

日時：令和5年1月18日（水）14：30～

場所：個人情報保護委員会 委員会室

出席者：丹野委員長、小川委員、中村委員、大島委員、浅井委員、加藤委員、藤原委員、梶田委員、高村委員、松元事務局長、三原事務局次長、山澄審議官、森川総務課長、吉屋参事官、栗原参事官、香月参事官、小嶋参事官、片岡参事官、石田参事官、松本研究官

○森川総務課長 それでは、定刻になりましたので、会議を始めます。

本日は、全委員が御出席となっております。

以後の委員会会議の進行につきましては、丹野委員長にお願いいたします。

○丹野委員長 それでは、ただいまから、第229回個人情報保護委員会を開会いたします。

本日の議題は一つでございます。

議題1「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について」、事務局から説明をお願いいたします。

○事務局 説明させていただきます。

(内容について一部非公表)

資料1を御覧ください。9医療機関、LDI、NTTデータにおける再発防止策の策定及び実施状況を取りまとめた表でございます。

一番下の「3. NTTデータ」から御説明をさせていただきます。

一つ目の事実概要として、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定としておりましたが、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ございまして、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の妥当性の確認不足がございました。

さらに、医療情報を次世代医療基盤法認定事業領域に移動する際に、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という事実がございます。

こちらについて二つ指導しており、一つ目として、システム開発に当たっては、開発開始からリリースまでの各プロセスにおいて、システム開発の妥当性を確認するプロセスを改善すること、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なく、委託先のLDIや外部の有識者による妥当性の確認を経ること、二つ目として、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を指導しております。

こちらに対して、一番右に二つございますが、一つ目として、システム要件定義時に、

システム開発部署以外の他部署である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みますが、これらを確実に実施するとともに、システム要件定義からリリースまでの段階において、LDIの承認を必須とするプロセスに改善をしております。

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については、プログラムを追加し、追加後のプログラムテストの結果については、LDIや第三者による確認を行っております。

二つ目の事実概要として、本件は、発覚から当委員会までの報告が遅れているところ、報告連絡体制や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という問題がございます。

こちらについて三つ指導しており、一つ目として、個人情報保護法違反の事実等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、二つ目として、当該連絡体制等の整備に関して、従業員に定期的な教育を実施すること、三つ目として、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、本事案と同様のインシデントの訓練内容を改善することを指導しております。

こちらに対して、一つ目として、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、緊急時の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こととしております。

二つ目として、LDIと連携して、連絡体制を含む教育・訓練に関する方針を改定し、当該方針に基づき、従業員に対して年1回以上の教育を実施することとしており、こちらについては、昨年11月30日までに実施済みでございます。

三つ目として、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、本事案と同様のインシデントを訓練内容に追加することとしております。こちらは3月に実施する予定でございます。

また、全社で年1回実施しているインターネットを活用した試験において、本件に係る課題を追加することとしており、こちらについては、6月までに実施予定でございます。

一つ上の「2. LDI」でございます。事実概要として、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、事後の検証を行っていないなど、委託先の監督が不十分であった、情報管理責任者による月次の管理・監督は、情報セキュリティを対象としたもので、個人データの取扱状況の把握をしていなかった、という問題点がございました。

こちらについて、三つ指導をしております。一つ目として、再委託先のNTTデータに個人データに関するシステム開発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、NTTデータが提示した方策の確認や事後（システム稼働後）の検証も継続的に行うこと、二つ目として、情報管理責任者による月次の管理・監

督の対象に個人データの取扱状況を含めること、三つ目として、NTTデータにおいて、個人情報保護法違反の事実が発覚した場合の責任者への報告連絡体制や報告期限を遵守できる目標時間を整備していること、定期的な教育を実施していること等を確認することの3点でございます。

こちらに対して、NTTデータと表裏の関係になりますけれども、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、システム要件定義からリリース判定までに確認・承認を必須とするプロセスに改善しております。さらに、システム稼働後については、漏えい等防止措置の妥当性について双方で確認し、LDIにおいて承認するプロセスに改善をしております。

情報セキュリティ責任者による月次の管理・監督の対象については、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双方で確認し、LDIが承認するプロセスに改善をしております。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双方で共有し、必要に応じてルールの変更等により改善することとしております。

また、NTTデータで実施した訓練や報告連絡体制が改善されていることを確認するとともに、従業員教育についてもLDIに報告をさせて報告内容を確認しているところでございます。

最後に、「1.9 医療機関」でございます。

事実概要としては、契約書において、LDIに対し医療情報等の取扱状況の報告を求められる旨が定められておりましたが、取扱状況を十分に把握していないなど、委託先のLDI、再委託先のNTTデータの監督が不十分でございました。

こちらについて、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、委託先に対する必要かつ適切な監督を行うこと、再委託を行う場合には、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、定期的に監査することを指導しております。

こちらに対して、委託先の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、各医療機関それぞれにおいてその内容を確認することを通じて管理・監督を行うこととしております。さらに、必要に応じて、各医療機関それぞれにおいて監査等を実施する予定でございます。

また、委託先のLDIに対して、安全管理措置について年1回以上報告させるとともに、各医療機関それぞれにおいてその内容を確認することを通じて管理・監督を行うこととしております。

(内容について一部非公表)

事務局からの説明は、以上でございます。

○丹野委員長 ありがとうございました。

ただいまの説明につきまして、御質問、御意見をお願いいたします。よろしいでしょうか。

それでは、私から一言申し上げます。本件は、ただいま事務局から説明がありましたように、当委員会がこれら11法人に対して昨年11月2日に行った指導に対する、それぞれが講じた再発防止策とその実施状況に関する報告が当委員会に提出されたものでございます。

現時点ではこの報告について、特段の問題は見当たらないものと考えますが、本件は、個人情報保護法の特別法である、次世代医療基盤法上の医療情報取扱事業者が関与する事案として、より厳格な対応がとられるべきものであること、そもそも、11法人は、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取り扱う機関であること、また、現在既に次世代医療基盤法の改正が検討されていること等を踏まえ、当委員会として、11法人の再発防止策が確実に実施されているか等を、今後も一層注視していく必要があると考えております。

ほかに御意見がないでしょうか。

それでは、特に修正の御意見がないようですので、原案のとおり進めたいと思いますが、よろしいでしょうか。

御異議がないようですので、そのように取り扱うことといたします。事務局においては所要の手続を進めてください。

また、本議題の資料、議事録及び議事概要の取扱いについてお諮りいたします。本議題は、事案の社会的な影響を勘案し、配付の公表資料と当該資料に係る議事録、議事概要の部分を、準備が整い次第、委員会のホームページで公表し、それ以外の資料と当該資料に係る議事録、議事概要の部分については公表しないこととしてよろしいでしょうか。

御異議がないようですので、そのように取り扱うことといたします。

本日の議題は以上でございます。

それでは、本日の会議はこれで閉会でございます。