

情報倫理の観点からみた医療情報の管理

亀田 彰喜 勝木 太一

概要

情報技術の進展とともに、電子商取引や電子マネーが普及してきている。情報技術の導入は商取引の分野だけではなく、医療の分野にも導入されてきている。しかし、最近、一部の情報の技術を習得した者により、これらの電子商取引や電子マネーが普及されるとともに、ネットワーク上での電子商取引の妨害や取引データの改ざんなどが多発してきている。このようなことは、医療機関においても同様で、医療情報すなわち患者の個人情報の取扱いにおいても情報倫理に基づいた医療情報の管理が求められる。このようなことから、医療機関に患者の個人情報に関与する人々に対する情報倫理に関する意識の高揚が求められる。そして、厚生労働省はこのような現況にたいして、法的な対応を実施している。

現在のように、インターネットが地球規模で普及し、われわれの日常生活においても情報ネットワークを利用し多くの情報に接し、それらがいつも簡単に入手可能になった。しかし、これらの情報を取り扱うにあたって、善悪の基準が不明確なまま、多くの事件にまき込まれることがある。このようなことから、医療従事者として、社会人として情報倫理における意識の高揚と教育が求められる。

1. はじめに

情報ネットワークの進展によって、私たちの生活は便利になり、企業においても、また政府や地方自治体においても、情報ネットワークシステムの構築がすすめられてきている。しかし、現在の情報化社会において、社会的な問題が起きてきている。それは、情報ネットワークにおける不正アクセスによるデータベースの破壊や個人情報の漏えいなどの問題である。特定の個人の情報が漏えいし、それが、悪意を持った者の手に渡ると個人情報が不適正に取り扱われ、個人の権利と利益が侵害されることがある。そのため、情報倫理に対する意識の高揚が求められる。

一般に、倫理とは人間として正しく生きるにはどうすればよいのか、また、そのためには一体どのようにすればよいのかということを通して、現代社会における人としての生き方についての問題であり、社会での人間関係などの問題であるが、現在のような情報化社会において、新しい倫理の問題が噴出してきた。それは、インターネットが普及したことによる情報倫理の問題である。この新しい情報倫理の問題は情報ネットワークが普及するにしたがって、取り上げられるようになった。

このような問題は、医療機関でも起こっている。特に最近では医療機関において、情報ネットワークを介して、患者の個人情報の流失やノートパソコンの紛失、盗難による個人情報の漏えいが多発している。医療機関の中でも、患者の個人情報の流失は、特に研究を主体とする大学病院で流出する事態が続出している。個人情報の管理の保護体制を整えるためには、組織や人的な管理体制を整えるだけでなく、情報システム等の技術的な管理体制も必要である。医療における個人情報は、医療技術の研究のためには欠かせない情報でもあるが、患者個人がその研究の重要性に納得していなければならない。また、医療機関においても、いかにこれらの個人の医療情報を医学の進歩のために役立てることができるか、また研究開発のために活用できるかが重要ではあるが、患者の個人情報は人権尊重という観点から取扱いには、十分に留意しなければならない。そこで、医療機関における個人情報の取扱いの実情と管理体制について述べてみる。

2. 情報倫理の観点からの個人情報の保護と厚生労働省の対応

一般に、メディアにおける倫理は不特定多数に対し、報道という形態での情報を提供していたが、情報通信は情報ネットワークといった通信媒体を経由して、これに接続している特定の相手を対象とし、情報を相互に提供している。このような点で、メディアと情報通信には違いはあるものの、情報といった無形の物を扱う点では共通している。しかし、情報はそれなりに経済価値と力をもった重要なものである。その重要な情報をねつ造、改ざん、破壊するなど、これらの情報を作為的に操作する行為に対して、何らかの抑制が必要である。法的規制にはいたらなくとも、何らかの倫理的抑制が求められる。すなわち、個人レベルでの倫理意識の向上が必要なのである。

情報通信における今日の問題として、不正アクセスがある。これは情報ネットワークを介して進入することを言うが、この行為は許可なく接続していることから不正行為となる。それは接続した行為が、他人のデータベースに対する不正操作につながるからである。不正アクセスの前提に、他人のパスワードの解読がある。パスワードの解読だけでは違法ではないとの議論もあるが、パスワードを解読した時点で、他人の情報システムに接続し、すでに進入していることになる。パスワードの解読だけでは、不法行為ではないとの意見もあるものの、パスワードの解読は、不正アクセスへの前段階としての行為とみることもできる。このような現況に対して、厚生労働省は次のような法的な対応をしている。

2005年4月1日に個人情報保護に関する法律の施行に先駆けて、厚生労働省から2004年12月24日に「医療・介護関係事業者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」が公表され、医療・介護関係事業者に対し個人情報の取扱いに対する指針が示された。

この厚生労働省からのガイドラインは、それぞれ3分野に対して出されている。医療機

関と介護関係事業者に対しては、この「医療・介護関係事業者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」（以下、本ガイドライン）が、健康保険組合に対しては、2004年12月27日に、「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」が通達され、また2005年4月20日に、「国民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」が掲載された。そして、医学研究分野に対しては、2004年12月28日に告示改定した「ヒトゲノム・遺伝子解析研究に関する倫理指針」、同じく2004年12月28日に「疫学研究に関する倫理指針」、「遺伝子治療臨床研究に関する指針」、「臨床研究に関する倫理指針」が告示改定され、更に、2006年7月3日に、「ヒト幹細胞を用いる臨床研究に関する指針」が告示された。

これらの通達や告示に対し、医療機関や医師は、個人情報保護に関する法律が如何なるものか、またどのように具体的に対処すれば良いのか、戸惑うこともある。個人情報の保護に関する法律の趣旨は、医療においては、患者の各個人の情報の権利を保障するものであり、医師をはじめとする医療関係者に課されている患者に対する守秘義務を遵守するとともに、患者の個人情報の利用目的の明示や、漏えい防止の安全管理等の管理体制の整備と強化が求められる。また、患者の個人情報におけるトラブルに対する対応策も求められる。

個人情報保護法の全面施行に対して、全ての公的機関や事業者および医療機関においても、個人情報保護に対する取組みが求められる。特に、最近では個人情報の保存された電子記憶媒体やノートパソコンの盗難や紛失が多く発生しているとともに、ネットワーク上でのファイル交換ソフトを介しての個人情報の漏えいが発生している。医療機関においても個人情報保護法や厚生労働省の本ガイドラインで示された趣旨に基づいて、患者の個人情報の安全管理と適正な利用に関して、管理体制と指針を設けなければならない。従来の紙カルテなどの個人情報の管理からの移行に伴い、特に電子情報化された個人情報の安全管理が必要である。それは、医療関係者と患者との信頼関係を深めるためにも、また医療サービスの向上を図る上においても個人情報の安全管理は必要である。

すなわち、個人情報保護に関する法律においては、特定の個人を識別可能な情報については全て保護しようというものである。現在では、医療においても個人情報の保護に関する環境整備は重大な課題である。そのため、個人情報の取扱いに対する基本原則を設けて、その下に業務を遂行することとしている。個人情報が個人の人格尊重の下で、慎重に取り扱われるべきであるとして、5つの原則、すなわち個人情報の利用目的による制限、適正な取得、正確性の確保、安全性の確保、透明性の確保に則して機関、法人、団体および個人において個人情報保護のために、適正な取扱いをすべきであることを規定している¹⁾。

特に医療機関においては個人情報保護の観点から、人格尊重の下で慎重な取扱いが求められる。個人情報のファイルの保有に関しては、掌握事務の遂行に必要な場合に限り、その目的に必要な範囲で業務を遂行し、個人情報の漏えいなどがないように安全確保の措置をとる必要がある²⁾。

最近、個人情報の保護に関する法律が完全施行されて以降、個人情報に対する意識が過剰になったようである。今まで発行していた会員名簿の発行をとりやめたり、医療関係においては、患者の呼び出しや家族や親類などからの安否の問い合わせなどにも、個人情報の保護を理由に拒否する事態もみられるようになってきた。今後、個人情報に対する意識過剰は、社会活動や経済活動にも影響をもたらしかねないかもしれない。このことが、個人情報保護に対する今後の検討課題と言える。

3. 医療機関における医療情報の流失および紛失等

医療分野においては、大学病院等における患者情報の流出の事例が多く見られる。そしてまた、医療においては、学術・研究においては個人情報保護法や独立行政法人等の保有する個人情報の保護に関する法律の適用が除外されている。しかし、その代わり倫理指針が所管省庁から示されるとともに、倫理審査委員会による承認が求められる。しかし、現実には、患者の個人情報の流失は研究を主体とする大学病院で流出する事態が続出しているのが実情である。

大学病院からの患者の個人情報流失事件の事例としては、2007年1月18日にA大学医学部付属病院において、医師が個人で使用していたパソコンから、約150人分の患者の個人情報、ファイル交換ソフトによって、インターネット上に患者の氏名、生年月日、病状や治療の経過等が流失した。

また、2007年2月13日にはB大学医学部の学生のパソコンから、やはりファイル交換ソフトを介して、患者の69人分の個人情報、氏名、生年月日、病歴等がネット上に流れた。

さらに、2007年2月21日には、C大学医学部付属病院で同院内の更衣室で、患者の個人情報24人分が記録されたUSBフラッシュメモリを紛失した。やはり、このメモリには患者の氏名、年齢、病名等が記録されていた。これらの大学病院における患者の個人情報の流失および紛失においては、いずれもデータに対する匿名化が施されていなかった。

このように、医療における個人情報は個人の人権性の高い情報でもあるため、流失して二次被害が発生して被害者から損害賠償が求められることもあり得る。医療における個人情報は、他の業種に比べ人権に係わる情報でもあることを十分に認識しておかなければならない。

また、患者の個人情報のネット上への流失以外に、医師のノートパソコンの紛失も続出している。

2007年8月1日にD大学病院で同大学病院の医師が患者の個人情報417人分の氏名、年齢、病名等の記録された医師個人のパソコンを紛失した。医師は学会発表のために417名の患者のデータをパソコンに保存していた。他の病院で非常勤の勤務終了後、同大学病院へ車で移動する際に、パソコンを紛失した。同大学病院では院外に患者のデータを持ち出す場合は、匿名化を指導していたが、この件では匿名化はされていなかった。

2007年8月27日に、E大学医学部付属病院で大学院の元研修医が患者の個人情報85人分を記憶したノートパソコンを電車で鞆に入れたまま置き忘れて紛失した。そのパソコンには、患者の氏名、生年月日、年齢、性別、住所、電話番号、病名、診療経過が保存されていたが、一応、このパソコンにはパスワードが設定されていて、容易にはファイルを開くことができないようにはなっていた。

最近では、患者のデータが保存されているパソコンには患者の匿名化とパスワードの設定の指導を推し進めている。医療における個人情報の特徴は、一つには、紛失したパソコンが個人所有のノートパソコンである点で、患者のデータの保存された自分のノートパソコンを、診療にあたって複数の医療機関の間を持ち歩いている点である。二つめには、多くの医療機関では医療情報システムが、非常勤勤務医に対して、情報システムにおいてあまり配慮されておらず、さらに医療機関によって患者の個人情報の管理体制がまちまちである場合が多く、例えばカルテが電子化されている病院もあれば、されていない病院もある。

大学病院の医師にとっては、ノートパソコンに診療に関するデータを保存し、各医療機関間を移動し、移動中にデータの処理作業や仕事および研究をするには、ノートパソコンは確かに便利なツールである。しかし、ノートパソコンには、重要な患者の個人情報が詰まっていることから、情報漏えいの点から見れば危険性の高いツールであることから、取扱いにおいては、慎重さが求められる。

ノートパソコンだけではなく、2007年8月23日にF医科大学付属病院の研修医が、自宅で医療の症例の資料を整理作成するため、患者の個人情報を記憶したUSBフラッシュメモリを鞆にいれて持ち出し、レストランで盗難に遭った。

また、2007年8月10日の朝、国立がんセンターで出勤してきた職員が机上にワイヤーで固定してあったノートパソコン1台が盗難にあっているのを見つけた。盗まれたそのノートパソコンには、がん患者1542件のデータとして、氏名、性別、生年月日、検診および手術の所見等が保存されていた。一応、盗まれたノートパソコンには、パスワードの設定はされていた。

医療機関における個人情報の流失を完全になくすことは困難であるが、個人情報の流失に対する安全対策を講じなければ、患者からの信頼を失いかねない。医療における個人情報の流失は単に一個人の責任だけではなく、チーム医療の観点から対処する必要がある。

このような医療における個人情報の流失やノートパソコンの紛失・盗難にたいして、2007年8月30日に独立行政法人の情報処理推進機構セキュリティセンター（IPA/ISEC）は個人情報が漏えいした時の対応策を公示している。個人情報の流失やパソコンの紛失・盗難の場合の対応策として、発見および報告、初動対応、調査、通知・報告・公表等、抑制措置と復旧、事後対応の6つの個人情報漏えい事後対策を示している。

具体的には、まず紛失・盗難にあった場合は、本人の事件の発見と報告が求められる。そして、紛失・盗難を確認後、個人情報の内容と量、そしてアクセスの制限の有無や暗号化についても確認する。また、ネットワーク上での個人情報の流失の場合は、パスワード

の変更やアカウントの停止等の初動処置をとることが必要である。個人情報の漏えいに関しては、特に事件後の初動処置の対応が重要である。

医療における個人情報保護における管理対策として、まず、院内の事故の発生場所、発生時間、事故の内容、例えば、個人情報の流失なのか、個人情報の保存されたパソコンの盗難なのか、そして、セキュリティ対策がパソコンに施されていたのか等の確認と、施設の管理体制の見直しや防犯体制の強化が求められる。パソコンの盗難による個人情報の流失は、何も医療機関だけの問題だけでなく、多くの事業所や職場でも起こり得る事である。個人情報の管理責任者が普段から、情報管理の留意を強く指導していても、徐々にマンネリ化、形骸化しがちであるが、一旦、外部に個人情報の流失事件やパソコン等の盗難事件がおきてから慌てても手遅れであるので、職員相互の啓発が必要である。

4. 医療情報に対する医療機関の対応

2005年4月1日から個人情報保護法が施行され、同法には5,000件以下の個人情報を保管する事業者に対して、適用除外と明記されているが、医療機関にあってはほとんどの医療機関は同法の適用を受ける。それは、厚生労働省が通達したこの「医療・介護関係事業者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」には、医療機関にあっては、5,000件以下であっても本ガイドラインを遵守することを求めている。そして、医療における個人情報とは、診療録（カルテ）、処方箋、手術記録、看護記録、紹介状等を含め、患者個人を識別できるもの全てをさしており、1人の個人情報を1件とカウントされるとしている。

そして、厚生労働省は医療機関にあっては医療機関の対応として、個人情報保護法、本ガイドラインや診療情報の提供に関する指針の内容に沿って、個人情報保護に関する「宣言」や「規則」を定め、その「宣言」や「規則の概要」を院内に掲示し、患者本人から診療録等の開示要求があった場合は、厚生労働省が制定した診療情報の提供等に関する指針に従って対応することを指示している。

厚生労働省は医療機関が掲示する「個人情報保護に関する宣言」には、個人の人格尊重の理念の下に個人情報を取扱うことと、本ガイドラインを遵守することを明記し、「個人情報取扱い規則」を策定し、その概要を院内に掲示することを求めている。

「個人情報取扱い規則」には、下記の内容を含まなければならないが、各医療機関の実情に応じて取捨選択しても良いとしている。

- ・ 通常、必要と考えられる個人情報の利用範囲
- ・ 個人情報に係る安全管理措置の概要
- ・ 本人等からの開示等の手続き

- ・第三者提供の取扱い
- ・苦情への対応

更に、個人情報保護に関する安全管理措置として、

- ・個人情報保護に関する「苦情への対応を行う体制」を定める。
- ・個人情報保護管理者を定める（病院等では、個人情報保護推進委員会等を設置）。
- ・雇用契約や就業規則を整備し、個人情報保護に関する規定を整備する（離職後も守秘義務を課す）。
- ・アルバイトや派遣労働者も含め、職員への教育および研修を行う。
- ・個人情報の流失や盗難の予防対策など、個人情報保管物の安全管理措置を講ずる。
- ・個人情報保管物にIDやパスワードによる認証などの技術措置を講ずる。
- ・本人の照会に対応できるような検索可能な個人情報の保管。
- ・不要な個人情報の廃棄と消去に際し、復元不可能な形での廃棄を行う。
- ・業務委託している場合、委託先に個人情報保護に関する安全管理措置も委託契約に入れる。

また、医療機関における個人情報の第三者への情報提供に関しては、患者の個人情報を提供する場合は、原則として本人の同意を得なければならない。しかし、本人の同意を必要とする場合と、本人の同意を得ずとも個人情報を提供できる場合とがある。下記に示してみる。

個人情報を本人の同意なくして提供してはならない場合として、法令で本人の同意が不要とされている民間保険会社、職場、学校、家族などからの健康状態や既往症、職場復帰の見込みなどの照会など以外については、本人の同意を得る必要がある。なお、医療機関内で掲示した範囲内で特段の申し出がなければ、本人の同意があったものとしている。

本人の同意を得ずに個人情報を提供できる場合としては、薬剤師からの医師へ処方箋の確認や照会、健康保険法や薬剤師法に基づくもの、医療法に基づく立入検査、介護保険の立入検査、介護保険の指定基準や特養ホームの基準に基づくもの、訪問看護ステーションへの指示書やケアマネージャーとの連絡などに関しては、本人の同意なくとも情報を提供できるとしている。このように上記のものは同意を得る必要はないものの、法令に基づく場合であっても利用目的以外の目的で個人情報を取扱う場合は、法令の趣旨を踏まえ、その取扱う範囲を必要な範囲内に限定することが求められる。

また、遺族への情報の提供などの対応については、患者の遺族からの診療記録の開示要求に対しては、「診療情報の提供に関する指針」に基づいて対応しなければならない。更に、個人情報の利用範囲に関しては、利用範囲を院内掲示している場合において、患者から特別の申し出がない限り、同意が得られたものと判断でき得る。院内掲示にない利用範囲においては、本人の同意を求める必要がある。

5. 医療における個人情報保護の対応と日常診療

日常診療において、個人情報の保護における留意点としては、医療機関内での受付などでの患者の呼び出し、病室の名札の提示などについて、これらについては、患者の取り違え防止のために常に留意する必要があるものである。

医療機関における診療情報とは、診療の際に作成される個人情報で、診療記録として作成されるカルテ情報である。すべての診療情報が記録されるわけではなく、例えば、紹介状などは診療情報提供書に記録される場合もある。医療機関で取扱われる個人情報は、下記のものがあげられる。

- ・患者基本情報として、氏名、年齢、生年月日、住所、電話番号など基本情報以外に、連絡先、勤務先、世帯状況なども含まれる場合がある。
- ・健康保険・福祉情報としては、健康保険情報、公費医療情報、障害者手帳情報など
- ・診療管理情報として、受診診療科情報、適用保険情報、受診日、入退院日など
- ・医学的背景情報として、出生時情報、予防接種歴、既往歴、輸血歴、アレルギー情報、家族既往歴など
- ・診療記録情報として、問診記録、現病歴、身体所見、経過記録など
- ・指示記録情報として、検査および結果、処方記録、手術記録、処置記録など

上記の日常診療の情報の他に、診療・手術時における同意情報や死亡記録情報などもあるが、さらに看護記録などの情報も医療に関する情報として取り扱われる³⁾。特に、医療機関においても最近では医療情報システムの導入が進み、電子カルテとして管理され、診療記録の効率化を進めている。このようにカルテの電子化は、従来の紙カルテの保管庫のスペースを縮小し、同時に複数の職員が院内ネットワークにアクセスし、医療情報や診療記録の閲覧を可能にしている。場合によっては、患者が自らのカルテの閲覧も可能である。電子カルテの導入により、紙カルテでは困難であった医療情報としての診療記録に、レントゲン写真や動画の診療記録もマルチメディア医療情報として記録可能である。このように診療記録を電子化することによって、情報の共有化が可能になる。そして、このカルテの電子化以外にも医療機関においては、医療情報システムとして、診療記録管理システム、診療計画支援システム、オーダーエントリシステム、医事会計システムなどを構築してきている⁴⁾。

このように、医療情報の電子化が進み、日常診療にも情報システムが導入される中で、この「医療・介護関係事業者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」は「個人情報の保護に関する法律」に基づき、対象となる病院、診療所、および介護保険法に規定するサービス事業者等が個人情報の適正に取り扱うためのガイドラインとして定められた。本ガイドラインの基本的な考え方として、医療機関において個人情報の性質や利

用方法において、適切かつ厳正な取扱いが求められる。また、介護の分野においても介護事業者においては、多くの利用者とその家族に関する個人情報を知り得る立場にあることから、医療分野と同様に個人情報の適正な取扱いが求められる。このようなことから、本ガイドラインでは個人情報保護法の趣旨を踏まえて、医療および介護関係事業者における個人情報の適正な取扱いが確保できるように、具体的な取り組むべき事項を示している。また、本ガイドラインが対象とする個人情報は、生存する個人に関する情報である。そして、医療・介護関係事業者が保存している生存者における個人情報は本ガイドラインの医療・介護の情報の対象であり、さらに、診療録の形態で保存されていない個人情報も本ガイドラインの対象となる。

そして、本ガイドラインにおいては、患者や利用者の死亡後であっても、医療・介護関係事業者が患者や利用者の情報を保存している場合は、漏えい、滅失および棄損の防止のための安全管理措置を講じることが求められる⁵⁾。

このようなことから、組織的安全管理体制が必要である。患者の個人情報に対する組織的安全管理においては、管理に対して従業員の責任と権限を明確にし、手順書を作成し、安全管理の実施状況を確認しておく。組織的安全管理においては、まず個人情報保護に関する方針、組織体制の整備、個人情報取扱い手順書の整備、組織的安全管理の評価、見直しや改善と漏えい事件に対する対処等に取り組んでおく。まず、組織内における個人情報の管理について役割を分担し、責任も明確にしておき、安全管理のための組織体制を整えなければならない。また、個人情報を扱う情報システムについて運用の責任者も設置する必要がある。さらに、個人情報保護の実現のために規程を置いて、そのためのマニュアルも整えておかねばならない。

すなわち、日常診療においても医療機関内の個人情報管理者を設置し、規程を定めるとともに組織体制を整えて、安全管理に対して技術的な措置を施すとともに、従事者に対する教育および研修が必要である。教育および研修は従事者と正規の職員だけでなく嘱託職員、契約職員、派遣職員を含む職員に対しても必要である。個人情報の漏えい事件が委託先の従事者による流出や取扱いのミスによって起こっていることもあるので管理体制が必要である。また、技術的な安全管理体制も必要である。技術的安全体制とは、個人情報の漏えいや消滅および棄損の防止のために個人情報を取扱う情報システムに対し、個人情報への不正アクセスの制御、個人情報の暗号化、個人情報を取扱う情報システムに対する管理体制である⁶⁾。

6. 医療機関における個人情報の安全管理の対策

医療機関における個人情報の安全管理としては、院内における情報ネットワークシステムへのアクセス権を限定することが必要である。職員のユーザーID、パスワードや、アクセスログを記録しておき、不正アクセスに対する適切な管理体制が求められる。収集し

たアクセスログを定期的にチェックし不正アクセスに対して、管理体制を強化し、アクセス制限、削除、などの対策が必要となる。また、コンピューターウイルスに対する保護対策も求められる。さらに、医療機関における管理者は個人情報に対する施策が適切に実施されるように、職員の採用に当たっては、雇用および契約時に個人情報保護に対する守秘に関する指導を行うとともに、定期的な個人情報保護に関する教育も行う。また、退職後の元職員に対しても、個人情報保護の規定を定めておくことも必要である⁷⁾。

個人情報の管理の保護体制を整えるためには、組織や人的な管理体制を整えるだけでなく、情報システム等の技術的な管理体制も不可欠である。医療機関内で規定を定めても、完全に管理することは困難である。最近、医療機関におけるネットワークを介しての患者の個人情報の流失やノートパソコンの紛失、盗難による個人情報の漏えいが多発している。ノートパソコンのパスワードの設定やファイル交換ソフトやウイルス対策および、ファイアウォールによるネットワークのセキュリティ体制を整えることが重要である。医療機関内において、端末からのネットワークやサーバーへのアクセスによる患者の個人情報の取扱いに対する運用管理規定を作成し、医療機関内での医療情報システムの管理責任も明確化して置くことも重要である⁸⁾。

医療における個人情報は医療技術の研究のためには欠かせない情報でもある。患者個人がその重要性に納得し、医療機関もいかにこれらの医療情報を進歩のために役立てることができるか、研究開発のために活用できるかが重要だが、患者の個人情報は人権尊重という観点から取扱いに十分留意しなければならない。益々、専門分化の進む医療技術と体制の中で、患者の個人情報の活用も不可欠である。しかし、これからの医療現場においては、従来からの医療現場の個人情報に対する意識から脱却し、医療従事者の患者の個人情報に対する守秘義務等の意識を高める必要がある⁹⁾。

医療機関においては個人情報保護の施策における責務を有するが、その方策としては組織内で統括する個人情報管理責任者を選定し、各部署においては個人情報保護対策の担当者を選任する。個人情報が管理体制の中でどのように流れているか、すなわち、個人情報の組織内での管理、利用、提供、廃棄がどのように行われているかを把握した上で具体的な対策をとる。そして、個人情報保護に対する方針を定める。その方針としては、取得した個人情報の利用目的に関する方針、個人情報の管理において開示の求め等に対する方針、安全管理措置に対する方針等を決めておく。個人情報を直接、取扱う担当者に対する取扱いマニュアルの作成、又運営面での監査が求められる。実際に大事なものは、医療従事者に対する個人情報保護に対する教育である。現実では、内部関係者による個人情報の漏えい事件が多々あるからである¹⁰⁾。

個人情報保護に関しては、特定の個人を識別可能な情報については全て保護しようというものであるが、そのため、医療機関において、個人情報の取扱いに対する基本原則を設けて、個人情報が個人の人格尊重の下で、慎重に取り扱われなければならない。そして、その下に医療を遂行しなければならない。個人情報の利用目的の制限、適正な取得、安全性のもとに個人情報保護のために、適正な取扱いをすべきである¹¹⁾。

個人情報保護法に違反した場合、個人情報保護法の罰則によって、医療機関は厚生労働大臣から求められた報告や命令に従わなかった場合に処罰されるが、個人情報保護法やガイドラインに反しただけで直ちに処罰されることはない。しかし、個人情報保護法やガイドラインに反して、患者の名誉やプライバシーを侵害した場合は、民事的な損害賠償責任を負うことがあり、社会的評価も下がる。

すなわち、医療における情報倫理はコンピュータを使用し、情報ネットワークを利用するにあたっての倫理問題であり、医療従事者として、またユーザーとして社会通念として、今後、認識しなければならない問題である。それは、情報システムや情報ネットワークの信頼性と安全性に関わる重要な問題でもある。そのため、医療に関わる専門家の間では、倫理綱領を採択し、情報倫理に対する意識を高めている。それは医療従事者として、事実やデータの尊重、ユーザーに対するリスクへの配慮、秘密情報の守秘などであり、また同様に、情報システムや情報ネットワークの管理者においては、システム運用上でのユーザーへの配慮を行うとともに、システムの利用規定の作成し、実施し、情報倫理の認識のもとに、業務に携わることである。また、一般のユーザーに対しても、社会人として他人の人格とプライバシーの尊重、知的財産権や知的成果の尊重、情報システムや情報ネットワークシステムの利用規則の遵守が求められる。

7. おわりに

医療機関において、最近ネットワーク上でのファイル交換ソフトを介しての個人情報の漏えいや、個人情報の保存された電子記憶媒体やノートパソコンの盗難や紛失が多く発生している。企業や行政だけでなく、医療機関においてもこのような事件は社会問題となりつつある。そのため、個人情報保護法や厚生労働省のガイドラインで示された趣旨に基づいて、医療機関においても患者の個人情報の安全管理と適正な利用に関して、管理体制と指針を設けなければならない。特に、紙からデジタル化されたカルテなどの個人情報の安全管理体制が求められる。それは、医療関係者と患者との信頼関係を深めるためにも、また医療サービスの向上を図る上においても個人情報の安全管理は重要である。

最近、社会では個人情報の保護に関する法律が完全施行されて以降、個人情報に対する意識が過剰になったと言われているが、もし医療や福祉関係で蓄積された個人情報が、当事者の意思とは無関係に売買され利用され、悪用された場合、個人の名誉や人権の侵害になることもある。

医療においては、患者の自己情報の権利を保障しなければならないし、医師をはじめとする医療関係者に課されている患者に対する守秘義務を遵守しなければならない。患者の個人情報の取扱いと、漏えい防止の安全管理体制の整備と強化が求められる。また、患者

の個人情報におけるトラブルに対する対応策も求められる。

パソコンの盗難による個人情報の流失は、何も医療機関だけの問題だけでなく、多くの事業所や職場でも起こり得る事であるが、個人情報の管理責任者が普段から、情報管理の留意を強く指導していても、徐々にマンネリ化、形骸化しがちになる。しかし、一旦外部に患者の個人情報の流失した場合、後から慌てても手遅れであるので、日常診療において職員相互の啓発が必要である。

単に医療技術や情報技術だけを習得させるのではなく、情報の重要性に対する認識を深めさせ、それに対する倫理意識を持たせる教育を進める必要がある。

情報倫理は現代の情報化社会に生きる人間として、情報に対する社会および経済的な意義と重要性を認識し、情報化社会に生きる人間としての不可欠な倫理意識をもたせることが、今後一層必要である。特に今後の情報化社会を担う若い世代に対し、医療技術の教育の課程での情報倫理における教育は必須のものである。

【参考文献】

- 1) 岡村久道・新保史生、『電子ネットワークと個人情報保護』、経済産業調査会、2002、511-513。
- 2) 和田英夫・原田三郎・日笠完治・鳥居壮行、『情報の法と倫理』、北樹出版、1999、118-120。
- 3) 開原成充・樋口範雄編、『医療の個人情報保護とセキュリティ』、2005、28-29。
- 4) 里村洋一編、『電子カルテが医療を変える』、日経BP社、2003、38-40。
- 5) 社団法人全国老人保健施設協会編、『個人情報保護制度の手引』、ぎょうせい、2005、37-40。
- 6) 渡部喬一、『個人情報保護法のしくみと実務対策』、日本実業出版社、2005、114-132。
- 7) 日経メディカル編、『医療機関のための個人情報保護法対応マニュアル』、日経BP社、2005、35-38。
- 8) 羽生正宗、『病・医院経営のための個人情報保護対策』、ビジネス教育出版社、2005、77-78。
- 9) 喜多紘一監修、『個人情報の保護と活用の手引き』、法研、2005、16-18。
- 10) 大保久哉・羽田晋朗・高野一彦、『個人情報保護法対策』、九天社、2005、30-41。
- 11) 岡村久道・新保史生、『電子ネットワークと個人情報保護』、経済産業調査会、2002、511-513。