4.1　医療機関等の管理者の情報保護責任について

医療機関等の管理者が医療情報を適切に管理するための善管注意義務を果たすためには、通常の運用時から払われているべき、医療情報保護の体制を構築し管理する局面での責任と、医療情報について何らかの不都合な事態（典型的には情報漏えい）が生じた場合に対処をすべき責任とがある。便宜上、本ガイドラインでは前者を「通常運用における責任」、後者を「事後責任」と呼ぶこととする。

(1) 通常運用における責任について

ここでいう通常運用における責任とは、医療情報の適切な保護のための適切な情報管理ということになるが、適切な情報管理を行うことが全てではなく、以下に示す 3 つの責任を含む必要がある。

① 説明責任

電子的に医療情報を取り扱うシステムの機能や運用方法が、その取り扱いに関する基準を満たしていることを患者等に説明する責任である。これを果たすためには、以下のことが必要である。

- システムの仕様や運用方法を明確に文書化すること
- 仕様や運用方法が当初の方針の通りに機能しているかどうかを定期的に監査すること
- 監査結果をあいまいさのない形で文書化すること
- 監査の結果問題があった場合は、真摯に対応すること
- 対応の記録を文書化し、第三者が検証可能な状況にすること

② 管理責任

医療情報を取り扱うシステムの運用管理を行う責任であり、当該システムの管理を請負事業者に任せきりにしているだけでは、これを果たしたことにはならないため、医療機関等においては、以下のことが必要である。

- 少なくとも管理状況の報告を定期的に受けること
- 管理に関する最終的な責任の所在を明確にする等の監督を行うこと

さらに、個人情報保護法上は、以下の事項を定め、請負事業者との対応にあたる必要がある。

- 個人情報保護の責任者を定めること
- 電子化された個人情報の保護について一定の知識を有する責任者を決めること

③ 定期的に見直し必要に応じて改善を行う責任