係る事務における追加措置＞
　情報セキュリティポリシーや特定個人情報の適正な取扱いに関するガイドライン等に基づき適切に当該システムを利用し、万が一、障害や情報漏えいが生じた場合、適切な対応をとることができる体制を構築する。

＜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活用することにより、設備環境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による高レベルのセキュリティ管理（入退室管理等）、ITリテラシ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。

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	東京都立中部総合精神保健福祉センター事務室自立支援医療担当 〒156－0057　東京都世田谷区上北沢2－1－7
②請求方法	指定様式による書面の提出により開示・訂正・利用停止請求を受け付ける。
特記事項	請求方法等について東京都公式ホームページ上で表示
③手数料等	[　　有料　　]　＜選択肢＞ 1) 有料　2) 無料 （手数料額、納付方法：納付書により、実費相当分（10円/枚）の手数料を納付する。　　）
④個人情報ファイル簿の公表	[　行っていない　]　＜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	
公表場所	
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	東京都立中部総合精神保健福祉センター事務室自立支援医療担当 〒156－0057　東京都世田谷区上北沢2－1－7
②対応方法	問合せの受付時に受付表を起票し、対応について記録を残す。

Ⅵ　評価実施手続

1. 基礎項目評価	
①実施日	令和7年12月26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	東京都ホームページにおいて意見募集の掲載及び窓口での閲覧（東京都庁第一本庁舎3階都民情報ルーム）を行い、電子メール、FAX,郵送にて意見を受け付ける。
②実施日・期間	令和7年8月15日から9月16日の33日間
③期間を短縮する特段の理由	
④主な意見の内容	意見なし
⑤評価書への反映	なし
3. 第三者点検	
①実施日	令和7年9月22日から同年11月6日まで
②方法	東京都情報公開・個人情報保護審査会、特定個人情報保護評価部会において点検を受けた。
③結果	以下の答申を受けた。 自立支援医療受給者証（精神通院）の交付に関する事務（以下「本件事務」という。）における特定個人情報ファイルの取扱いについては、個人のプライバシー等の権利利益に与える影響を予測した上で、特定個人情報の漏えいその他の事態の発生に関して考慮すべきリスクを分析し、リスクを軽減するための適切な措置をおおむね講じていると認められる。
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
平成29年2月10日	評価書及び評価書番号	6　自立支援医療受給者証（精神通院）の交付に関する事務→重点項目評価書	6　自立支援医療受給者証（精神通院）の交付に関する事務【法定・都単独事業】→全項目評価書	事前	事務内容が同一のため。
平成29年2月10日	表紙 評価書名	自立支援医療受給者証（精神通院）の交付に関する事務に係る重点項目評価書	自立支援医療受給者証（精神通院）の交付に関する事務に係る重点項目評価書【法定・都単独	事前	事務内容が同一のため。
平成29年2月10日	Ⅰ基本情報 1．特定個人情報ファイルを取	・障害者総合支援法に基づき、精神疾患のために継続的に通院による治療を受ける必要がある	・障害者総合支援法及び障害者総合支援法施行細則に基づき、精神疾患のために継続的に通院	事前	法定と都単独事業を合わせたため。
平成29年2月10日	Ⅰ基本情報 2．特定個人情報ファイルを取	システム1 ①システムの名称	システム1 ①システムの名称	事前	事務内容を具体的に記載したため。
平成29年2月10日	Ⅰ基本情報 4．特定個人情報ファイルを取	記載なし	①自立支援医療受給者証（精神通院）の交付に関する事務を適切に行うために、最新かつ正確	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	基本情報 5．個人番号の利用	法定分のみ	都単独事業分、区市町村の追加	事前	法定と都単独事業を合わせたため。
平成29年2月10日	基本情報 6．情報提供ネットワークシス	法定分のみ	都単独事業分、区市町村の追加	事前	法定と都単独事業を合わせたため。
平成29年2月10日	基本情報 8．他の評価実施機関	記載なし	東京都内各区市町村長	事前	基礎項目評価書の記載とあわせたため。
平成29年2月10日	（別添1）事務内容	参考資料添付	別添1に移動	事前	全項目評価に変更したため。
平成29年2月10日	Ⅱファイルの概要 3．特定個人情報の入手・使用	○評価実施機関内の他部署 総務局（住民基本台帳ネットワークシステム）	○本人又は本人の代理人 ○評価実施機関内の他部署	事前	外部機関への情報照会の事務に加え、庁内連携による情報
平成29年2月10日	Ⅱファイルの概要 3．特定個人情報の入手・使用	紙 電子記録媒体	紙 電子記録媒体	事前	外部機関への情報照会の事務に加え、庁内連携による情報
平成29年2月10日	Ⅱファイルの概要 3．特定個人情報の入手・使用	記載なし	区市町村が個人番号及び所得区分の確認ができず進達した場合等必要に応じて、入手する。	事前	外部機関への情報照会の事務に加え、庁内連携による情報
平成29年2月10日	Ⅱファイルの概要 3．特定個人情報の入手・使用	記載なし	・申請書類：「障害者の日常生活及び社会生活を総合的に支援するための法律」、「障害者の日常	事前	外部機関への情報照会の事務に加え、庁内連携による情報
平成29年2月10日	Ⅱファイルの概要 3．特定個人情報の入手・使用	記載なし	【法定】 障害者の日常生活及び社会生活を総合的に支	事前	外部機関への情報照会の事務に加え、庁内連携による情報
平成29年2月10日	Ⅱファイルの概要 3．特定個人情報の入手・使用	東京都立中部総合精神保健福祉センター広報援助課医療審査係	東京都立中部総合精神保健福祉センター事務室自立支援医療担当	事前	組織改正による名称変更等のため。
平成29年2月10日	Ⅱファイルの概要 3．特定個人情報の入手・使用	○情報の突合 生活保護・社会福祉関係情報・医療保険関係情	○情報の突合 生活保護・社会福祉関係情報と申告情報を突合	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	Ⅱファイルの概要 4．特定個人情報ファイルの取	②④⑤記載なし	②取扱いを委託する特定個人情報ファイルの範囲	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	Ⅱファイルの概要 4．特定個人情報ファイルの取	②④⑤記載なし	②取扱いを委託する特定個人情報ファイルの範囲	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	Ⅱファイルの概要 4．特定個人情報ファイルの取	②④⑤記載なし	②取扱いを委託する特定個人情報ファイルの範囲	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	Ⅱファイルの概要 4．特定個人情報ファイルの取	②④⑤記載なし	②取扱いを委託する特定個人情報ファイルの範囲	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	Ⅱファイルの概要 5．特定個人情報の提供・移転	市町村長	区市町村長	事前	具体的に記載するため。
平成29年2月10日	Ⅱファイルの概要 5．特定個人情報の提供・移転	情報提供ネットワークシステムを通じて特定個人情報の照会があった都度	区市町村長が災害対策基本法による被災者台帳を作成するに当たり、情報提供ネットワークシ	事前	具体的に記載するため。
平成29年2月10日	Ⅱファイルの概要 6．特定個人情報の保管・消去	【特定個人情報ファイル】 【団体内統合利用番号連携サーバ】	【医療費助成事務システム】 【連携サーバー】	事前	文言の修正。
平成29年2月10日	Ⅱファイルの概要 6．特定個人情報の保管・消去	記載なし	5年	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	Ⅱファイルの概要 6．特定個人情報の保管・消去	記載なし	【医療費助成事務システム】 【申請書類】	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10日	（別添2）特定個人情報ファイル記録項目	・保険所・申請区分	・保健所・申請区分 ・提供済フラグ	事前	漢字の修正
平成29年2月10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	庁内連携に関する記載なし	【庁内連携】 （連携サーバー）	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	庁内連携に関する記載なし	【庁内連携】 （連携サーバー）	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	庁内連携に関する記載なし	【庁内連携】 （連携サーバー）	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	庁内連携に関する記載なし	【庁内連携】 （連携サーバー）	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	庁内連携に関する記載なし	【庁内連携】 （連携サーバー）	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	庁内連携に関する記載なし	【庁内連携】 （連携サーバー）	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	庁内連携に関する記載なし	【庁内連携】 （連携サーバー）	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	記載なし	【区市町村】 ・国のガイドラインにのっとり、適切に安全管理措	事前	区市町村における措置を追加
平成29年2月10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	・個人番号に係る共通基盤（団体内統合利用番号連携サーバー）は、利用者・個別業務システム	【連携サーバー】 個人番号に係る共通基盤である連携サーバー	事前	連携サーバにおける管理方法の詳細を追加。
平成29年2月10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	・医療費助成事務システムでは、利用者IDによりアクセス可能な業務範囲を限定し、正当な権限	・医療費助成事務システムでは、利用者IDによりアクセス可能な業務範囲を限定し、正当な権限	事前	二要素認証機能追加による追加。
平成29年2月10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	二要素認証機能に関する記載なし。	・上記に加えて、次期医療費助成事務システムでは、二要素認証情報を用いた管理を行う。	事前	二要素認証機能追加による追加。
平成29年2月10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	二要素認証機能に関する記載なし。	・次期医療費助成事務システムでは、IDにより管理に加え、二要素認証を用い、アクセス権限管	事前	二要素認証機能追加による追加。
平成29年2月10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	・データベース内の特定個人情報ファイルは、端末で閲覧のみが可能となっており、端末では、外	・端末からの情報資産の複製・持ち出しは外部媒体の接続を制限し、個人情報の外部出力はセ	事前	二要素認証機能追加による追加。
平成29年2月10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	・個人情報をシステム外に持ち出す場合は、その都度、事前に情報セキュリティ責任者の許可を要	・個人情報をシステム外に持ち出す場合は、局の内規により、その都度、事前に管理者の許可を	事前	文言の修正。
平成29年2月10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	【委託事項2～4】 ・委託先の秘密の保持、目的外使用の禁止、複	【委託事項2～4】 ・秘密の保持、目的外使用の禁止、複写及び複	事前	文言の修正。
平成29年2月10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	【委託事項4】 二要素認証機能に関する記載なし。	【委託事項4】 ・次期医療費助成事務システムではサーバ機器	事前	二要素認証機能追加による追加。
平成29年2月10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	【委託事項1】 ・委託契約書において、「東京都個人情報の保護	【委託事項1、4】 ・委託契約書において、「東京都個人情報の保護	事前	委託事項4の追加。
平成29年2月10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	【委託事項2～4】 ・仕様書により、再委託を行う場合はあらかじめ	【委託事項2～4】 ・再委託は原則として行わない。	事前	文言の修正。
平成29年2月10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	【委託事項2、4】 次期医療費助成事務システムに関する記載な	【委託事項2、4】 ・次期医療費助成事務システムではサーバ機器	事前	次期医療費助成事務システムについて追加。
平成29年2月10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	記載なし	記載	事前	庁内連携を追加したため。
平成29年2月10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	記載なし	記載	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	記載なし	記載	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10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	平成27年度発生分の重大事故について記載なし	②返戻した書類の再提出ルール及び届出書類の管理（返戻受理後14日以内の再提出厳守及	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	平成27年度発生分の重大事故について記載なし	②返戻した書類の再提出ルール及び届出書類の管理（返戻受理後14日以内の再提出厳守及	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10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	記載なし	生存者に関する情報と同様に保管管理している。	事前	全項目評価に変更したことによる記載事項の追加。
平成29年2月10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	記載なし	【連携サーバー】 ・個別業務システム（事務）及び中間サーバとの	事前	外部機関への情報照会の事務及び庁内連携による情報照会
平成29年2月10日	Ⅳその他のリスク対策 1．監査	【医療費助成システム】 ・外部監査：外部専門機関による医療費助成事	【医療費助成事務システム】 ・外部監査：外部専門機関による医療費助成事	事前	文言の修正。
令和2年7月6日	5.個人番号の利用 法令上の根拠	【法定】 番号法第9条第1項　別表　第一の84の項　内閣	【法定】 番号法第9条第1項　別表　第一の84の項　内閣	事前	
令和2年7月6日	6.情報提供ネットワークシステムによる情報連携	【法定】 番号法第19条第7号　別表　第二の26、56の2、	【法定】 番号法第19条第6号　別表　第二の26、56の2、	事前	
令和2年7月6日	Ⅱ ファイルの概要 ④入手に係る妥当性	・申請書類：「障害者の日常生活及び社会生活を総合的に支援するための法律」、「障害者の日常	・申請書類：「障害者の日常生活及び社会生活を総合的に支援するための法律」、「障害者の日常		
令和2年9月24日	（別添1）事務内容	③東京都立中部総合精神保健福祉センター（以下、「センター」という。）に進達を行う。	③東京都立中部総合精神保健福祉センター（以下、「センター」という。）に進達を行う。	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2年10月28日	Ⅰ2.システム3①システムの名称	団体内統合利用番号連携サーバ	団体内統合利用番号連携サーバー（以下「連携サーバ」という。）	事前	
令和2年10月28日	（別添1）事務内容		フロー図修正	事前	
令和2年10月28日	（別添1）事務内容	㉓（1→2→3→4→3→2→1）外部記録媒体を使用し、情報提供ネットワークシステムと連携する（平	㉓-1情報提供ネットワークシステムと連携する。（医療費助成事務システムへの入力。）	事前	
令和2年10月28日	（別添1）事務内容	㉖（1→2→3→4→3→2→1）住基への照会件数が多い場合は、外部記録媒体を利用し、住民基	㉖住基への照会件数が多い場合は、一部外部記録媒体を利用し、都庁（総務局行政部）にて住	事前	
令和2年10月28日	Ⅱ2．2基本情報 ④主な記録項目	・記載なし ・生活保護・社会福祉関係情報：受給者の所得	年金関係情報に「○」 ・生活保護・社会福祉関係・年金関係情報：受給	事前	
令和2年10月28日	Ⅱ3④入手に係る妥当性	「市町村における東京都の事務処理の特例に関する条例に　基づき市町村が処理する事務の範	（予定）を削除	事前	
令和2年10月28日	（別添2）ファイル記録項目	保険者（保険履歴）、保険種別、被保険者証（記号・番号）、・障害区分（ICDコード）、個人番号、	末尾に「※要配慮個人情報」を追記	事前	
令和2年10月28日	Ⅲ2リスク1	【本人確認情報】 ・住民基本台帳ネットワークシステムに提供依頼	【本人確認情報】 ・住民基本台帳ネットワークシステムに提供依頼	事前	
令和2年10月28日	Ⅲ	連携サーバー端末	番号系端末（以下、8か所）	事前	
令和2年10月28日	Ⅲ	次期医療費助成事務システム	医療費助成事務システム（以下、2か所）	事前	
令和2年10月28日	Ⅲ3．特定個人情報の入手・使用リスク3		「リスク3従業者が事務外で使用するリスク」で以下を追記	事前	
令和2年10月28日	Ⅲ7特定個人情報の入手・使用⑨		「その内容」を時点更新	事前	
令和2年10月28日	Ⅳその他のリスク対策 1②監査　具体的な内容	・・・今後も定期的に監査を行っていく。	今後も定期的に監査を行っていく予定である。	事前	
令和2年10月28日	Ⅳその他のリスク対策 2具体的な方法	全職員を対象に情報セキュリティ・個人情報保護の研修を実施している。	全職員を対象に情報セキュリティ・個人情報保護の研修（特定個人情報含む）を実施している。	事前	
令和2年10月28日	Ⅳその他のリスク対策 2具体的な方法	記載無し	・未受講者が出ないように端末のない職員に紙	事前	
令和2年11月10日	Ⅰ.基本情報 2．特定個人情報ファイルを取	記載無し	①システム名称　中間サーバ ②システムの機能	事前	
令和2年11月10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	国のガイドライン	「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・地方公共団体等編）」（以下、6	事前	
令和2年11月10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	・「医療費助成事務システム情報セキュリティ実施手順」により、アクセスログは一定期間保管す	・「医療費助成事務システム情報セキュリティ実施手順」により、アクセスログは一定期間保管す	事前	
令和2年11月10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	【中間サーバ・プラットフォーム】 ・中間サーバ・プラットフォームをデータセンタに	【中間サーバ・プラットフォーム】 ・中間サーバ・プラットフォームをデータセンタに	事前	
令和3年9月1日	Ⅰ6.①法令上の根拠	【法定】 番号法第19条第7号　別表　第二の26、56の2、	【法定】 番号法第19条第8号　別表　第二の26、56の2、	事前	
令和3年9月1日	Ⅱ5．提供先1①法令上の根拠	番号法第19条第7号別表第二第26項	番号法第19条第8号別表第二第26項	事前	
令和3年9月1日	Ⅱ5．提供先2①法令上の根拠	番号法第19条第7号別表第二第26項	番号法第19条第8号別表第二第26項	事前	
令和3年9月1日	Ⅱ5．提供先3①法令上の根拠	番号法第19条第7号別表第二第26項	番号法第19条第8号別表第二第26項	事前	
令和3年9月1日	Ⅱ5．移転先3①法令上の根拠	番号法第19条第7号別表第二第26項	番号法第19条第8号別表第二第26項	事前	
令和4年1月1日	（別添1）事務内容		データのアップロード方法の変更に伴い更新	事前	
令和4年6月1日	（別添1）事務内容		印刷帳票の電子データ化に伴い更新	事前	
令和6年3月1日	（別添1）事務内容		申請書の搬送方法の変更、受給者証の納品方法の変更、局名の変更に伴い変更	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要	東京都福祉保健局保健政策部医療助成課医療調整担当	東京都福祉局生活福祉部医療助成課医療調整担当	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要	【委託先名】 株式会社コステム	【委託先名】 ビーエスロジスティクス株式会社	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要	【委託先名】 株式会社KDS	【委託先名】 株式会社アイネスリレーションズ	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要	【委託先名】 キャリアリンク株式会社	【委託先名】 エイジェック株式会社	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要	【委託先名】 みずほ情報総研株式会社	【委託先名】 みずほリサーチ&テクノロジーズ株式会社	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要		【委託事項5】を追加	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要		【委託事項6】を追加	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要	【中間サーバー・プラットフォームにおける措置】 ②ディスク交換やハード更改等の際は、中間	【中間サーバー・プラットフォームにおける措置】 ②ディスク交換やハード更改等の際は、中間	事前	
令和6年3月1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	・IDの有効期限は1年未満で設定することとし、パスワードについては3か月ごとに強制変更させ	・IDの有効期限は1年未満で設定することとし、パスワードについては必要に応じて変更するほ	事前	
令和6年3月1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	・東京都個人情報の保護に関する条例第10条	・個人情報の保護に関する法律第69条により、事務外での利用を制限されている。	事前	
令和6年3月1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	【委託事項1～4】について	【委託事項5、6】の追加に伴い、該当する「【委託事項】」の番号及び内容変更・追加	事前	
令和6年3月1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	【委託事項2～4】	【委託事項1～6】 ・委託先から他者への外部提供なし。	事前	
令和6年3月1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	【委託事項2】 ・帳票原票の受け渡しは施錠できる専用トランク	【委託事項2】 ・帳票原票の受け渡しは施錠できる専用トランク	事前	
令和6年3月1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	【中間サーバー・ソフトウェア】 ・中間サーバは、特定個人情報保護委員会との	【中間サーバー・ソフトウェア】 ・中間サーバは、特定個人情報保護委員会との	事前	
令和6年3月1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	【中間サーバー・ソフトウェア】 ・中間サーバは、特定個人情報保護委員会との	【中間サーバー・ソフトウェア】 ・中間サーバは、特定個人情報保護委員会との	事前	
令和6年3月1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	【連携サーバー】 ・機器のうち、特定個人情報等のデータが記録さ	【連携サーバー】 ・機器のうち、特定個人情報等のデータが記録さ	事前	
令和6年3月1日	Ⅱ特定個人情報ファイルの概要	【申請書類】 ・保存期間を満了した申請書類については、溶解	【申請書類】 ・保存期間を満了した申請書類については、溶解	事前	
令和6年3月1日	Ⅳ　その他のリスク対策 1．監査 ②監査	【医療費助成事務システム】 また、内部監査人による監査を毎年実施している。	【医療費助成事務システム】 また、内部監査人による監査を4年に一度実施している。	事前	
令和8年1月6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 ③他のシステムとの接続	その他 記載無し	その他（PMH）	事前	
令和8年1月6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5 ②システムの機能	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ①情報登録機能及びPMH-ID採番依頼機能等 東京都立中部総合精神保健福祉センター（以下、「センター」という。）で管理している個人番号及び公費医療費助成の資格情報等をPublic Medical Hub（PMH）に登録し、社会保険診療報酬支払基金（以下、「支払基金」という。）の医療保険者等向け中間サーバーと連動し、PMH-IDを自動採番する。すでにPMH-ID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-IDを利用する。	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ①情報登録機能及びPMHキー採番依頼機能等 東京都立中部総合精神保健福祉センター（以下、「センター」という。）で管理している個人番号及び公費医療費助成の資格情報等をPublic Medical Hub（PMH）に登録し、社会保険診療報酬支払基金（以下、「支払基金」という。※2026年度以降に「医療情報基盤・診療報酬審査支払機構」に組織名称の変更を予定）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。		

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8年1月6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5 ②システムの機能	②情報連携機能（医療機関システム） ・PMH連携キーを利用した情報提供機能 医療機関からの問い合わせに対し、公費医療費助成の資格情報を連携する。 医療機関のオンライン資格確認端末で、患者（利用者）が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上で都度、PMH連携キーが生成され、公費医療費助成の資格情報の照会が行われる。Public Medical Hub（PMH）は、PMH連携キーからPMH-IDを復号し、PMH-IDに紐付けられた公費医療費助成の資格情報を医療機関システムへ提供する。	②情報連携機能（医療機関システム） ・PMH連携キーを利用した情報提供機能 医療機関からの問い合わせに対し、公費医療費助成の資格情報を連携する。 医療機関のオンライン資格確認端末で、患者（利用者）が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上で都度、PMH連携キーが生成され、公費医療費助成の資格情報の照会が行われる。Public Medical Hub（PMH）は、PMH連携キーからPMHキーを復号し、PMHキーに紐付けられた公費医療費助成の資格情報を医療機関システムへ提供する。		
令和8年1月6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5 ②システムの機能	③情報連携機能（マイナポータル） ・識別子の格納機能 マイナポータルからのPublic Medical Hub（PMH）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-IDと紐付けてPublic Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報提供機能 公費医療費助成の対象者は、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。Public Medical Hub（PMH）は、PMH仮名識別子からPMH-IDを特定し、PMH-IDに紐付く公費医療費助成の資格情報をマイナポータルへ提供する。	③情報連携機能（マイナポータル） ・識別子の格納機能 マイナポータルからのPublic Medical Hub（PMH）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Public Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報提供機能 公費医療費助成の対象者は、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。Public Medical Hub（PMH）は、PMH仮名識別子からPMHキーを特定し、PMHキーに紐付く公費医療費助成の資格情報をマイナポータルへ提供する。		
令和8年1月6日	（別添1）事務内容	記載無し	㉚医療費助成システムから連携サーバ及び中間サーバを経由し情報提供ネットワークシステムへ保険情報の情報照会を行う。		
令和8年1月6日	（別添1）事務内容	⑪審査が終了した申請書類は、書類庫へ保管する。（職員）	⑪審査が終了した申請書類は、センター書類庫へ保管する。（職員）		
令和8年1月6日	（別添1）事務内容	㉒住基への照会件数が多い場合は、外部記録媒体を持参し、都庁（総務局行政部）にて住民基	㉒住基への照会件数が多い場合は、センターが外部記録媒体（CD）を持参し、都庁（総務局行政		
令和8年1月6日	（別添1）事務内容	㉗PMHHD採番　・PMHは、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMH-IDの採番処理を依頼し、医療保険者等向け中間サーバーは、PMH-IDを採番してPMHに回答する。医療保険者等向け中間サーバーは、PMH-IDと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。	㉗PMHHD採番　・PMHは、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPMHが連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、PMHキーを採番してPMHに回答する。医療保険者等向け中間サーバーは、PMHキーと紐付番号を紐付けて、オンライン資格確認等システムへ連携する。		
令和8年1月6日	（別添1）事務内容	㉘マイナポータルからの資格確認　・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-ID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-IDと紐付けて、PMHに連携する。（連携後、マイナポータル上からPMH-IDは削除される。）以降、マイナポータルからの資格確認が可能となる。 ・住民がマイナポータル経由で、自身の公費医療資格情報を確認する。	㉘マイナポータルからの資格確認　・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、PMH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、マイナポータルからの資格確認が可能となる。 ・住民がマイナポータル経由で、自身の公費医療資格情報を確認する。		
令和8年1月6日	（別添1）事務内容	㉙医療機関からの資格確認　・オンライン資格確認等システムは、紐付番号をキーにマイナンバーカードの電子証明書のシリアル番号とPMH-IDを紐付けて、一時的に利用するためのPMH連携キーを暗号化して生成する。オンライン資格確認等システムは、PMHにPMH連携キーで公費医療費助成の資格情報を照会し、照会元となる医療機関システム等に同資格情報を応答する。（PMH連携キーは都度作成され、利用後に削除される。）医療機関システム等を利用して受診者が、マイナンバーカードで認証し、同意する都度、資格確認が可能となる。	㉙医療機関からの資格確認　・オンライン資格確認等システムは、紐付番号をキーにマイナンバーカードの電子証明書のシリアル番号とPMHキーを紐付けて、一時的に利用するためのPMH連携キーを暗号化して生成する。オンライン資格確認等システムは、PMHにPMH連携キーで公費医療費助成の資格情報を照会し、照会元となる医療機関システム等に同資格情報を応答する。（PMH連携キーは都度作成され、利用後に削除される。）医療機関システム等を利用して受診者が、マイナンバーカードで認証し、同意する都度、資格確認が可能となる。		
令和8年1月6日	Ⅱ ファイルの概要 2. 基本情報 ④記録される項目 その妥当性	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ 〇・識別情報（その他識別情報） PMH-ID、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 自治体業務ID…PMH内で公費医療の種類を区別するために必要となる。 ・業務関係情報（その他） 医療助成資格情報…（医療費助成事務の適切な実施にあたり必要となる情報を管理し、）PMHが、外部と情報連携するために必要となる。	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ 〇・識別情報（その他識別情報） PMHキー、PMH仮名識別子…PMHが、外部と情報連携するために必要となる。 自治体業務ID…PMH内で公費医療の種類を区別するために必要となる。 ・業務関係情報（その他） 医療助成資格情報…（医療費助成事務の適切な実施にあたり必要となる情報を管理し、）PMHが、外部と情報連携するために必要となる。		
令和8年1月6日	Ⅱ ファイルの概要 3. 特定個人情報の入手・試用 ③入手の時期・頻度	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・PMH-IDの採番処理依頼時に都度、医療保険者等向け中間サーバーから特定個人情報を入手する。	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・PMHキーの採番処理依頼時に都度、医療保険者等向け中間サーバーから特定個人情報を入手する。		
令和8年1月6日	Ⅱ ファイルの概要 3. 特定個人情報の入手・試用 ④入手に係る妥当性	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・外部との情報連携のため、PMH-IDの採番処理依頼時に医療保険者等向け中間サーバーから自動的に入手される。	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・外部との情報連携のため、PMHキーの採番処理依頼時に医療保険者等向け中間サーバーから自動的に入手される。		

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8年1月6日	Ⅱ ファイルの概要 3. 特定個人情報の入手・試用 ⑧使用方法	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・情報連携のため、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む対象者情報、公費資格情報の紐付け及び登録を行う。 ・登録後、Public Medical Hub（PMH）は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub（PMH）が連動するためのPMH-IDの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMH-IDを採番して個人番号と共にPublic Medical Hub（PMH）に応答する。なお、採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金が医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。 ・PMH-IDが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルとPublic Medical Hub（PMH）で共有されることでマイナポータルや医療機関システムから公費資格情報の取得/閲覧を行うといった情報連携が可能となる。	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・情報連携のため、Public Medical Hub（PMH）へ本事務に係る対象者の個人番号を含む対象者情報、公費資格情報の紐付け及び登録を行う。 ・登録後、Public Medical Hub（PMH）は、医療保険者等向け中間サーバーに対してオンライン資格確認等システムとPublic Medical Hub（PMH）が連動するためのPMHキーの採番処理を依頼し、医療保険者等向け中間サーバーは、情報連携用の識別子としてPMHキーを採番して個人番号と共にPublic Medical Hub（PMH）に応答する。なお、採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金が医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。 ・PMHキーが、個人情報として医療保険者等向け中間サーバーから既存の紐付番号とともにオンライン資格確認等システムに連携され、更にマイナポータルで生成されたPMH仮名識別子がマイナポータルとPublic Medical Hub（PMH）で共有されることでマイナポータルや医療機関システムから公費資格情報の取得/閲覧を行うといった情報連携が可能となる。		
令和8年1月6日	Ⅱ ファイルの概要 3. 特定個人情報の入手・試用 ⑧使用方法 情報の突合	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・PMH-IDの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・PMHキーの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。		
令和8年1月6日	Ⅱ 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5 ⑥委託先名	記載無し	ビーエスロジスティクス株式会社		
令和8年1月6日	Ⅱ 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7 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	Public Medical Hub（PMH）は国（デジタル庁）が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMH-IDの採番において特定個人情報ファイルを取り扱う必要がある。 ただし、PMHに格納された特定個人情報は、自動処理により再委託先に情報連携されるため、国（デジタル庁）は特定個人情報にアクセスすることはない。	Public Medical Hub（PMH）は国（デジタル庁）が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。 ただし、PMHに格納された特定個人情報は、自動処理により再委託先に情報連携されるため、国（デジタル庁）は特定個人情報にアクセスすることはない。		
令和8年1月6日	Ⅱ 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7 ⑨再委託事項	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・Public Medical Hub（PMH）の運用保守 ・PMH-IDの採番 ・PMH-IDを介した医療機関システム・マイナポータルへの情報連携 ※情報連携はPMH-IDを介して行うため、特定個人情報を取り扱わない。	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ・Public Medical Hub（PMH）の運用保守 ・PMHキーの採番 ・PMHキーを介した医療機関システム・マイナポータルへの情報連携 ※情報連携はPMHキーを介して行うため、特定個人情報を取り扱わない。		
令和8年1月6日	Ⅱ ファイルの概要 6. 特定個人情報の保管・消去 ①保管場所	【中間サーバー・プラットフォーム】 ①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おり、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い、厳重に管理する。 ②特定個人情報は、サーバー室に設置された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。	【中間サーバー・プラットフォーム】 ①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。		
令和8年1月6日	Ⅱ ファイルの概要 6. 特定個人情報の保管・消去 ③消去方法	【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、物理的破壊により完全に消去する。	【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・運用を行う事業者及びクラウドサービス事業者が特定個人情報を消去することはない。 ②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。③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。		

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8年1月6日	（別添2）ファイル記録項目 <Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務追加の記録項目> (1)対象者情報	PMH-ID	PMHキー		
令和8年1月6日	Ⅲ リスク対策（プロセス） 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 対象者以外の情報の入手を防止するための措置の内容	【<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置】 ・PMH-IDの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで対象者以外の情報の入手を防止する。（当該機能は、R6年度中に実装予定）	【<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置】 ・PMHキーの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで対象者以外の情報の入手を防止する。（当該機能は、R6年度中に実装予定）		
令和8年1月6日	Ⅲ リスク対策（プロセス） 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 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	【<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務>における追加措置】 ・医療保険者等向け中間サーバーからPublic Medical Hub（PMH）へは、定められたインターフェース仕様に沿って決められたデータ項目（PMH-IDと個人番号）のみが返却されるようシステム的に制御している。	【<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務>における追加措置】 ・医療保険者等向け中間サーバーからPublic Medical Hub（PMH）へは、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステム的に制御している。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 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2 リスクに対する措置の内容	【<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務>における追加措置】 ・医療保険者等向け中間サーバーからPublic Medical Hub（PMH）へは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMH-IDと個人番号）のみが返却されるようシステム的に制御している。	【<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務>における追加措置】 ・医療保険者等向け中間サーバーからPublic Medical Hub（PMH）へは、システム自動処理により、定められたインターフェース仕様に沿って決められたデータ項目（PMHキーと個人番号）のみが返却されるようシステム的に制御している。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 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3 特定個人情報の正確性確保の措置の内容	【本人確認情報】 ・住民基本台帳を所管する各自治体で本人確認済み。	【本人確認情報】 ・正確性は、住民基本台帳を所管する各自治体が適切に対応している。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 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3 特定個人情報の正確性確保の措置の内容	<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置> ・PMH-IDの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで正確性を担保する。（当該機能は、R6年度中に実装予定）	<Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置> ・PMHキーの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことで正確性を担保する。（当該機能は、R6年度中に実装予定）		
令和8年1月6日	Ⅲ リスク対策（プロセス） 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	【委託事項1、5】 ・従事者名簿、計画書、業務報告書を提出させている。 【委託事項2、4】 ・ともにプライバシーマーク取得事業者である。また、システム運用管理業者はシステムセキュリティに関する内規によりISMS認証取得事業者としている。 【委託事項2～4】 ・契約時に取り交わす仕様書で、責任者、作業体制、連絡体制及び作業場所を書面にして提出、業務従事者への遵守事項の周知、再委託の承諾申請の提出、作業担当者の名簿の提出等を委託先に求めている。 ・委託元が委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認する。 【委託業務6】 ・溶解処理施設への運搬と機密文書の計量は委託者立ち合いの元で行い、溶解処分の証明書類として情報抹消証明書、再生資源管理伝票及び適正に処分した現場写真を提出させている。 【委託事項7】 Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務における特定個人情報の取扱いを国（デジタル庁）に委託することとする。 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）に基づき、委託先となる国（デジタル庁）の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。	【委託事項1、5】 ・従事者名簿、計画書、業務報告書を提出させている。 【委託事項2、4】 ・ともにプライバシーマーク取得事業者である。また、システム運用管理業者はシステムセキュリティに関する内規によりISMS認証取得事業者としている。 【委託事項2～4】 ・契約時に取り交わす仕様書で、責任者、作業体制、連絡体制及び作業場所を書面にして提出、業務従事者への遵守事項の周知、再委託の承諾申請の提出、作業担当者の名簿の提出等を委託先に求めている。 ・委託元が委託先に対して実地調査を定期的に行い、適切な管理体制をとっていることを確認する。 【委託業務2】 媒体を授受する際の双方確認、保管中の確実な施錠、速やかなデータ削除等、実施手順を遵守することを受託者に教育する。 【委託業務6】 ・溶解処理施設への運搬と機密文書の計量は委託者立ち合いの元で行い、溶解処分の証明書類として情報抹消証明書、再生資源管理伝票及び適正に処分した現場写真を提出させている。 ・廃棄委託における都職員の立会いの実施か、立会いに代えて受託者に証明書や写真等を提出させる場合は、写真を撮るポイントを具体的に指定する。 【委託事項7】 Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務における特定個人情報の取扱いを国（デジタル庁）に委託することとする。 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）に基づき、委託先となる国（デジタル庁）の設備、技術水準、従業者に対する監督・教育の状況等を事前に確認する。		

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8年1月6日	Ⅲ リスク対策（プロセス） 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限 具体的な制限方法	※特定個人情報に係るアクセス権限は、再委託先（PMH-ID採番や運用保守）のみに付与される。	※特定個人情報に係るアクセス権限は、再委託先（PMHキー採番や運用保守）のみに付与される。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの取扱いの記録 具体的な方法	※再委託先（PMH-ID採番や運用保守）に係る特定個人情報の取扱いログに限られる。	※再委託先（PMHキー採番や運用保守）に係る特定個人情報の取扱いログに限られる。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 4. 特定個人情報ファイルの取扱いの委託 その他の措置の内容	【委託事項7】 <Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置> ・PMH-IDの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。（当該機能は、R6年度中に実装予定） ・委託契約書に以下の規定を設ける。 委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。	【委託事項7】 <Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置> ・PMHキーの採番処理時には、Public Medical Hub（PMH）が保有する個人番号及び基本情報（カナ、氏名、生年月日、性別、住所）と支払基金の医療保険者等向け中間サーバーで保有する個人番号及び基本情報とを突合する誤りチェック機能で紐付け誤りを防ぐことが可能となる。（当該機能は、R6年度中に実装予定） ・委託契約書に以下の規定を設ける。 委託先は、従事者に対して情報セキュリティに関する教育を行い、業務外での特定個人情報の取扱いの禁止を徹底する。 ・委託先からの情報提供を十分に受けられるよう、Teamsによりコミュニケーションを行い、同システムを利用する他の部署とも連携して最新の情報を収集・共有する。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 6. 情報提供ネットワークシステムとの接続 リスク1 リスクに対する措置の内容	【区市町村】 ・「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）」に従った、区市町村の安全管理措置に委ねられる。	【区市町村】 ・「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）」に従って、区市町村が適切に安全管理措置を講じている。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 6. 情報提供ネットワークシステムとの接続 リスク2 リスクに対する措置の内容	【区市町村】 ・「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）」に従った、区市町村の安全管理措置に委ねられる。	【区市町村】 ・「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）」に従って、区市町村が適切に安全管理措置を講じている。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 6. 情報提供ネットワークシステムとの接続 リスク3 リスクに対する措置の内容	【区市町村】 ・「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）」に従った、区市町村の安全管理措置に委ねられる。	【区市町村】 ・「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）」に従って、区市町村が適切に安全管理措置を講じている。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 6. 情報提供ネットワークシステムとの接続 リスク4 リスクに対する措置の内容	【区市町村】 ・「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）」に従った、区市町村の安全管理措置に委ねられる。	【区市町村】 ・「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）」に従った、区市町村の安全管理措置で適切に対応している。 ＜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、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、クラウドサービス事業者の業務は、クラウドサービスの提供であり、業務上、特定個人情報へはアクセスすることはない。		

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8年1月6日	Ⅲ リスク対策（プロセス） 6. 情報提供ネットワークシステムとの接続 リスク5 リスクに対する措置の内容	記載無し	＜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。 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機微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。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 6. 情報提供ネットワークシステムとの接続 リスク6 リスクに対する措置の内容	記載無し	＜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。 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機微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		
令和8年1月6日	Ⅲ リスク対策（プロセス） 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	記載無し	＜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。		

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8年1月6日	Ⅲ リスク対策（プロセス） 7. 特定個人情報の保管・消去 リスク1 ⑤物理的対策	【区市町村】 ・「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）」にのっとり、区市町村の安全管理措置に委ねられる。	【区市町村】 ・「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）」に従って、区市町村が適切に安全管理措置を講じている。 ＜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。		
令和8年1月6日	Ⅳ リスク対策（その他） 1. 監査 ②監査	記載無し	＜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・プラットフォームについて、定期的に監査を行うこととしている。 ②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。		
令和8年1月6日	Ⅳ リスク対策（その他） 2. 従業者に対する教育・啓発	記載無し	＜中間サーバー・プラットフォームにおける措置＞ ①IPA（情報処理推進機構）が提供する最新の情報セキュリティ教育用資料等を基にセキュリティ教育資材を作成し、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、運用規則（接続運用規程等）や情報セキュリティに関する教育を年次（年2回）及び随時（新規要員着任時）実施することとしている。		
令和8年1月6日	Ⅳ リスク対策（その他） 2. 従業者に対する教育・啓発	【職員（非常勤含む。）】 全職員を対象に情報セキュリティ・特定個人情報保護の研修（特定個人情報含む）を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない）年1回 ・新規採用職員や他局転入職員等を対象とした研修 ・未受講者が出ないように端末のない職員に紙でeラーニング研修の実施を行い、結果の報告を受けることとしている。	【職員（非常勤含む。）】 全職員を対象に情報セキュリティ・特定個人情報保護の研修（特定個人情報含む）を実施している。研修の目的は、個人情報保護の重要性及び適正管理等に関する理解を深め、個人情報保護の遵守を徹底することである。具体的には、以下の研修を実施している。 ・個人端末からアクセスするeラーニング研修（理解度が基準に達しないと修了できない）年1回 ・新規採用職員や他局転入職員等を対象とした研修 ・未受講者が出ないように端末のない職員に紙でeラーニング研修の実施を行い、結果の報告を受けることとしている。 ・具体的な手順や体制について、都職員へ周知徹底する。		
令和8年1月6日	Ⅳ リスク対策（その他） 3. その他のリスク対策	記載無し	＜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活用することにより、設備環境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による高レベルのセキュリティ管理（入退室管理等）、ITリテラシ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。		
令和8年1月6日	（別添1）事務内容	⑭パンチ業者にて入力票の個人情報をシステムで処理可能なデータ入力用ファイルとして作成し、センターに外部記録媒体（CD-RW）で提出する。（委託事項2）	⑭パンチ業者にて入力票の個人情報をシステムで処理可能なデータ入力用ファイルとして作成し、センターに外部記録媒体（CD-RW）で返送する。（委託事項2）		
令和8年1月6日	（別添1）事務内容	③区市町村は東京都立中部総合精神保健福祉センター（以下、「センター」という。）に進達を行う。 （搬送委託または郵送）	③区市町村はセンターに進達を行う。 （搬送委託（委託事項5）または郵送（委託事項1）））		

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8年1月6日	Ⅰ 基本情報 システム5	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ①情報登録機能及びPMH-ID採番依頼機能等 東京都立中部総合精神保健福祉センターで管理している個人番号及び公費医療費助成の資格情報等をPublic Medical Hub（PMH）に登録し、社会保険診療報酬支払基金（以下、「支払基金」という。）の医療保険者等向け中間サーバーと連動し、PMH-IDを自動採番する。すでにPMH-ID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-IDを利用する。 ②情報連携機能（医療機関システム） ・PMH連携キーを利用した情報提供機能 医療機関からの問い合わせに対し、公費医療費助成の資格情報を連携する。 医療機関のオンライン資格確認端末で、患者（利用者）が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上で都度、PMH連携キーが生成され、公費医療費助成の資格情報の照会が行われる。Public Medical Hub（PMH）は、PMH連携キーからPMH-IDを復号し、PMH-IDに紐付けられた公費医療費助成の資格情報を医療機関システムへ提供する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 マイナポータルからのPublic Medical Hub（PMH）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-IDと紐付けてPublic Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報提供機能 公費医療費助成の対象者は、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。Public Medical Hub（PMH）は、PMH仮名識別子からPMH-IDを特定し、PMH-IDに紐付く公費医療費助成の資格情報をマイナ	＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務＞ ①情報登録機能及びPMH-ID採番依頼機能等 東京都立中部総合精神保健福祉センター（以下、「センター」という。）で管理している個人番号及び公費医療費助成の資格情報等をPublic Medical Hub（PMH）に登録し、社会保険診療報酬支払基金（以下、「支払基金」という。）の医療保険者等向け中間サーバーと連動し、PMH-IDを自動採番する。すでにPMH-ID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-IDを利用する。 ②情報連携機能（医療機関システム） ・PMH連携キーを利用した情報提供機能 医療機関からの問い合わせに対し、公費医療費助成の資格情報を連携する。 医療機関のオンライン資格確認端末で、患者（利用者）が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上で都度、PMH連携キーが生成され、公費医療費助成の資格情報の照会が行われる。Public Medical Hub（PMH）は、PMH連携キーからPMH-IDを復号し、PMH-IDに紐付けられた公費医療費助成の資格情報を医療機関システムへ提供する。 ③情報連携機能（マイナポータル） ・識別子の格納機能 マイナポータルからのPublic Medical Hub（PMH）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-IDと紐付けてPublic Medical Hub（PMH）に格納して保管する。 ・仮名識別子を利用した情報提供機能 公費医療費助成の対象者は、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。Public Medical Hub（PMH）は、PMH仮名識別子からPMH-IDを特定し、PMH-ID		
令和8年1月6日	Ⅲ リスク対策（プロセス） 4. 特定個人情報ファイルの取扱いの委託 特定個人情報ファイルの閲覧者・更新者の制限	【委託事項1～5】 ・作業者を限定するために、委託業務従事者名を書面により提出させている ・開封を禁止する取り決めを業者と交わしている。 【委託事項3、4】 ・委託先が使用するユーザIDは、ID管理に係る内規に基づき、割り当てを行っている。ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。 【委託事項2～4】 ・秘密の保持、目的外使用の禁止、複写及び複製の禁止、作業場所以外への持ち出し禁止、情報の保管及び管理等を規定した仕様書を取り交わし、委託処理に係る必要事項を定めている。 【委託事項6】 機密文書を保管している段ボール箱を開封することなく溶解させている。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・中総ではアクセス権限の管理状況を確認できる。 ・アクセス権限を付与する者を必要最小限に限定する。 ・アクセス権限を付与する範囲を必要最小限に限定する。 ・アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再委託先（PMH-ID採番や運用保守）のみに付与される。	【委託事項1～5】 ・作業者を限定するために、委託業務従事者名を書面により提出させている ・開封を禁止する取り決めを業者と交わしている。 【委託事項3、4】 ・委託先が使用するユーザIDは、ID管理に係る内規に基づき、割り当てを行っている。ユーザIDの設定に際しては、用途を確認した上で必要最小限の権限のみ付与し、使用する期間のみ有効とし、有効期間が経過した場合には当該ユーザIDでは特定個人情報ファイルを閲覧できないようにしている。 【委託事項2～4】 ・秘密の保持、目的外使用の禁止、複写及び複製の禁止、作業場所以外への持ち出し禁止、情報の保管及び管理等を規定した仕様書を取り交わし、委託処理に係る必要事項を定めている。 【委託事項6】 機密文書を保管している段ボール箱を開封することなく溶解させている。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・センターではアクセス権限の管理状況を確認できる。 ・アクセス権限を付与する者を必要最小限に限定する。 ・アクセス権限を付与する範囲を必要最小限に限定する。 ・アクセス権限を付与した者と権限の範囲を適切に管理する。 ※特定個人情報に係るアクセス権限は、再委託先（PMH-ID採番や運用保守）のみに付与される。		
令和8年1月6日	Ⅲ リスク対策（プロセス） 4. 特定個人情報ファイルの取扱いの委託 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	【委託事項1～6】 ・委託先から他者への外部提供なし。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・委託先（再委託も含む。）から他者への提供は行わない。 ・中総では委託契約に基づき、委託先（再委託先も含む。）から他者への提供が行われていないことを確認できる。	【委託事項1～6】 ・委託先から他者への外部提供なし。 【委託事項7】＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ ・委託先（再委託も含む。）から他者への提供は行わない。 ・センターでは委託契約に基づき、委託先（再委託先も含む。）から他者への提供が行われていないことを確認できる。		

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8年1月6日	Ⅲ リスク対策（プロセス） 7. 特定個人情報の保管・消去 ⑥技術的対策	【中間サーバ・プラットフォーム】 ・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。 ・中間サーバー・プラットフォームでは、ウィ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。 ・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。 【連携サーバー】 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントとそれ以外のセグメントの境界にファイアーウォールを導入するとともに、ログを取得する。 ・ウィルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア（OS）及びミドルウェアは、必要に応じてセキュリティパッチを適用する。 ・データベースにデータを暗号化して保存する。 ・データベースに対する操作権限を細分化し、連携サーバ管理者であっても真に必要な場合を除いてはデータにアクセスできないよう制御する。 ・データベースに対するアクセスログを取得する。 ・データベースのバックアップを取得する。 ・あらかじめ登録された機器だけがネットワークに接続できるよう制御する。 ・サーバ及びその管理に用いる機器は、書き出し可能な外部記録媒体を内蔵せず、かつUSB機器等に対する制御を行い、外部記録媒体の利用を制限する。 【医療費助成事務システム】 ・入手した特定個人情報を取り込むこととなる医療費助成システムは、専用回線又は閉塞ネットワークとし、外部ネットワークから第三者によるアクセスは不可能である。	【中間サーバ・プラットフォーム】 ・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。 ・中間サーバー・プラットフォームでは、ウィ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。 ・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。 【連携サーバー】 ・インターネットや庁内の他のネットワークから分離された専用のネットワーク上で稼働する。 ・サーバが接続されたセグメントとそれ以外のセグメントの境界にファイアーウォールを導入するとともに、ログを取得する。 ・ウィルス対策ソフトを導入し、パターンファイルを更新する。 ・基本ソフトウェア（OS）及びミドルウェアは、必要に応じてセキュリティパッチを適用する。 ・データベースにデータを暗号化して保存する。 ・データベースに対する操作権限を細分化し、連携サーバ管理者であっても真に必要な場合を除いてはデータにアクセスできないよう制御する。 ・データベースに対するアクセスログを取得する。 ・データベースのバックアップを取得する。 ・あらかじめ登録された機器だけがネットワークに接続できるよう制御する。 ・サーバ及びその管理に用いる機器は、書き出し可能な外部記録媒体を内蔵せず、かつUSB機器等に対する制御を行い、外部記録媒体の利用を制限する。 【医療費助成事務システム】 ・入手した特定個人情報を取り込むこととなる医療費助成システムは、専用回線又は閉塞ネットワークとし、外部ネットワークから第三者によるアクセスは不可能である。		
	Ⅰ 基本情報 1. 特定個人情報ファイルを取り扱う事務 ③対象人数	10万人以上30万人未満	30万人以上		
	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 ③他のシステムとの接続	その他　PMH	その他　PMH、連携サーバ		
	Ⅱ ファイルの概要 4. 特定個人情報ファイルの取り扱いの委託 委託事項3 ③委託先における取扱者数	10人以上50人未満	50人以上100人未満		
	Ⅱ ファイルの概要 4. 特定個人情報ファイルの取り扱いの委託 委託事項3 ⑥委託先名	株式会社バックスグループ	東武トップツアーズ株式会社		
	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	記載無し	・医療費助成事務システム（精神通院）システムの "③他のシステムとの接続"のその他 のところに "団体内統合利用番号連携サーバー"を追加		
	（別添1）事務内容 シート 事務・システムフロー図	記載無し	図の東京都医療費助成事務システムから連携サーバへの線を追加		
	（別添1）事務内容 シート 事務・システムフロー図		図の委託先（支払基金）を　委託先（DX審査支払基金）に変更		
	Ⅱ ファイルの概要 シート 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑥ 委託先名	みずほリサーチ&テクノロジーズ株式会社	システム開発終了後に保守委託契約を締結する。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅱ ファイルの概要 シート 4. 特定個人情報ファイルの取扱いの委託 委託事項4 ⑥ 委託先名	再委託する	削除	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅱ ファイルの概要 シート 4. 特定個人情報ファイルの取扱いの委託 委託事項7 ②取扱いを委託する特定個人情報ファイルの範囲	Public Medical Hub（PMH）は国（デジタル庁）が構築し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。 ただし、PMHに格納された特定個人情報は、自動処理により再委託先に情報連携されるため、国（デジタル庁）は特定個人情報にアクセスすることはない。	Public Medical Hub（PMH）はDX審査支払機構が運用し、希望する市区町村が利用するが、その適切な管理のため運用保守、PMHキーの採番において特定個人情報ファイルを取り扱う必要がある。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため

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
	Ⅱ ファイルの概要 シート 6. 特定個人情報の保管・消去 ① 保管場所	【医療費助成事務システム】 特定個人情報を保管するサーバーを設置するデータセンターは、災害発生時もサーバー室等へ滞りなく電力を供給できる冗長化された電力供給設備を備えていること等の防災性を考慮している。 なお、データセンターへの立入りはICカード所持者に限定しており、サーバー室に入るためには、ICカードに加え、入退室人数センサー感知、カメラによる監視等、厳重なセキュリティ対策を行っている。 データセンター、執務室いずれも媒体及び紙資料を施錠できるロッカー等に保管している。 端末設置場所は施錠管理するとともに、端末はセキュリティワイヤにより固定し、ワイヤ錠はシステム管理者が一元的に施錠保管としている。	【医療費助成事務システム】 医療費助成事務システムは、CSPが提供するクラウドサービスに東京都クラウドインフラとして必要と考えられる統制機能やセキュリティ設定を適用した「クラウドインフラサービス」基盤上に構築される。 採用するCSPは、AWSとなり、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となる。このため、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おり、主に以下の物理的対策を講じている。 ・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。 ・許可されたアカウント以外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。 ・特定個人情報は、CSP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に保存される。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅱ ファイルの概要 6. 特定個人情報の保管・消去 ③消去方法	【医療費助成事務システム】 ・5年間異動のないデータは定期処理により削除することとしている。 ・外部記録媒体内のデータは、職員が消去している。	【医療費助成事務システム】 ・5年間異動のないデータは定期処理により削除することとしている。 ・外部記録媒体内のデータは、職員が消去している。 ・特定個人情報の消去は管理組織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東京都クラウドインフラ管理者及び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。 ・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は、クラウド事業者はNIST 800-88 に詳細が説明されている方法を使用してメディアを廃棄する。 ・既存システムについては、管理組織が委託した開発事業者が既存の環境から東京都クラウドインフラへ 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	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅲ リスク対策（プロセス） 4. 特定個人情報ファイルの取扱いの委託 情報保護管理体制の確認	【委託事項7】 Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務における特定個人情報の取扱いを国（デジタル庁）に委託することとする。	【委託事項7】 Public Medical Hub（PMH）の利用・情報連携業務及び運用保守業務における特定個人情報の取扱いをDX審査支払機構に委託することとする。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅲ リスク対策（プロセス） シート 4. 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ルール 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	【委託事項4】 ・オンライン入力若しくはバッチ入力で受け渡された申請データが格納されるDBへのアクセス権限は都から付与されるIDにより設定され、必要最小限に制限されている。 ・本番データの参照・修正は都の指示に基づき行っている。 ・作業状況については週次の定例会で報告を行い確認している。 ・作業はデータセンタに設置されている専用端末により実施しており、データセンタへの立ち入りはICカード所持者に限定しており、サーバ室に入るためには、ICカードに加え、入退室人数センサー感知、カメラによる監視等、厳重なセキュリティ対策を行っている。 ・医療費助成事務システムではサーバ機器は東京都中央コンピュータ室に設置し、ICカードと二要素認証による入退室管理を行う。	【委託事項4】 ・オンライン入力若しくはバッチ入力で受け渡された申請データが格納されるDBへのアクセス権限は都から付与されるIDにより設定され、必要最小限に制限されている。 ・本番データの参照・修正は都の指示に基づき行っている。 ・作業状況については週次の定例会で報告を行い確認している。 ・作業は保守拠点に設置する都が貸与した専用端末により実施しており、専用端末が設置された部屋への立ち入りはICカード所持者に限定している。 ・委託先には、業務上、最低限必要な範囲の特定個人情報のみを提供できる。それ以外の提供は一切認められず、その旨を委託契約書にも明記する（予定）。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅲ リスク対策（プロセス） シート 4. 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ルール 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 具体的な方法	【委託事項7】 ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるデジタル庁が、再委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、年1回デジタル庁から報告を受ける。	【委託事項7】 ・再委託の相手方は、委託先が負っている本契約上の義務と同等の義務を負うことを委託契約書に定める。 ・委託先であるDX審査支払機構が、再委託先における特定個人情報ファイルの管理状況の定期的な点検（年1回程度又は随時）を実施する。 ・点検は、セルフチェックを基本とし、必要に応じて訪問確認をする。 ・点検後に改善事項があり、改善指示した場合は、改善状況のモニタリングを行う。 ・点検結果について、必要であると認めるときには、DX審査支払機構に報告を求めることができる。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため

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
	Ⅲ リスク対策（プロセス） シート 7. 特定個人情報の保管・消去 ⑤物理的対策	【医療費助成事務システム】 ・データセンタは、冗長化された電力供給設備、ガス消火装置等の設備を備え、防災性を考慮している。 ・データセンタへの立入りはICカード所持者に限定しており、サーバ室に入るためには、ICカードに加え、入退室人数センサー感知、カメラによる監視等、厳重なセキュリティ対策を行っている。 ・医療費助成事務システムのサーバ機器が設置される東京都中央コンピュータ室においても災害発生に備え、免震床、ガス消火を設置するなど対応している。また、入退室はICカード及び生体認証による入退室管理、カメラ・有人による監視を行っている。 ・データセンタ、執務室いずれも媒体及び紙資料は施錠保管している。 ・端末設置場所は施錠管理するとともに、端末はセキュリティワイヤにより固定し、ワイヤ錠は情報セキュリティ責任者（統括）が一元管理し、施錠保管している。	【東京都クラウド】 医療費助成事務システムは、CSPが提供するクラウドサービスに東京都クラウドインフラとして必要と考えられる統制機能やセキュリティ設定を適用した「クラウドインフラサービス」基盤上に構築される。 採用するCSPは、AWSとなり、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となる。このため、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おり、主に以下の物理的対策を講じている。 ・CSPが管理する物理的に保護されたデータセンター環境（ISMAP登録クラウドサービス）において、論理的に区分された領域にデータを保管する。なお、データセンターにおけるフェンス、監視カメラ、警備員等の物理的セキュリティ対策はCSPの責任範囲で実施する。 ・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。 【医療費助成事務システム】 執務室及び端末は、以下の対応をしている。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅲ リスク対策（プロセス） シート 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	【医療費助成事務システム】 ・入手した特定個人情報を取り込むこととなる医療費助成システムは、専用回線又は閉塞ネットワークとし、外部ネットワークから第三者によるアクセスは不可能である。 ・加えて、ファイアーウォールを設置し、許可していない端末やポート番号の通信遮断を行っている。 ・唯一の外部との接触点である外部記録媒体からのウィルス感染に備え、ウィルス対策ソフトを導入している。	【医療費助成事務システム】 ・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。 ・許可されたアカウント以外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。 ・入手した特定個人情報を取り込むこととなる医療費助成システムは、専用回線又は閉塞ネットワークとし、外部ネットワークから第三者によるアクセスは不可能である。 ・加えて、ファイアーウォールを設置し、許可していない端末やポート番号の通信遮断を行っている。 ・唯一の外部との接触点である外部記録媒体からのウィルス感染に備え、ウィルス対策ソフトを導入している。 ・業務継続及び災害復旧に備えバックアップを取得している。バックアップデータについてもアクセス制御及び暗号化を実施する。 【東京都クラウド】 ・個人番号が含まれる領域は独立しており、他のネットワーク系統からアクセスできないように制御している。 ・許可されたアカウント以外は東京都クラウドの基盤制御に関わる機能にアクセスできないように制御している。 ・ファイアウォール、IAM、多要素認証、CloudTrail	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅲ リスク対策（プロセス） シート 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	<Public Medic＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ Public Medical Hub（PMH）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または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。 ・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（デジタル庁）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。	<Public Medic＜Public Medical Hub（PMH）を活用した情報連携に係る自立支援医療受給者証交付事務における追加措置＞ Public Medical Hub（PMH）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または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。 ・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。 ・DX審査支払機構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。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅱ 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4 ①委託内容	医療費助成事務システムの運用・保守および、受給者証作成を行う。	医療費助成事務システムの運用・保守および、受給者証印刷データの作成を行う。	事前	受給者証を作成するためのデータ作成のみを対応するため
	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2 ③ 他のシステムとの接続	[ ] その他（ ）	[○] その他（中間サーバー）	事前	オンラインでアクセスする運用に変更となるため

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
	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4 ③ 他のシステムとの接続	[　　]住民基本台帳ネットワークシステム	[○]住民基本台帳ネットワークシステム	事前	オンラインでアクセスする運用に変更となるため
	Ⅲ リスク対策（プロセス） 3. 特定個人情報の使用 リスク2 ユーザ認証の管理	・システムセキュリティに係る内規により端末起動時にID・パスワードでのユーザ認証を行うこととしている。 ・IDの有効期限は1年未満で設定することとし、パスワードについては必要に応じて変更するほか、3回以上誤ったパスワードを入力すると該当IDはロックされることとしている。 ・アクセスログが一定期間保管され、誰がいつどの情報を参照・変更等の操作を行ったか把握でき、IDの不適正利用が確認された場合は、当該IDの利用を制限する。 ・ID管理に係る内規に基づき、利用者ID管理簿の定期的な棚卸を実施し、必要最低限の利用者ID付与を行っている。 ・上記に加えて、医療費助成事務システムでは、二要素認証情報を用いた管理を行う。	【医療費助成事務システム】 ・システムセキュリティに係る内規により端末起動時にID・パスワードでのユーザ認証を行うこととしている。 ・IDの有効期限は1年未満で設定することとし、パスワードについては必要に応じて変更するほか、3回以上誤ったパスワードを入力すると該当IDはロックされることとしている。 ・アクセスログが一定期間保管され、誰がいつどの情報を参照・変更等の操作を行ったか把握でき、IDの不適正利用が確認された場合は、当該IDの利用を制限する。 ・ID管理に係る内規に基づき、利用者ID管理簿の定期的な棚卸を実施し、必要最低限の利用者ID付与を行っている。 ・二要素認証情報を用いた管理を行う。 【東京都クラウド】 ・AWS IAMによる個別アカウント管理を実施している。 ・管理者アカウント（特権ユーザー）及び特権ユーザが作成したすべてのユーザに対し、多要素認証（MFA）及び接続元IPアドレス制限している。 ・管理対象サーバへの接続は東京都クラウドが提供する踏み台サーバを経由する。 ・AWS CloudTrailによりAWS API操作を記録するとともに、踏み台サーバのログイン履歴及び操作履歴を記録。なお、東京都クラウドインフラ利用者及び受託者はこれらの設定を変更すること及び収集されたログを変更・削除することはできない。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅲ リスク対策（プロセス） 3. 特定個人情報の使用 リスク2 アクセス権限の発効・失効の管理	・ID管理に係る内規に基づき、管理を行っている。 ・情報セキュリティ責任者（統括）が年度当初にシステム利用所管にあてた調査を実施し、利用者の異動情報を把握した上で、情報セキュリティ責任者（統括）が権限の付与・削除をID管理簿の加除訂正を行いながら一元管理する。 ・IDは年度末に失権するよう設定しており、調査時に連絡が漏れたり、遅れた場合、IDは失効するよう設定されている。 ・年度途中の権限付与管理は、職員については異動情報、委託先従事者については申請に基づき行っている。	【医療費助成事務システム】 ・ID管理に係る内規に基づき、管理を行っている。 ・情報セキュリティ責任者（統括）が年度当初にシステム利用所管にあてた調査を実施し、利用者の異動情報を把握した上で、情報セキュリティ責任者（統括）が権限の付与・削除をID管理簿の加除訂正を行いながら一元管理する。 ・IDは年度末に失権するよう設定しており、調査時に連絡が漏れたり、遅れた場合、IDは失効するよう設定されている。 ・年度途中の権限付与管理は、職員については異動情報、委託先従事者については申請に基づき行っている。 【東京都クラウド】 ・CSPの特権ユーザーは、CSP環境の払出し時に東京都クラウドインフラ管理者が発行する。利用者によるCSPの特権ユーザーの作成・削除・更新は不可。また、CSPの特権ユーザーの削除は、利用者からの東京都クラウドインフラ利用終了の申請（利用終了申請書）に基づき東京都クラウドインフラ管理者が実施する。 ・ 踏み台サーバーのログインユーザーは、東京都クラウドインフラ管理者より、踏み台サーバーの払出し時に提供する。以後の追加・削除・パスワードリセットは、利用者の申請（ユーザー申請（踏み台OS））に基づき東京都クラウドインフラ管理者が実施する。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	Ⅲ リスク対策（プロセス） 3. 特定個人情報の使用 リスク2 アクセス権限の管理	・アクセス権限については、情報セキュリティ責任者（統括）が全ての権限を一元的に管理しており、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定している。 ・ID管理簿の定期的な棚卸により、付与する権限に過不足が生じないようにし、どのIDにどのような権限が設定されているのかを把握できるようにしている。 ・IDの不適正利用が確認された場合は、システムセキュリティに係る内規により、当該IDの利用を制限する。 ・IDの一覧表は内部認証手続により、権限設定が適正であることを確認している。 ・医療費助成事務システムでは、IDにより管理に加え、二要素認証を用い、アクセス権限管理を行う。	【医療費助成事務システム】 ・アクセス権限については、情報セキュリティ責任者（統括）が全ての権限を一元的に管理しており、操作者の所属及び業務に合わせて、システムの機能ごとに「更新・参照可」、「参照のみ可」、「更新・参照不可」の権限を設定している。 ・ID管理簿の定期的な棚卸により、付与する権限に過不足が生じないようにし、どのIDにどのような権限が設定されているのかを把握できるようにしている。 ・IDの不適正利用が確認された場合は、システムセキュリティに係る内規により、当該IDの利用を制限する。 ・IDの一覧表は内部認証手続により、権限設定が適正であることを確認している。 ・IDにより管理に加え、二要素認証を用い、アクセス権限管理を行う。 【東京都クラウド】 ・AWS IAMにより職務に応じた最小権限の原則に基づくアクセス制御を実施している。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため

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
	Ⅳ リスク対策（その他） 1．監査 ②監査 具体的な内容	記述無し	【東京都クラウド】 デジタルサービス局が定める監査要綱に基づき、セキュリティ監査を実施しています。 実施サイクルは、内部監査を2年に1回、外部監査を5年に1回として計画しています。	事前	システム更改におけるオンプレからクラウドへの基盤変更のため
	（別添1）事務内容	審査会	審査会（特定個人情報ファイル）	事前	審査会でも特定個人情報を含む書類を扱うことを分かりやすくするため
	Ⅰ 基本情報 8．他の評価実施機関	東京都内各区市町村長、支払基金	東京都内各区市町村長、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	事前	支払基金名称変更
	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3③その他	中間サーバー	中間サーバー、医療費助成事務システム（精神通院）	事前	連携サーバーと医療費助成事務システム（精神通院）が連携しているため