医療分野における個人情報保護
－医療情報システムの安全管理措置を中心として－

矢野　一博
日本医師会　総合政策研究機構

1．はじめに

平成 17 年 4 月、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）が全面施行された。これにより、一定の数の個人情報を取り扱う事業者は、個人情報を適切に取り扱うことが求められる。個人情報をずさんに管理している場合、指導、勧告、最悪の場合は罰則が適用されることになる。医療機関も例外ではなく、個人情報保護法に則って患者等の個人情報を取り扱わなくてはならない。

個人情報保護法は、その成立時、国会において「特にその適正な取扱いの厳格な実施を確保する必要がある個人情報については、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるものとする」と附帯決議がされていた。

このため、平成 16 年 6 月、医療機関等における個人情報保護のあり方について幅広く検討を行うことを目的として、厚生労働省内に「医療機関等における個人情報保護のあり方に関する検討会」が設置された。その結果、同 12 月に「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」が通知されている。

このガイドラインは、診療録等の開示、個人情報保護法では対象外とされている死者の情報の取り扱い、一定数以上の個人情報を保有しない小規模事業者への努力義務などが盛り込まれている。

個人情報保護法は各分野に共通する必要最低限のものを定める法という位置付けとされている。従って、「個人情報の保護に関する基本方針」（平成 16 年 4 月　閣議決定）により事業分野毎のガイドライン等を定めることになった。特に厳格な実施を確保する必要のある医療等の分野については、格別の措置を検討し、法の全面施行までに一定の結論を得ることとされていた。「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」はこのような流れを受け策定されたものである。他に代表的なガイドラインとして、経済産業省の「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したガイドライン」（平成 16 年 6 月）などもある。

厚生労働省からはもうひとつ「医療情報システムの安全管理に関するガイドライン」（平成 17 年 3 月）が通達されている。

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」では、電子カルテ等の IT 関連システムの安全管理について、別途、厚生労働省の定めるガイドラインを参照することとなっていた。別途定めるガイドラインというのが、「医療情報システ

ムの安全管理に関するガイドライン」である。従って、「医療情報システムの安全管理に関するガイドライン」は、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」と対を成すものである。

昨今､医療機関では電子カルテなどの IT 関連システムを導入する機会も増えてきている。一度は上記 2 つのガイドラインにじっくりと目を通しておくことも必要であろう。

しかし、個人情報保護法が全面施行されるからといって、法対応のために特殊なことをしなくてはいけないということではない。ポイントを押さえ、適切に対処していくことが望まれる。次に、いくつかポイントを述べて行く。今後の参考となれば幸いである。

2. 個人情報保護法の全面施行とは

ポイントを述べて行くにあたり、まず個人情報の全面施行とは何かという点を簡単に説明しておきたい。

個人情報保護法は、以下の全 6 章で構成され、平成 15 年 5 月に既に公布されている法律である。ただし、経過措置として法令の第 4 章から第 6 章までの規程は、公布後 2 年以内に施行とされている。

第 1 章　総則
第 2 章　国及び地方公共団体の責務等
第 3 章　個人情報の保護に関する施策等
第 4 章　個人情報取扱事業者の義務等
第 5 章　雑則
第 6 章　罰則

このうち、第 4 章に個人情報取扱事業者の義務等として、「利用目的の特定、利用目的による制限」、「適正な取得、取得に際しての利用目的の通知等」、「安全管理措置、従業者・委託先の監督」、「第三者提供の制限」、「公表等、開示、訂正等、利用停止等」が並んでいる。つまり、全面施行されることで、個人情報を取り扱う民間事業者への規程が第 6 章で定められている罰則も含めて施行されたことになる。

このことから、医療機関も含めた幅広い事業者において、法に則った適切な個人情報の取り扱いが必要となるのである。

3. 『医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン』について

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」は、個人情報保護法よりも一歩踏み込んだ内容が含まれている。次に、その代表的なポイントについて個人情報保護法との関係を見てみる。

・ 診療録等の開示

個人情報保護法では、第 25 条（開示）の定めにより、開示を求められた場合は、同条第 1 項各号のいずれかに該当する場合を除いて、遅滞なく書面等の交付により開示を行うことと定められている。

一方、ガイドラインでは開示にあたっては平成 15 年 9 月の「診療情報の提供等に関する指針」にも配慮するようにとされている。

この指針では、開示の際には医療分野の情報の特性を踏まえて、担当の医師等が説明を行う等の対応が望ましいとなっている。また、開示・不開示の判断にあたっては、「医療機関内に設置する検討委員会で検討した上で決定すること」、「文章で理由を示すこと」、「苦情処理の体制についても併せて説明すること」と、客観的な評価が求められる。

つまり、診療録等の開示については、既により具体的な指針が示されていることになる。既に同指針に従って適切に診療録等の情報開示を実施していれば、個人情報の全面施行にあたり、医療機関において同法に対応した特別な措置が求められているということではない。

ただし、個人情報保護法と指針では開示請求できる者の規定が若干異なる。指針では親族や法定代理人などを限定的に定めているのに対して、個人情報保護法では親族関係などには関係なく、広く代理人からの請求を認めている。この点は、請求者が何を根拠に開示を求めて来ているのかを適切に判断しなくてはならない。従って、個人情報保護法に則って開示請求をして来た人に対する対応は一度検討しておく必要がある。

・ 死者の情報

個人情報保護法では、法の適用される個人として「生存する個人」に関する情報であって、特定の個人を識別することができるものと定義されている。

一方、ガイドラインでは、先述の指針に従って遺族へも情報を提供するように求めている。従って、患者が死亡した場合でも、情報を保存している場合は漏洩防止のために、生存する個人と同等の安全管理措置を講ずるべきとなっている。この点は、個人情報保護法より厳しい内容となっている。

・ 小規模事業者の取り扱い

個人情報保護法では、取り扱う個人情報の数が 5,000 件以下の小規模事業者に対しては、個人情報取扱事業者としての義務は課されない。（厳密には、過去 6 ヶ月以内に一度でも 5,000 件を越えた場合は対象となる。）

一方、ガイドラインでは小規模事業者に対しても、その遵守義務を求めている。その理由には、「事業者の規模によらず良質かつ適切なサービスの提供が期待されること」、「患者等からみればどの事業者が小規模事業者であるかの判断が難しい」ということが挙げられている。

つまり、医療分野においては 5,000 件以上の個人情報を取り扱わない事業者であっても、「従業者の監督」、「安全管理措置」、「委託先の監督」などについての遵守努力が求められることになる。医療機関であれば患者情報は、小規模、大規模によらず医師等の資格者の守秘義務とも相まって適切に取り扱われているはずである。規模の違いにより個人情報の保護対応に違いは生じないと考えられる。

4. 『医療情報システムの安全管理に関するガイドライン』について

厚生労働省から医療分野の個人情報保護法に関連する文章として、もうひとつ「医療情報システムの安全管理に関するガイドライン」が平成 17 年 3 月 31 日に通達されている。

このガイドラインは、医療機関等において医療情報システムを導入・運用する際の参酌基準として厚生労働省医政局長の私的諮問委員会である「医療情報ネットワーク基盤検討会」（平成 15 年 6 月設置）の答申を受けて作成された。

本ガイドラインは、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」の 18 ページ「Ⅲ.医療・介護関係事業者の義務等　4.安全管理措置、従業者の監督及び委託先の監督（第 20 条～第 22 条）（4）医療情報システムの導入及びそれに伴う情報の外部保存を行う場合の取り扱い」で述べられている、「厚生労働省が別途定める指針」に該当する。

従って、医療機関において情報システムを導入または運用しようとする場合、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」と併せて参照しなくてはならないガイドラインである。

本ガイドラインは、平成 11 年 4 月の「法令に保存義務が規定されている診療録及び診療諸記録の電子媒体による保存に関する通知」及び、平成 14 年 3 月通知「診療録等の保存を行う場所について」に基づき作成された各ガイドラインを統合して作成された。従来のガイドラインと異なり、最新の技術内容にも言及し、個人情報保護法や、平成 17 年 4 月に施行されている「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（通称、e-文書法）にも対応したガイドラインとなっている。

このガイドラインでは、医療情報システムの安全管理措置に重点を置き、医療機関等でどのように対策を施して行くべきかを、「B. 考え方」と共に「C. 最低限のガイドライン」、「D. 推奨されるガイドライン」に分けて具体的に記述している。

5. 具体的な取り組みのきっかけ

個人情報保護法の全面施行に伴い、医療機関ではいったい何から取り組めばよいのかという声が聞かれる。しかし、冒頭述べたように、医療機関における個人（患者）情報の取り扱い方を鑑みれば、法の施行に伴って特別に何かを実施しなくてはならない事項というのはほとんどないはずである。

それでも、いくつかは実施しなくてはならないこと、実施しておいた方が望ましいこと

などがある。取り組みのきっかけとして以下のような事項を確認してもらいたい。

・ 体制の構築

まず、個人情報を保護するにあたり、そのきっかけとしたいのが体制の構築である。万が一、個人情報が漏洩した場合、誰が責任を取り、また、被害者への対処、再発を防ぐ手立ての構築など、迅速に対応する必要がある。そのためには、指揮命令系統も含めた個人情報保護の体制作りが必要になる。また、体制を構築しても、それが実際に機能しなくては意味がない。そこで、経営判断のできるトップも関与する形で、全組織的に個人情報の保護体制を敷く必要がある。

これには、実際に個人情報に関する問い合わせや開示などの依頼が来た場合の受付窓口もしくは担当者の設置なども含まれる。個人情報に関する問い合わせ窓口がなく、依頼者がたらい回しにされるようなことがあれば、対外的に印象も悪く、個人情報の保護・管理がずさんだと言われかねない。そのような観点からも窓口を設置することは重要である。

その体制を構築した上で、組織として個人情報をどのように保護して行くかを定めた各種のドキュメントや手順書を作成して、外部に公開したり、組織内で教育・啓発して行く必要がある。一般的にいわれるドキュメントの体系は、「基本方針」、「基本規程」、「実施手順書等」という三層構成である。

「基本方針」で、組織の個人情報保護に対する理念や考え方を述べる。「基本規程」は、基本方針を受けて、それを実施するための基礎となる具体的な内容を規程する。最後の「実施手順書等」というのは、実際の業務の手順を定めるなど、具体的なマニュアルや手順書となる。これらは、個人情報保護を解説した書籍などでも必ず触れられているので、そちらを参照されるのがよいであろう。

・ 院内掲示

次に実施しておきたいのが、医療機関における個人情報に対する取り組みを表明する院内掲示である。

ポスター1 枚を掲示する程度で、医療機関で個人情報保護に取り組んでいるという姿勢表明と個人情報の利用目的などを患者等に示す。これは、体制の構築の中で述べた「基本方針」と同一でも構わない。これにより、医療機関内における個人情報に対して適切に対応しているという姿勢を対外的に明示することが重要である。

なお、この院内掲示の例については、日医会員であれば日医の作成した冊子、「医療機関における個人情報保護」にサンプルが掲載されている。そちらを活用すると良いだろう。ただし、あくまでサンプルのため、医療機関毎の実態に合わせて適宜変更する必要がある。

・ 契約等の見直し

忘れがちなのが契約の見直しである。医療機関は色々な局面で業務を外部に委託する。検査であったり、レセプトコンピュータの保守であったりする。この時、先ほどの院内掲示で個人情報を委託することがあると断っておくことも重要であるが、委託先との契約を見直したり確認することも忘れてはならない。

委託先と守秘義務を含めた契約を結ぶのはもとより、委託先での個人情報の適切な取り扱いも含めて、再度、現在締結している契約で問題ないかなど一度確認しておくべきである。これから新規で契約を結ぶのであれば、契約書にきちんとそれらの事項が含まれているかを確認しておきたい。

また、個人情報の委託を実施する場合、委託元には委託先管理という義務が発生する。これは、委託先が適切に個人情報を取り扱っているかを管理、監督する必要があるということである。従って、特に新規の契約の場合は、適切に個人情報を取り扱っている委託先を選びたい。その際のひとつの基準になるのが、「プライバシーマーク制度」である。ただし、委託先が同制度による認定を受けていても、これは基準のひとつに過ぎない。プライバシーマークがあれば安心ということではなく、委託した個人情報の取扱いについて可能な限り確認を実施することが望ましい。

6. さいごに

平成１７年４月から全面施行された個人情報保護法に対して、簡単な解説、ガイドラインとの比較などを述べてきた。

個人情報の施行に伴い、色々な業務が制限されたり、少しでも取り扱いを間違うと罰せられるというような話を耳にする。そもそも、個人情報保護法は、事業者に適用される法律であり、個人情報を取り扱う個人（従業者）に適用される法律ではない。また、その成立の目的も、「個人情報の有用性に配慮しつつ、個人の権利利益を保護」するものとされている。つまり、これまで曖昧に取り扱われていた個人情報を適切に取り扱い、適切な情報流通を図ろうというのが法律の趣旨になる。

従って、個人情報保護法の施行に伴って医療機関の業務が特に大きく変わったり制限されたりすることはない。いままで通り、適切な取り扱いをすれば十分である。

ただし、若干注意しなくてはならないこともある。それが、例えば院内掲示による利用目的の公表・通知であり、個人情報に関する問い合わせが来た場合の対処方法である。

また、個人情報保護法が施行されたことで、国民の個人情報に対する権利意識が高まっていることは確かである。今後、個人情報についての問い合わせが増えることも想定される。新たな時代の流れともいえる。

しかし、個人情報保護法の全面施行を新たな規制と考えるのではなく、既に確立した個人情報保護体制の見直しの機会と捉えて、より一層の個人情報の保護に取り組んでみてはいかがであろうか。