

外部保存の技術的な方法としては、例えばトラブル発生時のデータ修復作業等緊急時の対応を除き、原則として医療機関等のみがデータ内容を閲覧できることを担保することも考えられる。

さらに、外部保存を受託する事業者には保存される個人識別に係る情報の暗号化を行い適切に管理することや、あるいは情報処理関連事業者の管理者といえどもアクセスできない制御機構をもつことも考えられる。

具体的には、「(a) 暗号化を行う」、「(b) 情報を分散保管する」方法が考えられる。

この場合、不測の事故等を想定し、情報の可用性に十分留意しなければならない。医療機関等が自ら暗号化を行って暗号鍵を保管している場合、火災や事故等で暗号鍵が利用不可能になった場合、すべての保存委託を行っている医療情報が利用不可能になる可能性がある。

これを避けるためには暗号鍵を外部保存を受託する事業者に預託する、複数の信頼できる他の医療機関等に預託する等が考えられる。分散保管においても同様の可用性の保証が必要である。

ただし、外部保存を受託する事業者には暗号鍵を預託する場合においては、暗号鍵の使用について厳重な管理が必要である。

暗号鍵の使用に当たっては、非常時に限定することとし、使用における運用管理規程の策定、使用したときにその痕跡が残る封印等の利用、情報システムにおける証跡管理等を適切に実施し、外部保存を受託する事業者による不正な利用を防止する措置をとらなければならない。

3. 情報の提供

① 病院、診療所、医療法人等が適切に管理する場所に保存する場合

情報を保存している機関に患者がアクセスし、自らの記録を閲覧するような仕組みを提供する場合は、情報の保存を受託した病院、診療所、医療法人等は適切なアクセス権限を規定し、情報の漏えい、異なる患者の情報を見せたり、患者に見せてはいけない情報が見えたり等の誤った閲覧が起こらないように配慮しなくてはならない。

また、それら情報の提供は、原則、患者が受診している医療機関等と患者間の同意で実施されるものであり、情報の保存を受託した病院、診療所、医療法人等が患者からの何らの同意も得ずに実施してはならない。

② 行政機関等が開設したデータセンター等に保存する場合

いかなる形態であっても、保存された情報を外部保存を受託する事業者が独自に保存主体の医療機関等以外に提供してはならない。

外部保存を受託する事業者を通じて保存された情報を保存主体の医療機関以外にも提供する場合は、あくまで医療機関等同士の同意の上で実施されなくてはならず、当