参考　2

健康保険組合等の個人情報保護・情報セキュリティ対策について

○　役職員の秘密保持義務

・　健康保険法（大正11年法律第70号）第22条の2により準用される同法第7条の37第1項の規定により、健康保険組合の役員及び職員は、健康保険事業に関して職務上知り得た秘密を正当な理由がなく漏らしてはならない義務を負う。（第7条の37及び第22条の2については、平成20年10月施行。）

○「個人情報の保護に関する法律」（平成15年法律第57号）

・　個人情報取扱事業者（※）に該当する健康保険組合等に対して、安全管理措置、従業者・委託先の監督、第三者提供の制限等の個人情報保護のための義務を課している。

※　識別される特定の個人の数の合計が過去6ヶ月以内のいずれにおいても5,000を超えない事業者は除かれる。

・　特に、安全管理措置については同法第20条が「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」と規定。

○「健康保険組合等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」（平成16年12月）

・「個人情報の保護に関する法律」の規定に基づき定められた、健康保険組合及び健康保険組合連合会が行う個人情報の適正な取扱いの確保に関する活動を支援するためのガイドライン。

・　一般的な個人情報保護のためのガイドラインとして、利用目的の特定、適正な取得、安全管理措置、第三者提供の制限等について規定。

・　個人情報保護法上の個人情報取扱事業者に該当しない小規模な健康保険組合も含め、一律に遵守を求めている。

○「レセプトのオンライン請求に係るセキュリティに関するガイドライン」（平成18年4月）

・　医療機関、薬局、審査支払機関及び保険者に対し、診療報酬明細書等（レセプト）のオンライン請求業務に関わる組織及びシステムが最低限満たすことが必要と考えられる項目を示すガイドライン。

・　役割・責任の明確化、情報の分類、物理・人的・技術的セキュリティ、セキュリティポリシーの策定・運用等について規定。

（参考）「医療情報システムの安全管理に関するガイドライン」

医療機関等については、健康保険組合等に対するガイドラインと同様の一般的な個人情報保護のガイドラインとは別に、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いに関してガイドライン（「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月第1版、平成19年3月第2版））が定められ、PDCAサイクルによって行われる情報セキュリティマネジメントシステム（ISMS）の実践方法等の技術的ガイドラインが示されている。