参考資料８

医療情報を受託管理する情報処理事業者向けガイドライン

第 2 版

（抄）

平成 24 年 10 月

経済産業省

1　はじめに

医療機関等で扱う文書類のうち、診療録、助産録、調剤録等（以下、「診療録等」という。）については、平成 11 年 4 月通知「診療録等の電子媒体による保存について[1]」によって、初めて診療録等の電子媒体による保存について基準が示された[2]。更に、平成 14 年 3 月通知「診療録等の保存を行う場所について[3]」により、診療録等の電子保存及び保存場所に関する要件等が明確化された[4]（調剤録は電子保存可能だが、外部保存は許されていない）。この通知においては、それまで認められていなかった診療録等の外部保存を行う場合の基準が明記されていた。また、それぞれの通知に対して「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ガイドライン[5]」及び「診療録等の外部保存に関するガイドライン[6]（以下、「外部保存ガイドライン」という。）」が示されていた。一方、平成 15 年に「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下、「個人情報保護法」）が成立し、これを受けて医療・介護分野において平成 16 年 12 月には「医療・介護関係事業者における個人情報の適切な取扱のためのガイドライン」が公表され、平成 17 年 4 月の個人情報保護法の全面実施に際しての指針が示された。

さらに、平成 17 年 3 月、情報システムの導入及びそれに伴う外部保存を行う場合の取扱に関して、厚生労働省に設置された「医療情報ネットワーク基盤検討会」にて「医療情報システムの安全管理に関するガイドライン」が策定された。このガイドラインは、「診療録等の電子媒体による保存について」及び「診療録等の保存を行う場所について」の各通知に基づき作成された各ガイドラインを統合し、新たに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ガイドライン（紙等の媒体による外部保存を含む）、及び医療・介護関連機関における個人情報保護のための情報システム運用管理ガイドラインを含んだガイドラインである。また、個人情報保護法及び「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」（平成 16 年法律第 149 号）、「厚生労働省の所管する法令の規定に基づく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省令」（平成 17 年厚生労働省令第 44 号）に対する医療情

---

1 平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知

2 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等の施行等について」（平成 17 年 3 月 31 日付け医政発第 0331009 号・薬食発第 0331020 号・保発第 0331005 号厚生労働省医政局長・医薬食品局長・保険局長連名通知）にて廃止

3 平成 14 年 3 月 29 日付け医政発 0329003 号・保発第 0329001 号厚生労働省医政局長・保険局長連名通知

4 「「診療録等の保存を行う場所について」の一部改正について」（平成 17 年 3 月 31 日付け医政発第 0331010 号・保発第 0331006 号厚生労働省医政局長・保険局長連名通知）にて一部改正

5 平成 11 年 4 月 22 日付け健政発第 517 号・医薬発第 587 号・保発第 82 号厚生省健康政策局長・医薬安全局長・保険局長連名通知に添付

6 平成 14 年 5 月 31 日付け医政発第 0531005 号通知に添付

報システムの具体的指針という側面も持ち合わせる。

その後、平成 19 年 3 月には医療機関等で用いるのに適したネットワークに関するセキュリティ要件定義について、想定される用途、ネットワーク上に存在する脅威、その脅威への対抗策、普及方策とその課題等、様々な観点から医療に関わる諸機関間を結ぶ際に適したネットワークの要件等を追加して、「医療情報システムの安全管理に関するガイドライン第 2 版」が策定された。

平成 20 年 3 月には、医療資格を持たないものが医療・健康情報を取扱う際のルール策定を検討した上で、責任のあり方についてまとめ、更に昨今の業務体系の多様化にも対応するため、モバイルアクセスで利用できるネットワークの接続形態毎の脅威を検討し、情報および情報機器の持ち出し等について追記した、「医療情報システムの安全管理に関するガイドライン 第 3 版」、平成 21 年 3 月には、より適切な医療分野の情報基盤構築を目指した「医療情報システムの安全管理に関するガイドライン 第 4 版」、平成 22 年 2 月には「医療情報システムの安全管理に関するガイドライン 第 4.1 版」が策定された（以下、第 4.1 版を「医療情報安全管理ガイドライン」という。）。

このような一連の施策等により診療録等の情報を電子的に作成し保存することが許容されてきた。また、それらを外部に保存する場合も外部保存ガイドラインで具体的指針が示されている。医療情報安全管理ガイドライン第 4 版の公開後、平成 21 年 7 月に総務省が「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」を策定した。加えて、平成 20 年 7 月に経済産業省が告示した「医療情報を受託管理する情報処理事業者向けガイドライン」（平成 20 年 7 月 24 日経済産業省告示第 167 号）の整備等により、外部保存に対する対応方法が明確になったとの指摘がなされ、「医療情報ネットワーク基盤検討会」で外部保存先の基準に関する検討が行われ、各ガイドラインの要求事項の遵守を前提として「「民間事業者等との契約に基づいて確保した安全な場所」へと改定すべき」とする「診療録等の保存を行う場所に関する提言」が取りまとめられた。これを受けて、外部保存通知の改正が行われ、医療情報安全管理ガイドラインにおいても関連する各章の一部を中心に改定が実施され、医療情報安全管理ガイドラインの第 4.1 版が策定された。

医療機関等から医療情報を受託する事業者となる立場の情報処理事業者については、現在、「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」の規定が適用されている。同ガイドラインは、多様な業種の事業者が広汎な種類の個人情報を取り扱うことを想定しているため、機微性の高い医療情報の取扱に携わる医療情報受託者に対しては、必ずしも十分な安全管理措置が規定されていない。

このため、「パーソナル情報研究会[7]」にて、医療情報の外部保存の安全性に万全を期すべ

[7] 「パーソナライゼーション時代の本格到来をにらみ、個人情報その他個人に関する情報に

く、医療情報受託者が義務的に講ずべき措置を具体的に明記した本ガイドラインを別途策定することとした。その後、平成 20 年 7 月には、本ガイドラインの第 1 版に従い、「医療情報を受託管理する情報処理事業者向けガイドライン」（平成 20 年 7 月 24 日経済産業省告示第 167 号）を制定した。

本ガイドライン第 2 版では、医療情報安全管理ガイドラインの第 4 版及び第 4.1 版に合わせて内容を改めるとともに、経済産業省告示の医療情報を受託管理する情報処理事業者向けガイドラインに関する参考資料としての位置付けを明確にしたものである。すでに、安全基準、即ち情報セキュリティマネジメントシステムに関する標準規格として JIS Q 27001:2006、個人情報保護マネジメントシステムに関する標準規格として JIS Q 15001:2006 が策定され多くの組織において活用されているが、既存の情報セキュリティ対策に関する各種の規格は広範な事業を対象として一般化されたものであり、本ガイドラインで扱う「医療情報取扱情報処理」事業の特殊性を鑑みて一段と具体化及び対策の深化を図る必要がある。このため、本ガイドラインでは「医療情報の外部委託」という事業特有の課題に配慮し、この分野において情報セキュリティマネジメントシステムを実装する上でのガイドラインを示すことを目的とする。

また、本ガイドライン第 1 版の公開後に、医療情報の処理を ASP・SaaS で提供する事業者及び団体向けに「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン（総務省平成 21 年 7 月）」が策定されたことで、医療情報の外部保存を受託する事業者向けの本ガイドラインと合わせて、受託事業者サイドの情報処理事業に関するガイドラインの構成は図 1 のように整理されることとなった。なお、「ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン」は平成 22 年 12 月に第 1.1 版が公開されている（以下、第 1.1 版を「ASP・SaaS 事業者向けガイドライン」という。）。

本ガイドラインを含め、医療情報安全管理ガイドライン、ASP・SaaS 事業者向けガイドラインの関係を図 1 に示す。

ついて、将来想定される様々な利活用の方法を体系化すると共に、国民にとって安全・安心かつ適切な個人に関する情報の利活用を保証するための個人情報保護、セキュリティ、認証などのあり方について検討を行う」ことを目的として経済産業省商務情報政策局に設置された研究会。

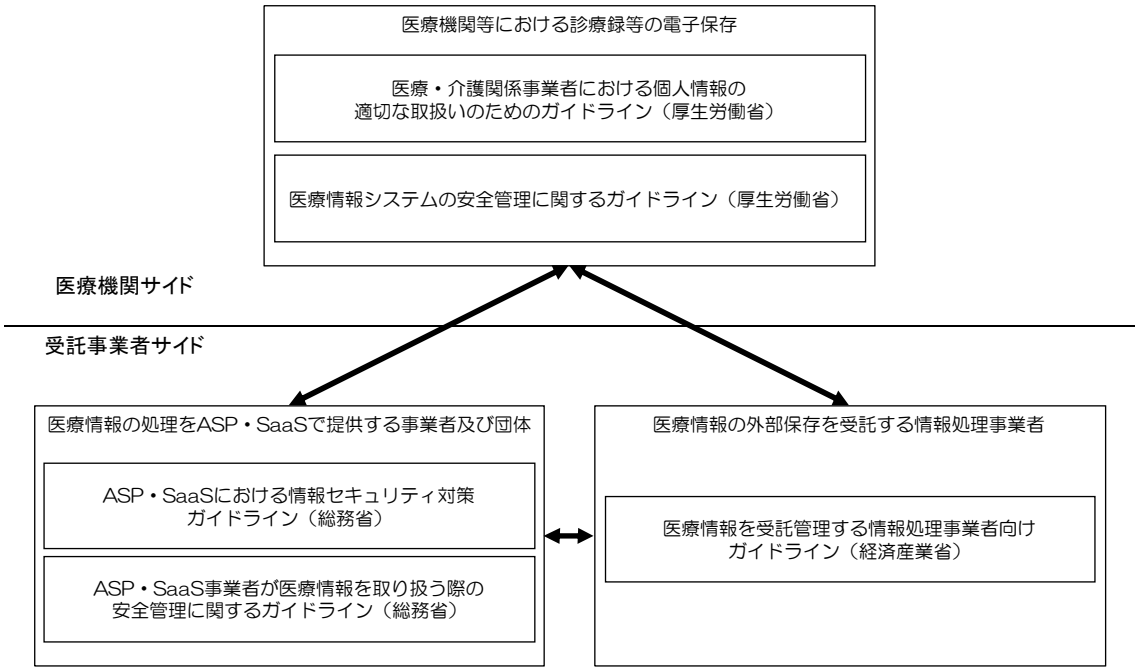

図 1 医療情報の取り扱いに係るガイドラインの関係

なお、本ガイドラインは、医療情報安全管理ガイドラインで示される安全管理策と同等の安全管理策として「実施すべき安全管理策」を示し、医療機関等及び情報処理事業者の判断で実施することが望ましい、同等以上の安全管理策を「推奨される安全管理策」として示している。どの安全管理策を実装するのかの判断において、単にセキュリティレベルの高さに配慮するだけではなく、個々の安全管理策が要求されている理由及び背景について、医療情報安全管理ガイドラインに記されている事柄を十分に理解しておくことが必要である。