【資料２】
平成 27 年 3 月 25 日
総合政策局総合政策部統計課

千葉市・東京大学との共同研究におけるデータの取扱いについて(案)

１　趣旨

本取扱いは、平成２６年６月２５日付で締結した「千葉市と東京大学との共同研究に関する協定書」に基づいて行う健康・医療データ分析に関する個人情報の適正な取扱いについて必要な手順等を定める。

２　定義

本取扱いにおいて使用する用語の意味は次の通りとする。

用　語	意　味
本共同研究	平成２６年６月２５日付で締結した「千葉市と東京大学との共同研究に関する協定書」に基づいて行う千葉市と東京大学との共同研究
個人情報	生存する個人に関する情報であって、特定の個人が識別され、又は識別され得るもの(他の情報と容易に照合することができ、それにより、特定の個人を識別することができることとなるものを含む。)
連結不可能匿名化	個人を識別できないように、その人と新たに付された符号又は番号の対応表を残さない方法による匿名化
匿名化	個人情報から、当該情報に含まれる氏名、生年月日、住所等、個人を識別する情報を取り除くこと、又は連結不可匿名化を行うことにより、特定の個人を識別できないようにすること

３　分析目的

千葉市の国民健康保険事業及び介護保険事業における市民の健康増進及び医療費適正化に資する予防医療等の実現のために分析する。

４　分析テーマ及び分析対象データ

分析テーマ		主な分析対象データ
医療	特定の疾患に焦点を当てた発症抑制のための分析	国民健康保険被保険者データ
		レセプトデータ
		特定健康診査対象者データ
介護	要介護度の上昇抑制のための原因分析	介護保険被保険者データ
		後期高齢者医療保険被保険者データ
		国民健康保険被保険者データ
		レセプトデータ

※　研究の進捗により他のデータ(個人情報を含まないものに限る。)を分析対象としなければならない場合の当該データの取扱いは、本取扱いに従うものとする。

５　分析対象データの提供方法等

(1)　提供に関する基本的な考え方

千葉市は、分析対象データを次に掲げる区分に応じて個人情報を匿名化し、東京大学に提供する。

ア　特定の個人を識別する項目（例：氏名、電話番号等）については、項目を全て削除する。

イ　特定の個人の推定に繋がる項目（例：生年月日、住所等）については、項目に含まれる値の一部を削除する（例 H45.10.21 生→H45.10 生）

ウ　個人を識別する符号または番号（例：被保険者番号等）については、本共同研究において個人を識別するために用いる符号または番号については連結不可能匿名化し、本共同研究において個人を識別するために用いない符号または番号については削除する。

※　取り扱う個人情報と提供方法（介護保険被保険者データ及び後期高齢者医療保険被保険者データについては、国民健康保険被保険者データの提供方法に準じる。）

(ｱ) 被保険者に関する情報

a　特定の個人を識別する項目	国保	レセプト	特定健診
氏名	○	○	
電話番号		○	
口座番号	○		

☆ 提供方法：項目をすべて削除

b　特定の個人の推定に繋がる項目	国保	レセプト	特定健診
住所	○		○
生年月日	○	○	

☆ 提供方法

住所：郵便番号または町名までに置き換え

生年月日：生年月に置き換え

c　個人を識別する符号または番号	国保	レセプト	特定健診
被保険者証記号		○	○
被保険者証番号		○	○
広域被保険者番号			○
公費受給者番号		○	
国保番号	○		
個人番号	○	○	○
世帯番号	○	○	
保険証番号	○	○	
住民コード	○		
受給者番号		○	
整理番号		○	○
負担者番号		○	
世帯管理番号		○	
個人管理番号		○	
受診券整理番号			○

☆ 提供方法：項目をすべて削除したうえで連結不可能匿名化

(ｲ) 診療者に関する情報

a 特定の個人を識別する項目	国保	レセプト	特定健診
医師氏名		○	○
初回面接実施者			○
支援実施者			○
中間評価実施者			○
評価実施者			○

☆ 提供方法：項目をすべて削除

(2) 分析対象データ及びデータ分析結果の運搬方法

千葉市職員が、当該分析対象データ及びデータ分析結果を CD-R､USB メモリ等の外部メディア（以下

「外部メディア」という。）に、パスワードを設定したうえで保存し、持参する方法によるものとする。

６　セキュリティ対策

東京大学における、千葉市が東京大学に提供するデータ（5(1)の手法により個人情報を匿名化したデータ(以下「匿名化データ」という。)に限る。）の取扱いは以下のとおりとする。

(1) 管理体制

ア　東京大学は、本共同研究の実施のために保護管理者を一人置き、本共同研究における匿名化データを適切に管理する任に当たらせるものとする。

イ　6(1)アに規定する保護管理者は、保護担当者を一人又は複数人指定し、当該保護担当者に、保護管理者を補佐させ、匿名化データの管理に関する事務を担当させるものとする。

(2) 作業者の責務

本共同研究において匿名化データを取り扱う者（以下「作業者」という。）は、関連する法令及び規程等の定め並びに保護管理者及び保護担当者の指示に従い、匿名化データを取り扱うものとする。

(3) 個人情報の取扱い

ア　保護管理者は、匿名化データの秘匿性等その内容に応じて、当該匿名化データにアクセスする権限を有する者をその利用目的を達成するために必要最小限の作業者に限定するものとする。

イ　アクセス権限を有しない作業者は、匿名化データにアクセスしてはならない。

ウ　作業者は、アクセス権限を有する場合であっても、業務上の目的以外の目的で匿名化データにアクセスしてはならない。また、特定の個人を再識別化してはならない。

エ　匿名化データ及び分析結果は、千葉市と東京大学との共同研究に関する協定書における秘密情報として取り扱う。

オ　匿名化データを取扱う場所は東京大学内に限るものとする。なお、作業する端末は、作業者の退席後一定時間操作がない場合は、スクリーンセーバーにより画面をロックし、復帰時には再度認証を行う、また、保護管理者以外の者はプログラムのインストールができない設定とする。

カ　作業者は、保護管理者の指示に従い、匿名化データが記録されている媒体（(4)ケにより書き出された外部メディアを含む。）を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行うものとする。

キ　作業者は、匿名化データ又は匿名化データが記録されている媒体（端末及びサーバに内蔵されているものを含む。）が不要となった場合には、保護管理者の指示に従い、当該匿名化データの復元又は判読が不可能な方法により当該情報の消去又は当該媒体の廃棄を行うものとする。

ク　保護管理者は、匿名化データの秘匿性等その内容に応じて、台帳等を整備する方法により、当該匿名化データの利用及び保管等の取扱いの状況について記録し、定期的に又は千葉市の求めに応じて、千葉市に報告するものとする。

(4)　情報システムにおける安全の確保等

ア　保護管理者は、匿名化データの秘匿性等その内容に応じて、パスワード等（パスワード、ＩＣカード、生体情報等をいう。以下同じ。）を使用して権限を識別する機能（以下「認証機能」という。）を設定する等のアクセス制御のために必要な措置を講ずるものとする。

イ　保護管理者は、(4)アの措置を講ずる場合には、パスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

ウ　保護管理者は、匿名化データの秘匿性等その内容に応じて、作業を行う端末及び当該匿名化データへのアクセス状況を記録し、その記録（以下「アクセス記録」という。）を一定の期間保存し、及びアクセス記録を定期に又は随時に分析するために必要な措置を講じ、定期的に又は千葉市の求めに応じて、千葉市に報告するものとする。

エ　保護管理者は、アクセス記録の改ざん、窃取又は不正な消去の防止のために必要な措置を講ずるものとする。

オ　保護管理者は、匿名化データを取り扱う情報システムへの外部からの不正アクセスを防止するため、ファイアウォールの設定等の必要な措置を講ずるとともに、ＩＤ及びパスワードによる認証を行うものとする。なお、処理を行う端末（インターネットを含む外部とのネットワーク接続を一切行わないものでなければならない。）は、保護管理者が必要と認めた場合以外には移動してはならず、また、当該パスワードは定期的に変更するものとする。

カ　保護管理者は、コンピュータウイルスによる匿名化データの漏えい、滅失又はき損の防止のため、ウイルス対策ソフト（最新の対策ファイルに随時更新したもの）の導入や随時の外部メディアのウイルスチェックなどコンピュータウイルスの感染防止等に必要な措置を講ずるものとする。

キ　保護管理者は、匿名化データの秘匿性等その内容に応じて、その暗号化のために必要な措置を講ずるものとする。

ク　保護管理者は、匿名化データの秘匿性等その内容に応じて、市の承認を得たうえで、その処理を行う端末を限定し、当該端末の盗難又は紛失の防止のため、端末の固定又は執務室の施錠等の必要な措置を講ずるものとする。

ケ　作業者は、データを外部メディアに書き出す場合は、保護管理者の許可を得たうえで、データの暗号化、パスワードの設定等の保護措置を行うものとする。

コ　作業者は、保護管理者が必要があると認めるときを除き、(4)クの端末を外部へ持ち出してはならず、また、当該端末の使用に当たっては、匿名化データが第三者に閲覧されることがないよう、使用状況に応じて情報システムからログオフを行うことを徹底する等の必要な措置を講ずるものとする。

(5)　情報システム室等の安全管理

ア　保護管理者は、匿名化データを取り扱う基幹的なサーバ等の機器を設置する室等（以下「情報システム室等」という。）を限定するとともに、当該情報システム室等に入室する権限を有する者を限定し、用件の確認、入退室の記録、部外者についての識別化、部外者が入室する場合の職員の立会い等の措置を講ずるものとする。また、匿名化データを記録する媒体を保管するための施設を設けている場合においては、必要があると認めるときは、同様の措置を講ずるものとする。

イ　保護管理者は、必要があると認めるときは、情報システム室等の出入口の特定化による入退室の管理の容易化、所在表示の制限等の措置を講ずるものとする。

ウ　保護管理者は、情報システム室等及び保管施設の入退室の管理について、必要があると認めるときは、入室に係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講ずるものとする。

エ　作業者は、文書の出力は必要最小限とし、当該文書を鍵付きのキャビネットで管理しなければならず、情報システム室等から持ち出す場合には、保護管理者の許可を得たうえで、台帳に目的、作業者名、持参先を記録するものとし、また、返却の際は、他の作業者をもって現物確認を行うものとする。

オ　作業者は、(5)エの規定により出力した文書について不要となった場合は、保護管理者の許可を得たうえで、速やかに当該文書をシュレッダー処理しなければならない。

カ　保護管理者は、外部からの不正な侵入に備え、情報システム室等に施錠装置、警報装置、監視設備の設置等の措置を講ずるものとする。

キ　保護管理者は、災害等に備え、情報システム室等に、耐震、防火、防煙、防水等の必要な措置を講ずるとともに、サーバ等の機器の予備電源の確保、配線の損傷防止等の措置を講ずるものとする。

(6)　安全確保上の問題への対応

ア　匿名化データの漏えい等安全確保の上で問題となる事案が発生した場合に、その事実を知った作業者は、速やかに保護管理者に報告するものとする。

イ　保護管理者は、被害の拡大防止又は復旧等のために必要な措置を講ずるとともに、事案の発生した経緯、被害状況等を直ちに千葉市に報告するものとする。

ウ　保護管理者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずるとともに、その対策等について千葉市の承認を得るものとする。

エ　千葉市及び東京大学は、事案の内容、影響等に応じて、事実関係及び再発防止策の公表、当該事案に係る本人への対応等の措置を講ずる。

(7)　計画書の作成、点検・報告の実施

ア　東京大学は、保護管理者をもって、(1)から(6)までに掲げる事項を包含し、また内容が確認できるセキュリティ対策をまとめさせ、データ提供を開始する１か月前にセキュリティ計画書として千葉市に提出し、承認を得なければならない。

イ　(7)アの計画書の提出は、東京大学内の関連規程等に定めるところにより必要となる諸手続きを行ったうえで行うものとする。

ウ　東京大学は、(7)イの手続の結果、この取扱いに定めるセキュリティ対策を上回るセキュリティ対策を行うこととなる場合は、この取扱いによるセキュリティ対策としてその基準を順守する責務を負うものとする

エ　東京大学は、保護管理者をもって、定期的又は千葉市の求めに応じて、匿名化データの管理の状況について、別紙チェックリストに基づき点検を行わせ、その結果を(3)ク及び(4)ウに掲げる事項と共に千葉市に報告するものとする。

オ　7(ｴ)の場合において、千葉市は、必要に応じ、東京大学に報告を求め又は実地に検査することができるものとし、東京大学は、保護管理者等をもって市の報告又は検査に誠実に協力しなければならない。

カ　東京大学は、千葉市が提供したデータについて、本共同研究の終了時に、復元又は判読が不可能な方法により、データの消去又は当該媒体の廃棄を行う（千葉市から提供した外部メディアについては返却し、千葉市の確認を受けるものとする。）ものとする。

キ　千葉市及び東京大学は、匿名化データの適切な管理のための措置について、点検・報告の結果等を踏まえ、実効性等の観点から評価し、必要があると認めるときは、その見直し等の措置を講ずるものとする。

共同研究実施の各場面において想定されるリスク及びその対策　1/2

	本共同研究における各場面におけるリスク及びその対策	該当項目
1	**千葉市から東京大学にデータを運搬する際のメディアの紛失、盗難等によるリスク**	
	(1)東京大学に提供するデータを匿名化データに限定	5(1)
	(2)データをメディアに収録する際のパスワードの設定	5(2)
	(3)千葉市職員の持参によるメディアの受渡し	5(2)
2	**東京大学におけるメディアの紛失等のリスク**	
	(1)責任体制の明確化	
	ア　保護管理者（本共同研究における総括責任者）の設置。	6(1)ｱ
	イ　保護管理者による一元的なデータ管理（保護担当者の指定）	6(1)ｲ
	ウ　作業者による適法かつ保護管理者の命に沿ったデータ管理	6(2)
	(2)個人情報取扱いの厳格化	
	ア　作業者の限定	6(3)ｱ､ｲ
	イ　業務上の目的外でのデータへのアクセスの禁止等	6(3)ｳ
	ウ　データの位置づけの明確化	6(3)ｴ
	エ　作業場所の限定	6(3)ｵ
	オ　保管する方法・場所の限定	6(3)ｶ
	カ　データ廃棄方法の明確化	6(3)ｷ
	キ　データの利用・保管の状況の記録	6(3)ｸ
	ク　ア～キについての千葉市への定期・随時の報告	6(3)ｸ
	ケ　各種災害対策	6(5)ｷ
3	**東京大学における権限のない者による不正操作等によるリスク**	
	(1)作業環境の物的整備	
	ア　作業室の管理の厳格化	6(5)ｱ
	イ　不正アクセス防止のためのファイアウォールの設定等	6(4)ｵ
	ウ　ウイルス対策の措置	6(4)ｶ
	エ　データの暗号化のための必要な措置	6(4)ｷ
	(2)作業環境の体制整備	
	ア　保護管理者によるパスワード管理等	6(4)ｱ､ｲ､ｴ
	イ　作業端末にプログラムをインストールする者の限定	6(3)ｵ
	ウ　作業を行わないときの端末のログオフの徹底、復帰時の再認証等	6(4)ｺ､(3)ｵ
	エ　データへのアクセス状況の記録及び千葉市への報告	6(4)ｳ
	オ　データの利用・保管の状況についての千葉市への定期・随時の報告	6(3)ｸ
4	**端末の紛失、盗難、破壊（ウイルス感染によるものも含む。）等によるリスク**	
	(1)作業室の管理の厳格化	6(5)ｱ､ｲ､ｳ
	(2)執務室の施錠等	6(4)ｸ
	(3)作業端末のウイルス対策の措置	6(4)ｶ
	(4)外部メディアのウイルスチェック	6(4)ｶ
	(5)作業室への警報装置・監視設備等の設置	6(5)ｶ
	(6)データの利用・保管の状況についての千葉市への定期・随時の報告	6(3)ｸ
5	**外部メディア等に書き出したデータの盗難、紛失等のリスク**	
	(1)外部メディアへデータを書き出す際の暗号化処理	6(4)ｹ
	(2)データの利用・保管の状況についての千葉市への定期・随時の報告	6(3)ｸ

共同研究実施の各場面において想定されるリスク及びその対策　2/2

本共同研究における各場面におけるリスク及びその対策		該当項目
6	出力した文書の紛失等のリスク	
	(1)出力した文書の管理の厳格化(鍵付きキャビネットでの保管、持ち出す際の記録、返却の際の他者の確認)	6(5)ｴ
	(2)出力した文書の廃棄	6(5)ｵ
	(3)データの利用・保管の状況についての千葉市への定期・随時の報告	6(3)ｸ
7	コンピュータネットワーク等を通じての流出、改ざん等のリスク	
	(1)作業端末の外部ネットワークとの遮断	6(4)ｵ
	(2)データの利用・保管の状況についての千葉市への定期・随時の報告	6(3)ｸ
8	漏えい事故が発生した場合の被害拡大のリスク	
	(1)事故発生時の東大内での報告	6(6)ｱ
	(2)拡大防止・復旧のための応急措置の実施、経緯等の千葉市への連絡	6(6)ｲ
	(3)原因分析及び再発防止策等の実施	6(6)ｳ
	(4)事実関係の公表及び被害者等への対応	6(6)ｴ
9	共同研究終了後に、データが継続保有されることのリスク	
	(1)データ廃棄方法の明確化	6(3)ｷ
	(2)データの利用・保管の状況の記録	6(3)ｸ
	(3)データの利用・保管の状況についての千葉市への定期・随時の報告	6(3)ｸ
	(4)本共同研究終了時のデータの消去、メディアの返却等	6(7)ｶ