

論点 2 : 個人情報の安全管理のために必要となる対応に関する論点

論点 2-1 : 安全管理措置、従業員の監督、委託先の監督

(1) 関係する義務の概要

- ① 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。(法第20条)
- ② 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。(法第21条)
- ③ 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。(法第22条)

(2) 主な論点

- ① 個人情報取扱事業者が講ずべき個人情報の保護のための措置について、個人情報の保護に関する基本方針等では以下のとおり規定されているが、医療機関等における安全管理措置等についても、基本的に重要な事項は同様であると考える。

【個人情報の保護に関する基本方針（抜粋）】

6 個人情報取扱事業者等が講ずべき個人情報の保護のための措置に関する基本的な事項

(1) 個人情報取扱事業者に関する事項

個人情報取扱事業者は、法の規定に従うほか、2の(3)の①の各省庁のガイドライン等に則し、個人情報の保護について主体的に取り組むことが期待されているところであり、事業者は、法の全面施行に向けて、体制の整備等に積極的に取り組んでいくことが求められている。各省庁等におけるガイドライン等の検討及び各事業者の取組に当たっては、特に以下の点が重要であると考えられる。

① 事業者が行う措置の対外的明確化

事業者の個人情報保護に関する考え方や方針に関する宣言(いわゆる、プライバシーポリシー、プライバシーステートメント等)の策定・公表により、個人情報を目的外に利用しないことや苦情処理に適切に取り組

むこと等を宣言するとともに、事業者が関係法令等を遵守し、利用目的の通知・公表、開示等の個人情報の取扱いに関する諸手続について、あらかじめ、対外的に分かりやすく説明することが、事業活動に対する社会の信頼を確保するために重要である。

また、事業者において、個人情報の漏えい等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点から、可能な限り事実関係等を公表することが重要である。

② 責任体制の確保

事業運営において個人情報の保護を適切に位置づける観点から、外部からの不正アクセスの防御対策のほか、個人情報保護管理者の設置、内部関係者のアクセス管理や持ち出し防止策等、個人情報の安全管理について、事業者の内部における責任体制を確保するための仕組みを整備することが重要である。

また、個人情報の取扱いを外部に委託することとなる際には、委託契約の中で、個人情報の流出防止をはじめとする保護のための措置が委託先において確保されるよう、委託元と委託先のそれぞれの責任等を明確に定めることにより、再委託される場合も含めて実効的な監督体制を確保することが重要である。

③ 従業員の啓発

事業者において、個人情報の漏えい等の防止等、その取り扱う個人情報の適切な保護が確保されるためには、教育研修の実施等を通じて、個人情報を実際に業務で取り扱うこととなる従業員の啓発を図ることにより、従業員の個人情報保護意識を徹底することが重要である。

【個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成16年6月 経済産業省：抜粋）】

2. 個人情報取扱事業者の義務等

(3) 2) 安全管理措置（法第20条）

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的、及び技術的安全管理措置を講じなければならない。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱い状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることが望ましい。

(注) なお、同ガイドラインにおける組織的、人的、物理的及び技術的安全管理措置の内容及び講じることが望ましい具体的措置等については、第1回検討会参考資料21～34ページを参照。

- ② 医療情報や医療機関等の業務の特性からみて、個人情報保護法を遵守する上で必要な対応やより高いレベルの対応として、各種の安全管理措置のうち、例えば、次のような事項について、医療機関等の規模等も踏まえつつ、医療機関等に求めることとしてはどうか。

ア. 個人情報保護に関する規程の整備、公表

(参考)「診療情報の提供等に関する指針」においては、「診療情報の提供に関する規程」を整備することとされている。

【診療情報の提供等に関する指針（抜粋）】

1.2 診療情報の提供に関する規程の整備

医療機関の管理者は、診療記録の開示手続等を定めた診療情報の提供に関する規程を整備し、苦情処理体制も含めて、院内掲示を行うなど、患者に対しての周知徹底を図らなければならない。

イ. 個人情報保護推進のための委員会や責任者等の設置

ウ. 個人情報の漏洩等の問題が発生した場合の報告連絡体制の整備

エ. 医療資格者でない者も含めた従業者との雇用契約において、個人情報を漏えいしないことを義務づけること

オ. 従業者に対する教育研修の実施

カ. 個人情報の提供が必要な業務委託を行う際の委託契約において、個人情報の漏えい防止その他の安全管理措置の実施を義務づけること

※ ITに係る技術的な安全管理措置等については、「医療情報ネットワーク基盤検討会」の検討結果を踏まえ検討。

- ③ 受付での呼び出しや、病室の患者の名札などについては、患者の取り違えを防止するなど業務を適正に実施する上で必要と考えられるが、患者の希望に応じて一定の配慮をすることが適当ではないか。