

個人情報保護法と情報の安全管理

野口 雄司 (社)日本画像医療システム工業会
経済部会 部会長

個人情報保護法施行から一年以上経過した。院内リスクマネジメントシステムの一環として、さらに運用と管理の情報管理システムとして捉えなおし安全管理対策の必須事項と位置づけられ運用しているにも係わらず、後を絶たない個人情報の漏洩。改めて個人情報保護のための管理運用は確実に体系化されたシステムの中で行われているのだろうか？ 院内で管理・運用している各種個人情報は安全に管理する義務がある。安全管理措置を実施するためにもリスクマネジメント活動により院内の各種情報の取り扱いリスクを見極め重篤なものから順に低減するための改善措置を施していかなければならない。リスクマネジメント活動そのものはヒアリング・ハット運動等でおなじみであるが、全職員の安全に対する意識共有の上、収集・活用・保管 等の洗い出しが必要である。さて、リスクの低減のための施策であるが各種ガイドラインによれば安全対策の四つの視点で①組織的安全管理措置、②人的安全管理措置、③物理的安全管理措置、④技術的安全管理措置 が指摘されている。これらの視点はひとつひとつのリスクに対して組み合わせて実施されるべきものであり、どれかひとつの視点だけに偏ると、業務が止まってしまったり、反対にコストがかさむ割には実効性がまったく見えないものになってしまう。例えばワークステーションの自動ログオフ機能やユーザー認証の設定ひとつとってみても、院内では不特多数の眼に触れる場所での運用は厳格にするべきだが、職員が IDカードで入室する事務所内や医局内へはやや強制ログオフの間隔はやや長めに設定してもいいかもしれない。即ち実態に即した組織的・かつ物理的なルールの徹底との組み合わせで若干技術的なルールの緩和できそうである。さらに、放射線科サーバー室など、大量の情報が集積する場所には常時施錠【物理的措置】、入退室記録【組織的措置】、メンテナンス企業の訪問時にも名札着用と責任者への報告の徹底【組織的、契約等の締結】、サーバー管理者による ID管理の徹底【技術的】、をするという何重かの措置を重ね合わせることでより強度の高い安全管理措置が実現できる。この点、いくら指紋認証などの高額な装置を導入しても教育不徹底であったり、職員の意識が低かったりすると全く意味をなさない。情報管理と情報保護を実効性あるものにするには医療者の守秘義務の努力だけではいかんともしがたいケースが存在する。電子保存の要求事項でも経験したように「もの」に縛りをかけた時代から「マネジメント」に主眼が置かれた時代へ。即ち、四つの措置を組織的に組み合わせ、組織的に対応するマネジメントの重要性を改めて強調したい。