資料２

公表資料

医療分野の研究開発に資するための匿名加工医療情報に関する法律の医療情報取扱事業者等である個人情報取扱事業者に対する個人情報の保護に関する法律に基づく行政上の対応について

令和４年●月●日
個人情報保護委員会

個人情報保護委員会は、医療分野の研究開発に資するための匿名加工医療情報に関する法律（以下「次世代医療基盤法」という。）の医療情報取扱事業者（以下「医療機関」という。）である９医療機関、医療機関の委託先である一般社団法人ライフデータイニシアティブ（以下「ＬＤＩ」という。）及び医療機関の再委託先である株式会社エヌ・ティ・ティ・データ（以下「ＮＴＴデータ」という。）に対し、令和４年●月●日に個人情報の保護に関する法律（以下「個人情報保護法」という。）第 144 条に基づく指導を行った。

事案の概要、漏えいした医療情報の件数並びに個人情報保護法上の指導の原因となる事実及び指導の内容は以下のとおり。

１．事案の概要

医療機関は、医療情報の管理等の業務をＬＤＩに委託し、ＬＤＩは、当該業務をＮＴＴデータに再委託している（以下「医療情報取扱事業」という。）。

本件は、医療機関の再委託先としてのＮＴＴデータ（以下「再委託先ＮＴＴデータ」という。）が、プログラムの設定ミス等により、医療情報取扱事業の運用を開始した令和２年９月から令和４年７月 15 日までの間、次世代医療基盤法第 30 条第１項柱書の通知（以下「通知」という。）が行われていない患者（以下「未通知患者」という。）の医療情報を、次世代医療基盤法の認定匿名加工医療情報作成事業者（以下「認定事業者」という。）及び認定医療情報等取扱受託事業者（以下「認定受託事業者」という。）としてのＬＤＩ及びＮＴＴデータ（以下、認定事業者としてのＬＤＩを「認定ＬＤＩ」、認定受託事業者としてのＮＴＴデータを「認定受託ＮＴＴデータ」という。）に漏えい（意図せず提供）した事案。

２．漏えいした医療情報の件数

再委託先ＮＴＴデータが漏えいした未通知患者の医療情報は、下記表のとおり、15 医療機関、94,579 名分である（15 医療機関から提供された医療情報の全体は、令和４年６月末時点で、約 300 万名分の患者の医療情報である。）。このうち、６医療機関（網掛け表示分）は地方独立行政法人であり、本件発生時点で個人情報保護法は適用されないことから、個人情報保護法の適用対象となる９医療機関から提供された医療情報のうち、漏えいした人数は 44,395 名分となる。

番号	医療機関	漏えいした未通知患者の医療情報の数（名）
1	北見赤十字病院	27
2	医療法人鉄蕉会　亀田総合病院	2
3	社会医療法人財団董仙会　恵寿総合病院	4,137
4	地方独立行政法人岐阜県立多治見病院	17
5	地方独立行政法人静岡県立病院機構　静岡県立総合病院	15,722
6	地方独立行政法人静岡県立病院機構　静岡県立こども病院	7,055
7	日本赤十字社愛知医療センター名古屋第一病院	11,274
8	京都大学医学部附属病院	15,365
9	大阪赤十字病院	422
10	公益財団法人田附興風会医学研究所北野病院	173
11	地方独立行政法人神戸市民病院機構　神戸市立医療センター西市民病院	6,395
12	地方独立行政法人神戸市民病院機構　神戸市立医療センター中央市民病院	20,993
13	地方独立行政法人神戸市民病院機構　神戸市立西神戸医療センター	2
14	独立行政法人労働者健康安全機構　熊本労災病院	247
15	宮崎大学医学部附属病院	12,748
	合計	94,579

３．指導の原因となる事実

⑴　本件の特性と問題の所在

ア　本件は、個人情報保護法の特別法として制定された次世代医療基盤法上の医療機関等が関与する事案である。個人情報保護法においては、要配慮個人情報をオプトアウトにより第三者に提供することはできないところ、次世代医療基盤法においては、本人に対して一定の事項を通知する等の同法に定める手続を履践することにより、提供停止の求めを行っていない本人に係る医療情報について、①医療機関等から認定事業者へ要配慮個人情報である医療情報を提供することができることに加えて、さらに、②認定事業者から利活用者へ匿名加工医療情報を提供することができる特例を認めている。医療機関は、個人情報保護法上の個人情報取扱事業者であるところ、多数の患者の要配慮個人情報を含む個人データである医療情報を日常的に取り扱っている。自己の生命身体に関する極めて機微な情報である医療情報を本人たる患者が医療機関に提供する趣旨は、治療のためにこれを包み隠さず伝えることが不可欠であるという特殊性に起因する。すなわち、医療情報は、患者が治療という目的を達成するために選択の余地が極めて乏しい中で提供した情報であるという側面を持っているのであり、当該個人データの性質及びその量からすると、漏えい等が発生した場合のリスクは特に高く、医療機関においてはこれを常に意識し、当該個人データの取扱いに関して個人情報保護法を厳に遵守すること、とりわけ、高い水準の安全管理措置等を講じることが求められる。

また、医療情報に係る患者本人は、次世代医療基盤法に基づき、医療機関による認定事業者への医療情報の提供の停止を求める権利を有するところ、未通知患者の医療情報が認定事業者に提供されることは、患者本人が医療情報に関して有する権利行使の機会を奪うもの（通知がされていなければ、患者本人は、医療情報が認定事業者に提供されていることを認知できず、権利を有していること自体を認知できない。）であり、そのような事態が生じないようにする観点からも、とりわけ、高い水準の安全管理措置等を講じることが求められる。

さらに、委託先であるＬＤＩ（以下「委託先ＬＤＩ」という。）及び再委託先ＮＴＴデータは、複数の医療機関から医療情報の管理等の業務の委託を受け、委託に伴って多数の医療情報の提供を受けており、両社においても、とりわけ、高い水準の安全管理措置等を講じることが求められる。

イ　本件は、ＮＴＴデータ内の医療情報取扱事業領域から次世代医療基盤法認定事業領域における漏えい事案であり、外見上は同一事業者内とも見えるが、その本質は、医療機関から認定事業者及び認定受託事業者への漏えいであるから、このことにより、各当事者の責任が減じられるものではない。むしろ、個人データを提供する者と提供される者が、同一の事業者であるという本件の特質を踏まえると、規律が緩まることなく、逆に、なれ合いを防止する観点から、とりわけ、高い水準の安全管理措置等を講じることが求められる。

ウ　本件では、各当事者において、いずれも、その責任に見合った高い水準の安全管理措置等を講じられていたとは言い難い。

本件漏えいが事業開始当初から長期間発見されなかったことにも鑑みると、当該体制を生み出した各当事者において、改めて、根本的な意識改革を促す必要がある。

⑵　各事業者における事実

本件では、医療情報の提供停止の求めがあった患者に係る全ての医療情報を確実に除外するために、同一人のデータと疑われるデータが幅広く紐付く設計としていたところ、当該設計を他の患者に係る医療情報の処理にも使用した結果、通知済みの患者の医療情報に未通知患者の医療情報が紐付けされた。さらに、医療情報取扱事業領域から次世代医療基盤法認定事業領域に医療情報を移動する際に、未通知患者の医療情報が削除されていることを確認する仕組みが構築されていなかったことから、未通知患者情報の漏えいを覚知する端緒自体、存在しなかったため、被害の拡大及び長期化が生じた。

ア　９医療機関

９医療機関は、ＬＤＩとの間において、医療情報の提供に関する契約を締結しているところ、当該契約において、９医療機関は、ＬＤＩに対

し、ＬＤＩによる医療情報等の取扱状況の報告を求めることができる旨定められている。

しかし、９医療機関では、委託先ＬＤＩにおける医療情報の取扱状況の報告を適切に求めておらず、委託先ＬＤＩ及び再委託先ＮＴＴデータにおける医療情報の取扱状況を十分に把握していないなど、９医療機関における委託先ＬＤＩ及び再委託先ＮＴＴデータの監督が不十分であった。

イ　ＬＤＩ

委託先ＬＤＩでは、再委託先ＮＴＴデータに個人データの取扱いに関するシステム開発を全面的に委託していたにもかかわらず、その漏えい等防止措置の妥当性に関する検討を自ら行わず、再委託先ＮＴＴデータが提示した方策の確認や事後の検証を行っていないなど、再委託先ＮＴＴデータの個人データの取扱状況に関する委託先の監督が不十分であった。

ウ　ＮＴＴデータ

本件において、再委託先ＮＴＴデータでは、認定ＬＤＩ及び認定受託ＮＴＴデータに医療情報を提供するに当たり、医療情報の提供停止の求めがあった患者に係る全ての医療情報を確実に除外するために、同一人のデータと疑われるデータが幅広く紐付く設計としていた。しかし、当該設計を他の患者に係る医療情報の処理にも使用した結果、通知済みの患者の医療情報に未通知患者の医療情報が紐付けされたものであり、開発責任者やプロジェクトの責任者による確認不足、ひいては、ＮＴＴデータによるシステム開発（プログラム設定）の妥当性の確認不足があった。さらに、未通知患者の医療情報が含まれていないことを確認する仕組みを構築していなかった。

また、次世代医療基盤法認定事業領域内に未通知患者が提供されるなど法令に違反するおそれのあるデータを検知した場合の報告連絡体制や報告の目標時間に係る規定の運用が十分に機能していなかった。

４．個人情報保護法第 144 条に基づく指導の内容

⑴　９医療機関

委託先の監督として、個人データの取扱いの全部又は一部を委託する場合には、委託先において当該個人データについて安全管理措置が適切に講じられるよう、委託先に対し必要かつ適切な監督（委託先における個人データの取扱状況の把握を含む。）を行うこと。

また、委託先が再委託を行おうとする場合には、再委託先における委託された個人データの取扱状況を把握するために、委託先を通じて又は必要に応じて自らが、定期的に監査を実施すること。

⑵　ＬＤＩ

委託先の監督として、再委託先ＮＴＴデータに個人データに関するシステム開発（修正を含む。）を委託する場合には、その漏えい等防止措置の妥当性に関する検討を自ら行うとともに、再委託先ＮＴＴデータが提示した方策の確認や、事後（システム稼働後）の検証を継続的に行うこと。

情報管理責任者による再委託先ＮＴＴデータの月次の管理・監督の対象について、情報セキュリティに加えて、再委託先ＮＴＴデータにおいて、未通知患者の医療情報が適切に削除されているかなど、個人データの取扱状況の把握を行うこと。

⑶　ＮＴＴデータ

ア　組織的安全管理措置（取扱状況の把握及び安全管理措置の見直し）、技術的安全管理措置（情報システムの使用に伴う漏えい等の防止）

システム開発（プログラムの修正を含む。）に当たっては、開発開始からリリースまでの各プロセスにおいて、システム開発（プログラム設定）の妥当性（漏えい等防止措置の妥当性）を確認するプロセスを改善すること。

なお、本件を踏まえた着眼点の一つとして、自社の責任者による確認だけではなく、委託先や外部の有識者による妥当性の確認を経ること。

さらに、未通知患者の医療情報が削除されていることを確認する仕組みを構築すること。

イ　組織的安全管理措置（漏えい等事案に対応する体制の整備）、人的安全管理措置

漏えい等事案の発生又は兆候を把握した場合その他個人情報保護法違反の事実を把握した場合の責任者への報告連絡体制や報告の目標時

間を整備すること。

さらに、当該連絡体制等の整備に関して、医療情報取扱事業及び次世代医療基盤法認定事業に従事する責任者を含む従業者に定期的な教育を実施すること。

全ての従業者に対して年１回実施しているセキュリティインシデントに対する訓練において、本件と同様の漏えい等事案の発生又は兆候を把握した場合その他個人情報保護法違反のインシデントの訓練内容を改善すること。

各事業者は、⑴ないし⑶に対応する再発防止策を策定するとともに、実施状況（予定も含む）を、令和４年 12 月 28 日（水）までに報告すること。

（以　上）