① 「情報処理関連事業者の提供するネットワーク」を通じて医療情報の提供元医療機関等と提供先医療機関等で患者情報を交換する場合の責任分界点

ここでいう「情報処理関連事業者の提供するネットワーク」とは、情報処理関連事業者の責任でネットワーク経路上のセキュリティを担保する場合を言う。

提供元医療機関等と提供先医療機関等はネットワーク経路における責任分界点を定め、不通時や事故発生時の対処も含めて契約等で合意しておく。

その上で、自らの責任範囲において、情報処理関連事業者と管理責任の分担について責任分界点を定め、委託する管理責任の範囲及びサービスに何らかの障害が起こった際の対処をどの事業者が主体となって行うかを明らかにしておく。

ただし、委託の場合は、通常運用における責任、事後責任は、原則として提供元医療機関等にあり、第三者提供において適切に情報が提供された場合は、原則として提供先医療機関等にあり、情報処理関連事業者に瑕疵のない場合は、情報処理関連事業者に生じるのは管理責任の一部のみであることに留意する必要がある。

② 提供元医療機関等と提供先医療機関等が独自に接続する場合の責任分界点

ここでいう「独自に接続」とは、情報処理関連事業者のネットワークではあるが、接続しようとする医療機関等同士がルータ等の接続機器を自ら設定して1対1や1対Nで相互に接続する場合や電話回線等の公衆網を使う場合を言う。

この場合、あらかじめ提供先または提供先となる可能性がある医療機関等を特定できる場合は、委託または第三者提供の要件に従って両機関等が責務を果たさなければならない。

情報処理関連事業者に対しては、管理責任の分担は発生せず、通信の品質確保は発生するとしても、情報処理関連事業者が提示する約款に示される一般的な責任しか存在しない。

さらに、提供元医療機関等と提供先医療機関等が1対N通信で、提供先医療機関等が一つでも特定できない場合は原則として医療情報を提供できない。ただし、法令で定められている場合等の例外を除く。

(b) 情報処理関連事業者に対する考え方

① 医療情報が発信元／送信先で適切に暗号化／復号される場合の責任分界点

患者情報を送信しようとする医療機関等（発信元）の情報システムにおいて、送信前に患者情報が暗号化され、情報を受け取った医療機関等(送信先)の情報システムにおいて患者情報が復号される場合、情報処理関連事業者は盗聴の脅威に対する個人情報保護上の責務とは無関係であり、責任は限定的になる。

この場合、情報処理関連事業者に存在するのは管理責任であり、ネットワーク

上の情報の改ざんや侵入、妨害の脅威に対する管理責任の範囲やネットワークの可用性等の品質に関して契約で明らかにしておく。

なお、暗号化等のネットワークに係る考え方や最低限のガイドラインについては、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

② 医療情報が情報処理関連事業者の管理範囲の開始点で適切に暗号化される場合の責任分界点

情報処理関連事業者の中には、例えば暗号化された安全なネットワーク回線の提供を主たるサービスとしている事業者も存在する。

そのようなネットワーク回線を使う場合、事業者が提供するネットワーク回線上における外部からの情報の盗聴や改ざん、侵入等やサービスの可用性等の品質については事業者に管理責任が発生する。従って、それらの責任については契約で明らかにしておく。

ただし、事業者が提供するネットワーク回線に到達するまでの管理責任やネットワーク回線を流れる情報に対する管理責任は医療機関等に存在するため、「Ⅰ 医療機関等における考え方 ①医療情報の提供元医療機関等と提供先医療機関等の責任分界点」に則った考え方の整理が必要である。

なお、ネットワーク回線上とネットワーク回線を流れる情報に対する考え方や最低限のガイドラインについては、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」を参照されたい。

(c) 外部保存機関が介在する場合に対する考え方

この場合、保存する情報は外部保存機関に委託することになるため、通常運用における責任、事後責任は医療機関等にある。

これを他の医療機関等と共用しようとする場合は、双方の医療機関等における管理責任の分担を明確にし、共用に対する患者の同意も得ておく必要がある。

また、外部保存機関とは、サービスに何らかの障害が起こった際の対処について契約で明らかにしておく。

なお、医療機関等が外部保存機関を通じて患者情報を交換する場合の医療機関等及び外部保存機関に対する考え方は、「8.1.2 外部保存を受託する機関の選定基準及び情報の取り扱いに関する基準」で定める保存機関毎に「2. 情報の取り扱い」及び「3. 情報の提供」として別途、詳細に規定しているため8.1.2を参照されたい。

(2) 業務の必要に応じて医療機関等の「施設外から情報システムにアクセス」する場合

施設外から情報システムにアクセスする場合のネットワーク全般の考え方について

は、「6.11 外部と個人情報を含む医療情報を交換する場合の安全管理」の、特に「B-2. 選択すべきネットワークのセキュリティの考え方 Ⅲ．モバイル端末等を使って医療機関の外部から接続する場合」を参照されたい。ここでは特に責任分界点の考え方について述べる。

(a) 自らの機関の情報システムにアクセスし業務を行う、いわゆるテレワーク

昨今、医療機関等においても医療機関等の施設外から自らの機関の情報システムにアクセスし業務を行う、いわゆるテレワークも一般的になってきた。

この場合、責任分界の観点では自施設に閉じているが、情報処理関連事業者が間に入って通信回線の両端で一医療機関等の従業者が関わることになる。

さらに、この場合には通信回線がインターネットだけでなく携帯電話網、公衆回線等多彩なものが利用されることになり、個人情報保護について広範な対応が求められることになる。

特に、医療機関等の管理責任者でない医療機関等の従業者についても管理責任が問われる事態も発生することに注意を払う必要がある。

この例の場合、責任分界点としては基本的に自施設に閉じているため、責任のあり方の原則としては、「4.1 医療機関等の管理者の情報保護責任について」となることに留意しなくてはならない。

(b) 第三者が保守を目的としてアクセスする、いわゆるリモートメンテナンス

この例のような、リモートログインを用いた保守業者の遠隔保守のためのアクセスが考えられる。この場合、適切な情報管理や情報アクセス制御がなされていないと一時保存しているディスク上の個人情報を含む医療情報の不正な読み取りや改ざんが行われる可能性もある。他方、リモートログイン機能を全面的に禁止してしまうと、遠隔保守が不可能となり、保守に要する時間等の保守コストが増大する。

従って、保守の利便性と情報保護との兼ね合いを見極めつつ実施する必要がある。

ただし、この場合でも、当然、医療機関等に対して「通常運用における責任」、「事後責任」が存在するため、管理状況の報告を定期的に受け、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い、管理責任を果たす必要がある。

なお、リモートログインも含めた、保守の考え方については「6.8 情報システムの改造と保守」を参照されたい。

(3) 医療機関等の業務の一部を委託することに伴い情報が「一時的に外部に保存」される場合

ここでいう委託とは遠隔画像診断、臨床検査等、診療等を目的とした業務の第三者委託であり、これに伴い一時的にせよ情報を第三者が保管することとなる。