資料75

個人情報保護管理運営会議　付議事項

件名	特定健康診査受診者の糖尿病治療中の者に対する保健指導等業務に係る外部結合等について（受渡方法の追加）

内容は別紙のとおり

要綱の根拠

◇第３条第１項第３号（外部結合、業務委託）

（担当部課：健康部健康づくり課）

事業の概要

事業名	糖尿病性腎症等重症化予防事業（新宿区国民健康保険事業（保健事業））
担当課	健康づくり課
目　的	新宿区特定健康診査受診者のうち、糖尿病の治療中で、血糖と腎機能が基準値を超えている者に対し、医療機関（かかりつけ医）と連携の上、保健指導を行い、糖尿病性腎症による透析等の合併症の発症を防止する。
対象者	新宿区特定健康診査受診者のうち、糖尿病の治療中で、血糖と腎機能が基準値を超えている者。
事業内容	１　概要 区では、糖尿病性腎症等の重症化を予防するため、糖尿病治療に関する十分な知識と経験を有した委託事業者に、当該予防事業の全体統括業務（スケジュール管理、参加勧奨業務、対象者からの問い合わせ等受電業務）や対面及び電話等（ＷＥＢ面談含む）による保健指導を委託している。（平成３０年度第９回、令和３年度第７回情報公開・個人情報保護審議会にて了承済） この度、ＬＧＷＡＮ回線による受渡し方法を追加することで、情報セキュリティ対策の向上や事務処理の効率化を図る。 ２　個人情報保護管理運営会議付議内容 （１）外部結合 対象者データ及び指導結果報告書の送付について、ＬＧＷＡＮ回線を通じ、委託事業者との間で外部結合を行う。 （２）業務委託 糖尿病性腎症等重症化予防の保健指導を行うため、業務の全体統括管理、保健指導及び報告書の作成業務を専門業者に委託する。 ３　予定対象者数 約２００名 ※個人情報の流れは、資料７５－１のとおり

別紙(電子計算機の外部結合関係)

◇外部結合(第３条第１項第３号)

件名　特定健康診査受診者の糖尿病治療中の者に対する保健指導等業務に係る外部結合について

※太字ゴシック（下線）は、令和３年度第７回情報公開・個人情報保護審議会了承済みの内容からの変更箇所

保有課（担当課）	健康づくり課
登録業務の名称	糖尿病性腎症等重症化予防事業
結合される情報項目（だれの、どのような項目か）	《個人の範囲》 糖尿病性腎症等重症化予防事業対象者 《委託先に処理させる項目》 氏名（カナ・漢字）、生年月日、性別、住所、電話番号、メールアドレス、特定健康診査の受診結果及びかかりつけ医における検査結果（身体測定結果、血圧測定、脂質検査、肝機能検査、血糖検査、尿検査、貧血検査、喫煙、腎機能検査）、傷病名、治療状況、保健指導における指示事項
結合の相手方	株式会社データホライゾン（プライバシーマーク、IS027001 取得事業者）
結合する理由	対象者データ及び指導結果報告書の受渡しにおいて、従来の電磁的媒体に加え、迅速かつ安全にデータを授受できるよう、**区イントラパソコンとLGWAN-ASP サービス提供事業者のサーバを結合する必要があるため。**
結合の形態	**地方公共団体を相互に接続する行政専用の総合行政ネットワーク「LGWAN」を利用し、区イントラネットパソコン（情報システム課が管理）と LGWAN-ASP サービス提供事業者のサーバとを接続する。**
結合の開始時期と期間	**令和７年４月１日から令和８年３月３１日まで**（次年度以降も、同様の外部結合を行う。）
情報保護対策	別紙チェックリストのとおり

別紙(業務委託)

◇業務委託(第３条第１項第３号)

件名　特定健康診査受診者の糖尿病治療中の者に対する保健指導業務の委託について（委託内容の変更）

保有課(担当課)	健康づくり課
登録業務の名称	糖尿病性腎症等重症化予防事業
委託先	株式会社データホライゾン（プライバシーマーク、IS027001 取得事業者）
委託に伴い事業者に処理させる情報項目（だれの、どのような項目か)	《個人の範囲》 糖尿病性腎症等重症化予防事業対象者 《委託先に処理させる項目》 氏名（カナ・漢字）、生年月日、性別、住所、電話番号、メールアドレス、特定健康診査の受診結果及びかかりつけ医における検査結果（身体測定結果、血圧測定、脂質検査、肝機能検査、血糖検査、尿検査、貧血検査、喫煙、腎機能検査）、傷病名、治療状況、保健指導における指示事項
処理させる情報項目の記録媒体	紙及び電磁的媒体（委託先のシステム及びＣＤ－Ｒ）
委託理由	糖尿病性腎症等重症化予防の保健指導を行うためには、業務の全体統括管理のもとで、十分な知識と経験がある専門業者に委託することで、より効率的に業務を行うため。
委託の内容	１　全体統括管理（スケジュール管理、報告書のとりまとめ、意見・苦情対応） ２　保健指導（対面、電話、手紙、ＷＥＢ） ３　報告書の作成業務
委託の開始時期及び期限	令和７年４月１日から令和８年３月３１日まで（次年度以降も、同様の外部結合を行う。）
委託にあたり区が行う情報保護対策	別紙チェックリストのとおり
受託事業者に行わせる情報保護対策	別紙チェックリストのとおり

糖尿病性腎症等重症化予防事業における個人情報の流れ（委託先が保健指導する場合）

（資料７５－１）

※赤字の部分が、今回の付議事項。

新宿区

国保データベースシステム

対象者データ

・氏名
・生年月日
・性別
・住所
・電話番号等

①対象者データ出力

イントラパソコン

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・通信内容の暗号化
・外部からの攻撃防御（ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等）
・ウィルス対策
・最新のパターンファイルの適用
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセス制御
・システムネットワーク状態等の監視
・アクセスログ取得
・サーバ冗長化　・バックアップ
・入退室管理
・国内法が適用されるサーバ環境

⑧保健指導結果の報告書を確認

・鍵付きカバン等による運搬
・受渡し時の管理簿への記載

②対象者データの提供（LGWAN回線またはCD-Rの手渡し）

【LGWAN回線】

通信暗号化

⑦保健指導結果の報告書を提出（LGWAN回線またはCD-Rの手渡し）

・鍵付きカバン等による運搬
・受渡し時の管理簿への記載

・特記事項等の遵守
・立入調査等及び状況報告
・責任者及び取扱者の報告
・区が作成した業務フローに基づく業務の履行
・データの暗号化
・鍵付きカバン等による運搬
・受渡し時の管理簿への記載
・鍵付キャビネット等での保管
・個人情報の返却及び消去
・事故等への対応体制及び手順の整備
・事故発生時等の協議

委託先

・特記事項等の遵守
・立入調査等及び状況報告
・責任者及び取扱者の報告
・区が作成した業務フローに基づく業務の履行
・データの暗号化
・鍵付きカバン等による運搬
・受渡し時の管理簿への記載
・鍵付キャビネット等での保管
・個人情報の返却及び消去
・事故等への対応体制及び手順の整備
・事故発生時等の協議

【委託先PC】

対象者データ

・氏名
・生年月日
・性別
・住所
・電話番号等
・メールアドレス等

・特定相手以外との通信不可
・ネットワーク機器やサーバの制御
・通信内容の暗号化
・外部からの攻撃防御（ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等）
・ウィルス対策
・最新のパターンファイルの適用
・ＩＤ／パスワード等認証
・ファイルのパスワード設定
・アクセス制御
・システムネットワーク状態等の監視
・アクセスログ取得
・サーバ冗長化　・バックアップ
・入退室管理
・国内法が適用されるサーバ環境

⑥保健指導結果の報告書を作成

③対象者へ対面、電話、手紙及びWEB面談の案内（電話・紙）

④対象者へWEB面談内容の通知（メール）

対象者

⑤対面、電話、手紙、WEB面談での保健指導を実施

4　外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
区が行う情報保護対策 【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。
	○	システム上で不要となった電子データを削除し、電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、結合先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに結合先と今後の対応を協議する。
区が行う情報保護対策 【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

4　外部結合にかかる個人情報保護対策チェックリスト

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
結合先に行わせる情報保護対策【運用上の対策】	○	個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	必要に応じて、事業者への立入り調査等を受けさせるとともに、結合先に対し速やかに状況報告をさせる。
	○	システム上で不要となった電子データを削除させ、電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
結合先に行わせる情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とさせる。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「－」	情報保護対策
委託にあたり区が行う情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。
	○	契約履行の間、特記事項に基づき立入り調査等を実施するとともに、委託先に対し速やかに状況報告をするよう指導する。
	○	取扱責任者及び取扱者をあらかじめ指定し、区に報告するよう指導する。
	○	全体の業務フローを作成し、委託先と共有する。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化する。また、電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用して、手渡しで行うよう指導する。
	○	個人情報を手交する場合は、鍵付きカバン等を使用して運搬する。
	○	個人情報の受渡しにあたっては、管理簿に記載する。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにする。
	○	個人情報は、施錠できる金庫又はキャビネット等に保管する。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却し、電子データは消去するよう指導する。また、区に電子データの消去を行ったことの報告書を提出するよう指導する。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、委託先と緊急時の連絡体制や対応手順を確認する。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに委託先と今後の対応を協議する。
委託にあたり区が行う情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定する。
	○	通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。
	○	入退室管理等により情報資産の危殆化を防止する。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。

5　業務委託にかかる個人情報保護対策チェックリスト

（電磁的媒体・紙媒体の取扱い）

	・対策が可能であれば「○」 ・対策の必要がない場合は「ー」	情報保護対策
委託事業者に行わせる情報保護対策【運用上の対策】	○	契約にあたり、「特記事項」を付すとともに、個人情報保護法及び新宿区情報セキュリティポリシーを遵守させる。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠させる。
	○	契約履行の間、特記事項に基づき立入り調査等を受けさせるとともに、委託先に対し速やかに状況報告をさせる。
	○	取扱責任者及び取扱者をあらかじめ指定させ、区に報告させる。
	○	区が作成した業務フローに基づき、業務を行わせる。
	○	個人情報を含むデータを作成する必要が生じた場合は、パスワードを付してデータを暗号化させる。電磁的媒体（DVD-R等）とパスワード通知書の受渡しは、それぞれ別の機会を設定し、鍵付きカバン等を使用させ、手渡しで行わせる。
	○	個人情報を手交する場合は、鍵付きカバン等を使用して運搬させる。
	○	個人情報の受け渡しにあたっては、管理簿に記載させる。管理簿には、日時、取扱者、情報の内容、数量を確認記録票に記録し、履歴を追跡できるようにさせる。
	○	個人情報は、施錠できる金庫又はキャビネット等に保管させる。
	○	業務履行後、個人情報が記録された電磁的媒体（DVD-R等）、紙媒体及びパスワード通知書は返却させ、電子データは消去させる。また、区に電子データの消去を行ったことの報告書を提出させる。
	○	業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備させ、区と緊急時の連絡体制や対応手順を確認させる。
	○	事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに区と今後の対応を協議させる。
委託事業者に行わせる情報保護対策【システム上の対策】	○	接続するネットワークについては、特定相手以外との通信を不可とする。
	○	ネットワーク機器やサーバを制御し、通信できるシステムを限定させる。
	○	通信内容は暗号化させ、通信途上の個人情報の盗用、改ざん、成りすましを防止させる。
	○	ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じさせ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御させる。
	○	コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用させる。
	○	ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止させる。
	○	個人情報を保存する場合は、保存先フォルダへアクセス権を設定させるとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底させる。
	○	システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得させる。取得したログは、定期的に分析させる。
	○	サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備させる。
	○	入退室管理等により情報資産の危殆化を防止させる。
	○	システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にさせる。