資料１

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おける再発防止策の策定及び実施状況

令和５年１月18日　個人情報保護委員会

- 個人情報保護委員会は、９医療機関（注）、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。）及び株式会社エヌ・ティ・ティ・データ（以下「ＮＴＴデータ」という。）の計11法人に対し、令和４年11月２日に指導を行い、同年12月28日を期日とし再発防止策の策定及び実施状況について報告を求めていた。
- 今回の再発防止策の策定及び実施状況に関して、現時点では特に問題は見当たらない。当委員会としては、前記11法人が、前記再発防止策を確実に実施することなどを、引き続き注視していく。

注　北見赤十字病院、医療法人鉄蕉会亀田総合病院、社会医療法人財団董仙会恵寿総合病院、日本赤十字社愛知医療センター名古屋第一病院、京都大学医学部附属病院、大阪赤十字病院、公益財団法人田附興風会医学研究所北野病院、独立行政法人労働者健康安全機構熊本労災病院、宮崎大学医学部附属病院を指す。

１．９医療機関

	事実概要	指導概要	策定した再発防止策及び実施状況
委託先の監督	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、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。	・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。 ・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。	・委託先ＬＤＩに対し、委託先及び再委託先における個人データの取扱状況について月次で報告させるとともに、各医療機関においてその内容を確認することを通じて管理・監督を行う。さらに、必要に応じて、各医療機関において監査等を実施する。 また、委託先ＬＤＩに対し、安全管理措置について年に１回以上報告させるとともに、各医療機関においてその内容を確認することを通じて管理・監督を行う。

２．ＬＤＩ

	事実概要	指導概要	策定した再発防止策及び実施状況
委託先の監督	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。 さらに、情報管理責任者による月次の管理・監督は、システムログのアクセス状況やセキュリティルームにおけるセキュリティ対策の実施状況といった情報セキュリティを対象としたものであり、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していなかった。	・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。 ・再委託先ＮＴＴデータにおいて、漏えい等事案の発生又は兆候を把握した場合など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個人情報保護法ガイドラインで定めている個人情報保護委員会への報告期限を遵守できる報告の目標時間を整備していること、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していることなどを確認すること。	・ＮＴＴデータにおいて、システム要件定義時に有識者レビューを確実に実施させるとともに、ＬＤＩにおいて、システム要件定義、ＡＰ（アプリケーション）外部設計及びリリース判定時に確認・承認を必須とするプロセスに改善する。さらに、システム稼働後、漏えい等防止措置の妥当性について、ＬＤＩ及びＮＴＴデータ双方で確認し、ＬＤＩにおいて承認するプロセスに改善する。 ・情報セキュリティ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、未通知患者の医療情報が存在していないことをＬＤＩ及びＮＴＴデータ双方で確認し、ＬＤＩが承認するプロセスに改善する。さらに、漏えい等防止措置全般について、ヒヤリハットを含めたインシデントをＬＤＩ及びＮＴＴデータ双方で共有し、ルールの変更等により改善する。 ・ＮＴＴデータにおいて、漏えい等事案の発生又は兆候を把握した場合など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を、各階層への同報展開に変更するとともに、個人情報保護法ガイドラインで定めている個人情報保護委員会への報告期限を遵守できる報告の目標時間を整備する。 また、ＮＴＴデータと連携して、漏えい等事案の発生又は兆候を把握した場合の連絡体制等を含む教育・訓練に関する方針を改定し、ＮＴＴデータにおいて、従業者に対し年１回以上の教育等を実施し、ＬＤＩに報告させる（今年度は令和４年11月30日までに実施済）。

３．ＮＴＴデータ

	事実概要	指導概要	策定した再発防止策及び実施状況
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）及び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）	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よう３段階の紐付け処理を行う設計としていた。 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、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。	・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ＬＤＩや外部の有識者による妥当性の確認を経ること。 ・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。	・システム要件定義時に他部署（法務部や情報セキュリティ推進室等）による有識者レビュー（必要に応じて外部の有識者による確認を含む。）を確実に実施するとともに、システム要件定義、ＡＰ外部設計及びリリース時にＬＤＩの承認を必須とするプロセスに改善する。 ・確実に同一人と確認できる識別番号の突合のみを行う紐付け処理などプログラムの改修を行うとともに、改修後のプログラムテスト結果について、ＬＤＩ及び第三者の確認を行った。さらに、医療機関における医療情報の提供に関する事前通知運用を開始した日と診療年月を比較し、未通知患者の医療情報が認定医療情報等取扱受託事業者等に提供されないプログラムの追加を行うとともに、追加後のプログラムテスト結果について、ＬＤＩ及び第三者の確認を行った。
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）及び人的安全管理措置	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。	・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個人情報保護法ガイドラインで定めている個人情報保護委員会への報告期限を遵守できる報告の目標時間を整備すること。 ・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。	・ＮＴＴデータの責任者への報告連絡体制を、段階ごとの報告から各階層への同報展開に変更するとともに、緊急時連絡体制に個人情報保護委員会への報告目標時間を明記する。 ・ＬＤＩと連携して、漏えい等事案の発生又は兆候を把握した場合の連絡体制等を含む教育・訓練に関する方針を改定し、当該方針に基づいて、従業員に対し年１回以上の教育を実施する（今年度は令和４年11月30日までに実施済）。 ・全ての従業員に対して年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、訓練内容に本件と同様の法違反のインシデントを追加する（今年度は令和５年３月に実施予定）。さらに、全社で年１回実施している「情報セキュリティ／個人情報保護ＩＢＴ」（インターネットを活用した試験方式）において、本件に関する課題を追加する（令和５年６月までに実施予定）。