



平成25年度 病院長・幹部職員セミナー

平成25年8月・東京都

# これからの病院医療 個人情報保護と電子カルテ

青木・関根・田中法律事務所 弁護士  
日本病院会 認定個人情報保護団体 審査委員会 委員

青木 一男

# これからの病院医療 個人情報保護と電子カルテ

青木・関根・田中法律事務所 弁護士  
日本病院会 認定個人情報保護団体 審査委員会 委員

青木 一男

**座長（崎原）** おはようございます。日本病院会認定個人情報保護団体審査委員会の崎原でございます。本日は、本年度の「病院長・幹部職員セミナー」の1コマをいただきまして、電子カルテを中心とした個人情報の問題をお話しいたします。

雑誌の『新医療』によりますと、2011年度末で、全国で電子カルテを導入した病院は約1,300病院に上ると推定されています。そのほかオーダーリングシステム、レセプト、それからレントゲンなどの画像診断のIT化を入れますと、全国約8,800病院のほとんどが、何らかのかたちでIT化をしているのではないかと考えております。電子カルテは、カルテの書き込みの容易さ、それから情報が共有化できること、保存の容易さ、そしてデータを加工することの容易さなど、非常に有益です。しかしそういう点が、個人情報保護の問題を起こす可能性があると思っております。

個人情報については、漏洩などの事態が生じたときは一瞬かつ大量の情報が漏洩する可能性があること、外部からシステムに侵入がありますとダメージが非常に広範囲にわたるといこと、それから、医療の従事者というのは、基本的には電子カルテなどのITに不慣れであることなどの問題点が指摘されています。インターネットで調べましたところ、2012年7月から2013年7月までの約1年間に電子

媒体に関係した個人情報の漏洩は約22件ありました。その原因の多くは、パソコンとかUSB、SDカードの紛失などです。また、今年の7月10日の読売新聞に載っていますが、全国7つの医療・介護施設でメールなどの問題で300人以上のカルテが公開状態になっていたということが分かり、先日、厚生労働省から注意があったと思います。地域医療の連携などネットワーク化がこれから進むことも予想されておりますので、こういう事例が増えてくるのが予想されると思います。

そこで本日、「個人情報保護と電子カルテ」というテーマで、当委員会の弁護士であられる青木一男先生に、この件に関してお話しをしていただきたいと思っております。

恒例ですので、青木先生のご略歴を簡単にご紹介いたします。昭和14年11月27日にお生まれで、昭和38年10月、中央大学在学中に司法試験に合格されまして、昭和41年に弁護士登録をされました。

弁護士関係のご略歴では、日本弁護士連合会の常務理事をされました。それから公職関係では、最高裁判所の司法研修所の民事弁護教官、法務省の民事行政審議会の委員、司法試験考査委員などをなさっております。そして平成22年の春、これらの業績により旭日小綬章を受章されました。

それでは青木先生、よろしく願いいたします。

**座長：**日本病院会 認定個人情報保護団体 審査委員会委員長  
崎原 宏

青木 おはようございます，青木でございます。  
よろしくお願ひいたします。

さっそく個人情報保護と電子カルテの話ですが，まず，電子カルテの関わりでぜひ知って  
おいていただきたいというところからお話を始めま  
す。

## ■個人情報の保護とは何か

(スライド1) 個人情報の保護とは要するにプ  
ライバシーの保護です。プライバシーというは私生  
活の自由という権利で，憲法で保障されている権利  
です。そういうことで非常に重要なものなので，  
いろいろな法律で保護されています。

まず刑法では名誉毀損罪ということで対象になっ  
ています。それから民法では，プライバシーを侵害  
しますと不法行為ということで損害賠償請求とか，  
あるいは例えば小説で何か個人生活が暴露される  
というときにその小説の発行を差し止めるとい  
う差し止め請求権，そういったようなかたちで保  
護されます。このようにもともと刑法と民法で保  
護されていたのですが，それでは保護が足りない  
ということで，平成15年に「個人情報保護に  
関する法律」という法律ができ，きめ細かく規  
制されるようになりました。

ご記憶にあるかもしれませんが，昔，三島由紀夫  
の小説で『宴のあと』という，ある政治家の女  
性関係を含む小説が出版され，それについて損  
害賠償が裁判所で認められたというのが，プ  
ライバシーについての法的な関心もたれた最  
初でした。昭和30年代の後半のことでした。

### 個人情報の保護とは何か



スライド1

## ■個人情報と電子カルテ，紙カルテ

(スライド2) それでは，どういうものが個人情報  
として保護されていくのでしょうか。皆さんのお仕  
事のなかに紙カルテがありますが，このなかには個  
人情報が含まれているわけです。そして電子カルテ  
というのが始まりました。電子カルテと紙カルテの  
違いは何でしょうか。書いてある中身は同じよう  
なものです，個人情報保護法では個人情報とその  
電子化されたデータとに分けておきまして，電子  
化されたものにはいろいろなかたちで規制がかか  
ってまいります。そういうことで，電子カルテに  
対しては非常に厳しい規制があります。

### ●電子カルテに対する規制

電子カルテが個人情報保護法のなかでどのよう  
に位置づけられているのかですが，これ(電子カル  
テ)はデータベースですので，データベースを対  
象とするいろいろな規制があります。我々病院は  
電子カルテを通じて個人情報を管理しています  
ので，そういうものを管理する事業者(情報取  
扱事業者)という立場です。法律はその事業  
者に対して規制をかけています。

### ●電子カルテ情報にかかわる権利・義務は誰にあるのか

まず医師と事業者ですが，医師は事業者に雇  
用された職員であり，事業者そのものではありません。  
そして，いろいろな個人情報の義務や権利は医  
師ではなくて事業者である病院にあります。で  
すから，医師が「自分の情報である」とか「自  
分のものでは」

### 電子カルテの個人情報保護法上の 権利と義務

個人情報と保有 個人データ データベース	• 紙カルテは個人情報 • 電子カルテは個人データ 規制厳格 データベース
情報取扱事業者 の権利	• 内容訂正、開示、追加・削除、提供
個人の権利	• 閲覧請求権 訂正・追加・削除請求

スライド2

る」ということは言えないということです。個人情報の内容を訂正したり開示したり、あるいは追加したり削除したり、いろいろなかたちで提供するとかの権利は医師ではなく病院にあるわけです。

一方、この個人情報の対象になっている個人の権利とはいったい何だろうかということですが、ここでは閲覧請求権、それから内容について訂正とか追加とか削除を請求することができるというところまで、それを実行させる請求権ではないのです。権利としてあるのは閲覧請求権にとどまります。訂正、追加、削除というのは請求ができるだけであって、それを実行させる権利ではありません。請求されたことを実行するかどうかは病院側の判断という、その違いになります。

## ■個人情報取扱事業者の責任

(スライド3) それでは我々病院の、個人情報取扱事業者の責任は何かということですが、法律で定めているのは、まず、適正に取得しなければならないということで、これは当たり前です。そして、正確

### 個人情報取扱事業者の責任

- d. 適正取得 正確性と最新性
- e. 安全管理
  - ・システムの機械的防御  
(セキュリティのハード・ソフト、  
開錠キー、修正・削除の履歴等)
  - ・人間管理による防御  
(規則 教育 監査 台帳)

スライド3

### 個人情報とは何か

- ・ 生存する個人  
死者の情報は遺族の情報
- ・ 特定個人の識別
- ・ Aと特定される+Aと識別できる  
匿名化・背番号は対応表が<sup>秘</sup>か

スライド4

なものでなければならない。常に最新でなければならない。それからもう1つ、安全管理義務というものを強く定めています。

## ●安全管理

安全管理には、ご存じのとおり2つ方法があります。機械に委ねる防御と、人間の統制で管理し防御するものとの2つです。

### ・機械に委ねる部分

機械というのはご存じのとおりで、セキュリティのハードあるいはソフトです。具体的に言いますと解除キーがあります。誰がそれを見ることができるか、誰がどの部分を見ることができるかというのを、その職務の立場にある人ごとにキーを変えて、ある範囲の職種の人はある範囲しか見られないというようにしたのが解除キーです。それから、修正したときに元の内容が消えてしまうと消したということになるわけです。ですから、それが消えないで、訂正したという履歴で出るような仕組みにしておく。そういうものが機械的な部分です。

### ・人間管理による部分

人間管理は忘れがちですが非常に大切なことです。まず「規則」をつくることです。誰がどういうところまで関与できるとか誰の責任であるとか、そういう規則を定める。それから「教育」です。それから「監査システム」。それから非常に大事なものは「台帳」をつくることです。患者さんの誰からどういう請求があったということをきちんと記録して、それに対してどういう措置をした、そういうことを記録する台帳をつくるのが大事です。

## ■個人情報とは何か

(スライド4) そこで、少し戻りますけれども、個人情報とは何かということです。

まず、生存する個人の情報であるということです。患者さんが亡くなったら、カルテの情報は誰の情報になるのかということでは、亡くなってしまった死者の権利というものではありません。死者の情報は遺族の情報になるということになります。ですから、先ほどちょっと述べましたが、追加とか修正とか削除とか、そういうものを請求する権利とまでは言えませんけれども、「請求することができる」というのは、遺族がそういう立場に立ちます。遺族はそういう追加とか修正とか削除とかを請求をすることがで

きるということです。

もう1つキーワードがあります。それは、個人情報とは特定個人のものであるということです。例えばAと特定される。私であれば青木一男です。その青木一男であるという名前と個人に結び付くものとして、どのように識別するかという方法。普通ですと氏名を挙げれば識別されるわけです。野球の選手には背番号があります。Aの背番号は何番と皆が知っていれば背番号で個人が識別されるわけです。個人情報はそのように、「識別される」というプロセスと組み合わせられています。匿名化されればこれは分からないわけです。単純にA, B, C……, あるいは1番さん, 2番さん, 3番さん……, それだけでは1番さんが青木一男であることは分からない。ですから1番, 2番とされたデータだけでは個人情報ではないということになります。しかしその対応表が誰にでも分かるということだと、対応表で結び付きますから識別されることになります。ですから、そういう対応表がマル秘になっているかどうかが大事になります。

大事なことは「特定個人」「匿名化」というところですが、匿名にされたものはいいんですが、匿名化される前の段階、例えば、何かの研究発表で、ある患者さんをAという記号で匿名にして発表したとします。そうしますと、このように発表されたあとは個人情報ではなくなるのですが、そのAという記号で何か本に書くという、そこまでのところで個人の「青木一男」の情報を使ったというところでは、これは規制対象になるわけです。ですから大事なことは、A, B, C……という記号にしてしまえば使っていいというわけではないのです。その「青木一男」という情報を利用したというところはやはり残ります。ですから、単純に匿名はいいといっているけれども、匿名されるまでのプロセスのところは規制対象になるということです。

## ■個人情報は誰のものか

(スライド5) よく患者さんから、「カルテの内容は個人情報でおれのものだから修正しろ」とか、「ここはおかしいじゃないか」とか、いろいろ言うてくるわけです。ではそのカルテの情報はいったい誰のものなのか。その当該患者のものなのか、それとも病院のものなのか、あるいはそれを書いた医者のも

## 個人情報は誰のものか

### 情報媒体作成者の著作権

- 写真撮影者と被写体モデル
- 小説とモデル

### 情報媒体作成の目的

- 診療する者にとっての業務記録

### ソース権

- 診療内容は診療者の権利
- 個人特定事項は患者の権利

スライド5

のなのか。

### ●情報媒体作成者の著作権

個人情報というのは記述されたものです。ですから書かれたものは1つの記述されているメディア、情報媒体です。その記述の当該の患者さんは、写真であれば被写体のモデル、小説であれば登場人物のモデルとおなじです。情報媒体として考えると患者さんは単なるモデル、対象物ですので、そういったことからカルテの情報は患者さんのものではない。そうすると誰のものかという、それをつくった人の権利、著作権なわけです。ですから情報媒体であるカルテ（電子カルテも含めて）は誰のものかという、病院のものであるということです。

### ●情報媒体作成の目的

それを何のためにつくるかですが、これは診療する者にとっての業務上の記録のためです。

ソース権。よくニュースソースと言いますが、このソースの権利がカルテではどうなるか考えてみますと、どういように診察したか、どうい病名であるかという内容は診療した者の権利になる、つまりソースは診療した者、病院にあるわけです。そのなかに患者を特定する「青木一男」というような名前、あるいは家族関係も書かれることがあります。それはその個人を特定する部分で、そのソースは患者から出たわけですから、その部分のソースは患者の権利であるということは言えますけれど、言えるのはそこまでです。

### ●利用制限と目的の範囲

(スライド6) 先述したように、法律は規制をかけていますが、一番大事なことは目的です。その情報を利用する目的がはっきりしていること。そして、

その利用はその目的に限られます。ですから目的を特定するということが大事です。当たり前ですが、カルテの目的は1人の患者の診療です。医学研究は直接の目的ではありません。医学研究にもし使うということであれば、目的の範囲を広げる必要があります。診療目的だけではなくて医学研究ということも目的の範囲に入れなければならない。そして法律は、この利用の目的を開示しなければならない、通知しなければならない、と定めています。ですから、院内のいろいろなところに掲示したり、インターネットに載せたり、あるいは患者さんに渡す最初の書類——病院の診察を受けるにあたってのお知らせとか、診療を受けるにあたっての注意とか、いろいろなものがあります——、具体的には最初の1枚のペラの紙にきちんと書く必要があります。それが大事であるということです。

#### ●目的外利用と第三者提供

これがいつも問題になるところです。目的外利用というのは、先ほど言いましたように、診療で得た情報は医学研究とか疫学調査——保健所が中心になるかもしれませんが、どういう病気にどのような地域的な特徴があるとか、いろいろな疫学的調査があります——の対象にもなるわけです。疫学というのは直接の目的ではありませんから目的外利用になるので、これ（医学研究や疫学調査に利用するという）も明記しておかなければなりません。

それから第三者提供。これをするには患者の同意が必要です。事前に同意してもらう必要があります。

## 個人情報とは誰のものか

- 利用制限と目的の範囲  
特定患者の診療 医学研究
- 個人の権利 プライバシー権
- 目的外利用と第三者提供  
事前同意 グレーゾーン(医療連携)

スライド6

ですから先ほどの最初に患者さんに渡すペーパーに、「こういう場合にこういう第三者に情報が提供されることがあります。ご承知おきください」というようなかたちで、きちんと書いておかなければなりません。

最近、医療連携が広く行われますが、これは目的の範囲内なのか範囲外なのか、これはなかなか分りにくいグレーゾーンです。そういうことで、「医療連携の目的」と「関連する医療機関それから自治体に提供されることがあります」ということもきちんと明記しておく必要があります。

## ■個人情報取扱事業者の責任

(スライド7) 個人情報取扱事業者である病院の責任です。先ほど言いましたように、「利用目的の特定」が一番大事なことです。

### ●利用目的の範囲外の利用の禁止と事前同意

「利用目的の範囲外の利用」は法律で禁止されています。しかし「事前の同意」があればいいので、事前の同意書を取っておくことが必要になります。

範囲外の利用にどういうものがあるかという、研究もそうです。広く言いますと、病気に関する情報はその患者さんだけのものではなくて、世の中のために広く使われる必要があります。

例えば法律のうえでこういうことがあります。予防注射です。子ども

## 個人情報取扱事業者の責任

- a. 利用目的の特定
- b. 利用目的の範囲外利用の禁止と事前同意  
(研究 薬品開発 疫学・統計等)適用除外:大学等研究機関
- c. 第三者提供の禁止と事前同意(医学研究、疫学資料、薬品開発、診療連携、これらは病院の管理下で行われ医師の個人的利用禁止)適用除外:大学等研究機関  
第三者の例:生命保険、賠償保険、職場、学校、アンケート、マーケティング、医療連携?

- abcについての院内掲示、ネット上の掲示、同意文書
- 適用除外者も厚生労働省告示

スライド7

に予防注射をする。そのお金を誰が払うかですが、親が払うとなるとお金を取られるのは権利（財産権）の侵害であるというわけです。予防注射はいったい誰のためにするのでしょうか？ 普通の人は自分のためと思うでしょうが、そうではなくて、ほかの人に移さないために予防注射をするんですね。法律はそのように見るんです。ですから予防注射でお金を出したり痛い目をするというのは、自分のためではなくて人のため、つまり公のためにそういう負担をする。だから予防注射は無料でなければならないという考え方です。公のためにするわけですから。

そういうことから考えますと、病気というのは、自分のために病気を治すだけでなく、自分のデータが人様の健康のためにも役立つわけです。だから、そういう情報は個人のものだけでなく公のものもある、そういう考え方が出てきます。研究はみんなのためですから、個人は公共の福祉のために提供しなければならない、そういう義務を負っているという考え方をするとき、研究は利用目的の範囲内に入ってくるでしょう。けれども、これはグレーゾーンなわけです。1つの考え方ではない。そう見てきますと、研究のためというのもグレーゾーンなので、目的の範囲外ととられる心配があるということで、先述したように事前同意を取る必要があります。

それから医薬品開発。これも同じことです。これも公共のためではあるんですけど、別な人を見ると、それは薬屋のためじゃないか、とそんなようにとられてしまうわけです。疫学とか統計とか、いろいろなグレーゾーンがあります。

ただし、法律では範囲外の利用の禁止についての適用除外を明記しております。それは、大学などの研究機関で利用するについては、個人情報保護の対象外、適用除外となっています。事前同意も要らないということになります。

一般の病院も広い意味では研究機関です。しかし、普通の病院は研究機関ではないと言う人もいますので、これもグレーゾーンです。ですから、「当病院における研究に使います」ということを利用目的として明示しておくことが必要です。

#### ●第三者提供の禁止と事前同意

先述しましたように、第三者提供は原則禁止です。ただし事前に同意がある場合には許されます。です

から同意書に同意文言を書いておくことです。第三者提供には、先ほど言いました医学研究、疫学資料、薬品開発、診療連携……まあいろいろあります。第三者提供は、先述の利用目的とはまた違う次元の話ですので、利用目的の範囲内であっても第三者提供であれば、事前同意を受けなければならないことになります。これはきちんと書類で承諾してもらう必要があるということです。

病院に患者さんが言ってくる文句のなかに、「保険会社になぜ知らせたんだ」というのがよくありますが、保険会社は明確に第三者です。患者さんの入っている生命保険の生命保険会社もそうですし、交通事故とか賠償型の保険で患者さんとは関係なく加害者のほうの保険会社からも聞かれます。よくあるのは、「うちの社員が病気だと言って休んでるけど、どうなんでしょうか」と会社から聞いてくるわけです。これも第三者提供です。それから、「うちの生徒が病気で休んでいるのだけれどどうなんでしょうか」と学校から聞いてくる。この学校も第三者です。この辺は常識的に教えてもいいのではないかと思われるがちですが、第三者です。アンケートとかマーケティングとかの問合せがきたらこれも第三者です。これらは分かりますが、医療連携は先述のとおりグレーゾーンです。

第三者提供というのは重要で、ひっかかりがちですがまず全面禁止と置いていてください。ですから事前同意が絶対的に必要であるということです。

#### ●利用目的、第三者提供に関する患者への通知

これらを患者さんにどう知らせたらいいかですが、院内掲示、ネット上の掲示、それから先述の同意文書です。先ほど大学などの研究機関は適用除外と言いましたが、適用除外とはいえ国は非常に厳格な規制をしています。見たことがあると思いますが、厚労省の告示というかたちで「特別な〇〇疾病に関する□□研究に関する告示」というようなかたちで出てきます。あれがそうです。

#### ■個人情報取扱事業者の措置

（スライド8）個人情報取扱事業者の措置というのは法律で決めてあることですから、これはきちんとやらなければなりません。

質問応答体制。質問があったらこういうように応答します、というその体制を整備しておかなければ

なりません。具体的に言うと、担当者を決めておく。担当者は聞かれたら、誰に対して応答するか、情報を誰から取ったらいいか、そういう組織図と言いますか、そういうものをきちんとつくっておくことです。それがないとおたおたしてしまうでしょう。おたおたしないような体制ということです。

閲覧・コピー体制。個人（患者）は自分に関する情報を閲覧することができますし、コピーを求めることができます。だから請求があったらきちんと閲覧・コピーできるような体制にしておかなければなりません。

個人データの訂正請求があったら、それを調査して、必要があれば訂正し、説明し、通知をするという体制が必要です。

利用目的の範囲外とか不正取得、そういう問題があればすぐ利用停止の措置をする。また、利用停止請求に対する対応を決めておく。そういう体制をきちんと整備しておかなければいけません。

それから、手続き、手数料、窓口などを院内掲示などできちんと分かるようにしておきなさいということも、細かいことですが法律に書いてあります。

## ■厚生労働省のガイドライン

法律は、「個人情報取扱事業者の責任」という言葉と「取扱事業者の措置」という2つの言葉を使っています。つまり「こういう責任ですよ」と「こういう措置をしなければなりませんよ」ということです。法律が決めているこの2つの場面を実現するために、厚労省ではガイドラインを決めています。このガイドラインはとても分厚いものです。それから、法律

## 個人情報取扱事業者の措置

- a. 質問応答体制
- b. 閲覧、コピー体制
- c. 保有個人データの訂正請求に対する調査、訂正、説明、通知等
- d. 利用目的範囲外、不正取得の理由で利用停止請求に対する対応
- e. 手続き、手数料、窓口等の院内掲示等

スライド 8

のガイドラインもありますが、これも分厚いものです。ですから読むのは大変です。今日皆さんにお配りしているレジュメに、その分厚いガイドラインをまとめてあります。分厚いガイドラインを読むのが面倒な人はお配りしたレジュメを読んでください（本記事の最後に収録）。それで大体は分かります。それと、日本病院会にメールでもファックスでも何でもいいですから質問を送ってください。きちんとメールやファックスでお答えいたしますので。

サラッとガイドラインについて触れておきます。

### ●外部委託と第三者提供

（スライド10）外部委託と第三者提供。病院はいろいろな外注業者にいろいろなことを頼んでいます。最近、病院にけっこう多いんですけど、医療事務を外部の業者に委託していたり、どこかの都立病院は請求書に病院の名前でなく委託先の会社名が書いてあったりします。そのように委託者がたくさんあるわけです。その場合、第三者に情報を委託しているということになるんですが、大事なものは責任分界の明確化です。責任分界という言葉はしょっちゅう出てきます。どこからがどっちの責任だということをきちんと規則で決める、契約書で決めるということです。

自治体や医師会との協定も契約書できちんとする。それから暗号化なども必要になります。テレワーク。最近では往診を電話でやりとりするとかもあります。

### ●情報の相互運用性と標準化

情報の相互運用性と標準化とは、要するに分かりやすくということ、標準化ということです。ただ、最近では電子カルテで言葉が共通化していますが、あ

## 厚労省のガイドライン

### 通常運営における責任

- システムについての説明責任
- 管理責任
- 定期的見直し責任
- 責任体制の明確化（諸規則）
- 患者・利用者窓口の設置、表示

### 事後責任

- 行政機関への報告、公表、原因と対処の説明
- 善後策責任

スライド 9



れはある意味では困るんですね。内容が薄くなっているんです。普通の紙のカルテのように細かく書いてない。そのために、裁判で病院が損するということが起こってきます。カルテはできるだけ詳しく書くということが大事なんです。が……。

保存性の確保。この辺は当たり前です。

●情報の持ち出しの不可、管理

一番問題なのは情報の持ち出しです。病院の職員が「この名前、私の知人だわ。うちの親戚だわ」といって盗み見しちゃうんです。これ、けっこう地方であるんです。これをどのように防ぐか。先ほど言った規則とかシステムとか、いろいろな方法があります。

それから、「ちょっとこれ大変だから、カルテはうちへ帰って書こう」というんで、先生が情報をUSBに取り込んで持ち帰って、メディアをなくしたりとか、家のパソコンから漏洩したりとか、そういう問題が実際に起きています。

●厚生労働省ガイドラインに載っていること

(スライド11) ガイドラインは、いろいろなことを言っています。

災害時・非常時マニュアル。災害時・非常時にはどうしたらいいのかをきちんと規則で決めておかなければならないということです。早い話、地震になったら誰が何を持ち出すか、どうするかということです。

それから、外部と医療情報を交換する場合の安全管理。研究会とか地域協議会とかいろいろなことがあります。その場合に何を持ち出せるか、何を持ち出してはいけないのかということ。こういったことはみんな規則で決めなければならないということです。

スキャナーの利用もそうですけれど、そういう基本的な安全管理をしっかりするということです。

それから、サーバーが一杯になっていきますと、何年分もそのままにしておくわけにいかなくなりま

### 厚労省のガイドライン

外部委託と第三者提供	情報の相互運用性と標準化	情報の持ち出しの不可、管理
<ul style="list-style-type: none"> <li>• 委託の責任分界の明確性、契約書</li> <li>• 地域医療連携における自治体・医師会と協定</li> <li>• 第三者提供の責任分界</li> <li>• 暗号化、外部保存機関との責任分界</li> <li>• テレワーク</li> <li>• 技術的対策と運用における対策の責任分界</li> </ul>	<ul style="list-style-type: none"> <li>• 見読性、共通言語の標準化</li> <li>• 保存性の確保</li> <li>• 真正性の確保</li> </ul>	<ul style="list-style-type: none"> <li>• 機械対応</li> <li>• 規則対応</li> </ul>

スライド10

### 厚労省のガイドライン

災害時・非常時マニュアル	情報システムの基本的な安全管理	安全対策
外部との医療情報交換する場合の安全管理	電磁保存の要求事項	診療記録及び診療諸記録を外部に保存する際の基準
診療記録等をスキャナ等により電子化して保存する場合について	運用管理について	情報システムの安全管理と法的責任

スライド11

す。DVDに移し替えて保管するとかいろいろありますが、そういう場合の細かいこと、どういうものは消していいとか、どういうものは消していけないとか、そういうことも大事です。

運用管理。先ほどいくつか言いましたけれども、そういった日常の安全対策です。例えば昔は——今もそうですけれど——紙カルテ、ものすごく膨大な量なので倉庫会社に保管してもらうんですが、その場合の責任分界を契約書できちんとしておくということなどです。

ちょっと参考までにお話ししておきます。カルテは何年分保管したらいいのかということですけど、皆さん、どう思いますか。医療法には5年というのがあるんですね。じゃあ5年保存すればいいのかというと、もう膨大なので1年保管であとは捨てちゃいたいとか、3年保管にしたいとか、いろいろ考え

方があります。視点は2つあります。それは責任の問題と学術資料としての面です。責任の面では消滅時効というのがあります。患者さんから損害賠償を請求されたときの、その時効です。それは患者さんが損害賠償の請求をできる時——何か事故であることに気がついたその時——から10年です。ですから最低10年は防御のためには保存が必要だということなのです。

なぜ5年という説が出るかという、1つは先ほどの医療法の規定がありますが、税金の時効が5年ですので、その辺が1つ根拠になっているのかもしれない。

大学なんかでは、統計資料・疫学資料という面がありますので、この面からは何十年という可能性はあるでしょう。そういう学術研究、疫学、そういう

面の必要もまた考えなければならないでしょう。

時間が過ぎていきますので、あとはお手元に配布したレジュメをお読みいただけたらと思います。たくさんご質問をいただけるとありがたいと思っております。ありがとうございました。

**座長(崎原)** 青木先生、どうもありがとうございました。

個人情報の基本的な問題から、レジュメに書いてある電子カルテまで、先生にいろいろ教えていただきました。時間がないのでここで質問をお受けすることができませんので、質問がありましたら、青木先生が言われたように、先生のほうにメールとか何か質問書を送っていただければ幸いです。

(当日配付資料)

## 個人情報保護と電子カルテ

弁護士 青木 一 男

### 1 保護法益 プライバシー、名誉、信用 非財産権としての人格権

私法秩序 権利侵害のないかぎり原則自由 侵害に対しては

①民法の不法行為として慰謝料の損害賠償請求権

②人格権、受忍限度論から妨害予防請求権 妨害排除請求権として侵害行為の差止請求権

個人情報保護法の制定 原則自由(人権侵害があれば損害賠償)から法的規制へ

### 2 個人情報とは何か

#### (1) 個人情報の保護に関する法律の定義

生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述により特定の個人を識別されることが出来るもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。)(2条)

#### (2) 個人情報保護法 法律の目的 個人の権利利益を保護する。(1条)

個人の人格、尊厳、プライバシー等保護すべき情報 他に伝達されることによって個人が侵害される情報

死亡者の個人情報は、どう取り扱うか。

開示請求権 コピー請求権は遺族あるいは相続人にあるか

遺族、相続人に関する個人情報といえるか

#### (3) 個人情報とはどのような情報か

特定の個人と結びつく情報 個人が特定されない情報は個人情報ではない。

個人が識別されない情報は個人情報ではない。

A, B, Cなどでも背番号のように、個人を特定する標識は個人が特定されていることになる。

個人特定性のない標本は個人情報ではない。

情報とは何か 人にかかわる知らせ 伝達の対象となり得る事柄

### 3 個人情報は誰のものか

個人情報の取り扱い者（情報入手者、媒体作成者、利用者等）が、情報を創出する。

自分のため（自己目的 自己の記録 著作活動 自己の事業）は自分のもの

他人のために（他人からの委託）は委託者である他人のもの

診療記録（カルテ 看護記録 検査記録 画像記録等）は、診療機関の事業目的のためであり、診療機関のもの

診療記録の著作権 作成者に著作権が帰属する。作成した医師等は職務著作であるから病院が著作権者

### 4 利用制限

利用目的をできる限り特定しなければならない。（15条）

利用目的の変更は変更前と相当の関連性を有すると合理的に認められる範囲に限られる。

目的達成に必用な範囲を超えて個人情報を取り扱ってはならない（16条）

診療記録の利用目的 当該患者の診療

医学研究の資料としては目的内か目的外か 大学病院は医学研究の場なので、診療記録は利用目的内といえるか

大学病院でない病院でも所属医師の学問研究は同様といえるか

診療記録から個人特定を抹消（氏名を黒塗り）すれば、個人情報ではなくなる。情報管理者である病院の責任で個人特定を抹消する。

### 5 個人に情報について権利はあるか

個人に情報の所有権や権利帰属性はない 小説のモデルは権利帰属者ではない。名誉やプライバシーの保護の対象者としての人格権がある立場

個人の権利 個人が特定ないし識別されてなければ人格侵害は起らない。

名誉やプライバシーの権利からの妨害予防請求権としての利用制限の請求権

人格権の妨害予防請求権、妨害排除請求権（人格権の物権的請求権）

利用目的必要範囲逸脱差し止め請求権（15条による禁止請求権）

個人が識別されない標本としての利用は侵害とならないが、法16条の利用目的制限違反となることはある。研究発表など

「診療記録の内容は、医学向上のために氏名等個人が特定される部分は削除又は抹消したうえで研究の資料及び研究発表に利用されることがあります。」と患者に最初に交付する書面や院内掲示することが望ましい。

### 6 診療（診察と治療）記録（カルテ 看護記録 画像 検査記録等）

個人情報利用の目的 診療目的で研究は目的外

個人情報目的外利用の事前同意

目的の範囲外利用の範囲を特定し、その取扱いの事前同意は必要か

個人の特定制別不能な標本とした情報は、個人情報ではない。（2条）

第三者提供の事前同意

転院先診療機関への提供に事前同意は必要か

診療目的の範囲内の取り扱いであり不必要

研究機関の研究、製薬会社等の治験等のための提供に事前同意は必要か

本来の治療目的ではないので必要だが、個人識別不能な標本となっていれば事前同意は不必要

## 7 電子カルテの法律上の位置づけ

「個人情報」と「個人データ」との違い 個人情報は裸の情報 個人データはコンピュータのデータ  
電子カルテとペーパーカルテの違い 情報の媒体の違いからくる違いだけ  
個人データ、保有個人データ（2条2項、4項、5項）

「個人データ」とは、個人情報データベース等を構成する個人情報をいい、「個人情報データベース等」とは、個人情報を含む情報の集合体であって、特定の個人情報を電子計算機を用いて検索できるように体系的に構成したものをいい、「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止を行うことができる権限を有する個人データをいう。

## 8 個人情報取扱事業者の責任（16条ないし23条）

- ①個人情報の利用目的の特定
- ②利用目的の範囲外の利用の禁止 範囲外には事前の同意（最初の交付書面に同意書の明記）
- ③適正な取得 偽りその他不正の手段による取得の禁止
- ④個人情報取得に際しての利用目的の通知と公表（院内掲示、インターネットと最初の交付書面に明記）
- ⑤データ内容の正確性と最新性の確保
- ⑥安全管理措置 漏えい、滅失、き損の防止その他個人データの安全管理に必用かつ適切な措置（院内組織に個人情報安全委員会の設置、パトロール等）
- ⑦従業者（職員、派遣従業員、請負従業員）に安全管理が図られるように必要かつ適切な監督（就業規則、契約書に義務の明確化）
- ⑧個人情報の取扱を外部に委託する場合の委託先に対する安全管理の監督（契約書に明記）
- ⑨あらかじめ本人の同意のない個人データの第三者提供の禁止（必要な場合には、書面で事前の同意書）

## 9 個人情報取扱事業者の措置（24条から31条）

- ①保有個人データについて、本人から求めがあれば、遅滞なく回答できる状態に置く（診療内容の質問に対するの応答体制）
- ②本人から保有個人データの開示（閲覧やコピー）の求めがあれば、直ちに対応できる体制
- ③本人から保有個人データの内容が事実でないとの理由で内容の訂正、追加又は削除を求められたときは、遅滞なく調査を行い、必要があれば訂正等を行う（調査の結果訂正等の必要がなければ行わない）
- ④訂正を行ったとき、行わなかったとき、いずれの場合も遅滞なく本人に調査の結果と訂正を行ったか、行わなかったかを通知する。
- ⑤本人から個人データが利用目的に必用な範囲外に利用されているとか、不正な方法で取得としたという理由で利用停止を求められたときは、遅滞なく調査を行い、理由があれば、当該利用を停止し、停止する場合にはその通知、停止しない場合には調査結果と理由を通知する。
- ⑥本人からの開示の求め、訂正等の求めについて、受け付ける方法を定めることができる。また、開示、訂正等を求める事項を特定するに足る事項の提示を求める。
- ⑦利用目的の通知や閲覧、コピー、について合理的な範囲の手数料を定めることができる。
- ⑧個人情報の取扱に関する苦情の適切かつ迅速な処理に努めなければならない。
- ⑨個人情報取扱事業者は、個人情報の利用目的、閲覧、コピー等の手数料、政令事項等の公表（院内掲示、インターネット）

## 10 電子カルテにおける個人情報保護の仕組み

システムにアクセスできる者の範囲と開錠キー  
データの複製不可と外部への取り出し、持ち出し不可  
プリント、画像複製の許可条件と可能な開錠キー  
データの書き換え、修正、日付変更等の不可、修正は修正履歴が残るアクセスの記録（日時アクセス者の氏名等）

## 11 個人情報管理台帳

開示申出の日時、申出者の住所氏名、申出と回答・意見等の内容

(当日配付資料)

# 厚労省の「医療情報システムの安全管理に関するガイドライン」(H22.2)

## (1) 通常運用における責任

医療情報の適切な保護のための適切な情報管理

### ① 説明責任

システムの機能、運用方法が基準を充たしていることの説明、システムの仕様、運用方法の文書化、定期監査と監査報告書、問題のあった場合の真摯な対応、対応記録と検証可能状況

### ② 管理責任

管理状況の定期的な報告、管理責任の監督体制、個人情報保護責任者の指名、電子カルテ個人情報保護の有知識責任者を置く、就業規則・雇用契約書・外注先との業務委託契約書等において個人情報保護に関する条項、守秘義務等の明記、教育の実施、保守作業・清掃作業後の定期的なチェック・作業内容・結果の確認、退職・契約終了等の事後責任の明確な書面、情報の破棄については破棄権限者・破棄の承認等の手順、

### ③ 定期的見直し改善責任

システムの運用管理状況の定期監査、問題点の洗い出し改善、管理の再評価・再検討の定期的実施

## (2) 事後責任

不都合な事態（情報漏えい等）が生じた場合の責任

### ① 説明責任

事態発生を行政機関に報告、公表、原因と対処法の説明

### ② 善後策を講じる責任

原因追究し明らかにする、損害補てん、再発防止策を講じる

## (3) 委託と第三者提供

外部の医療機関や情報処理関連事業者、製薬会社、研究者、その他に医療情報が伝送あるいは提供される場合がある。この場合は「委託先」と「提供先」とに分けられる。

① 委託における責任分界

委託先との協同で(1)(2)の対応をする。委託者と受託者との分担業務の振り分けと責任帰属者の振り分けの明確性、契約書で明確に

② 第三者提供における責任分界

第三者の情報利用の適法性 目的の適法性が医療機関にとっての正当性となる。あとは第三者の責任範疇。例えば情報処理関連事業者等

製薬会社, 研究者, 大学等の研究機関についてはどうか。

③ 地域医療連携での患者情報交換

送信について情報処理関連事業者が何らかの積極的役割を担う場合と通信手段となるだけの場合とがある。前者では、業者と契約で分界を明確に、後者では協定書等で送信側と受信側での責任分界を明確に

④ 暗号化やデータ外部保存機関との責任分界

盗聴, 改ざん, 侵入等に対する暗号化等の安全性や責任を明確にする

⑤ テレワーク (往診と院内との情報交換) の管理

専用通信業者が介在する場合の責任分界, 一般公衆通信を使用する場合の安全管理

⑥ オンライン外部保存の委託

外部保存機関の選定基準と情報取扱いに関する基準の適合, 契約で(1)(2)の責任分界を明記と監督, 要報告

⑦ 技術的対策と運用における対策の責任分界

システムの安全性は技術的対策と運用との総合的な組み合わせによって達成される。前者はコストがかかるので, 経済的余裕がなければどのような運用でカバーするか計画。運用規定, チェックリスト

(4) 情報の相互運用性と標準化

入力された情報の再利用, 共有, 再入力不要等の便利性的見地

① 見読性の確保 見易さ 扱い易さ 共通言語等の標準化, 間違いが起き難い (フェイルセーフ)

② 保存性の確保 保存の安全性, 恒久性, システム更新に易移転性

③ 真正性の確保 改変・消去は, その内容・履歴が確認できるシステム, 作成及び改変等の責任の所在を明確にすること

(5) 情報の持ち出し

持ち出し禁止とするか。持ち出し可の場合の条件についての規則化

持ち出し後のウイルス感染データが戻されシステム感染源となることもある。

(6) 災害時, 非常時での運用のマニュアル

システムダウンや停電時等でのシステムによらない手作業による診療業務と病院運営のマニュアル, 復旧時のシステムへの引き継ぎや連結の整合性・方法

(7) 情報システムの基本的な安全管理

① 安全管理措置 個人データの漏えい, 滅失・き損の防止その他データの安全管理のための必要かつ適切な措置

従業者の監督・就業規則等の規則 委託先の監督・契約書で責任限界の明記

- ② 方針の策定と公表 具体的な内容はJIS Q15001：2006（個人情報保護マネジメントシステム要求事項）
- ③ ISMS（情報セキュリティマネジメント） 具体的な内容はISO／IEC27001：2005ならびにJIS Q27001 @ 27006の規格の構築と実践
- ④ 取扱い情報の把握  
取り扱う情報のリストアップ 重要度に応じた分類, 最新の状態の維持 必要に応じて速やかに確認できる状態
- ⑤ リスクの分析  
管理上・操作上の過誤 機器の故障 外部からの侵入 利用者の悪意・過誤 無権限者による不正アクセス・改ざん・き損・漏えい・滅失 権限者による不当目的でのアクセス・改ざん・き損・漏えい・滅失 ウイルス・サイバー攻撃 入力に使用した原稿・データ・資料等の破棄 端末機器・媒体の持ち出し 打ち出したペーパー・フィルム等の持ち出し 欠陥・バグ・操作ミス・故障・機能不全 情報漏えい
- ⑥ 運用管理規定・運用マニュアルの策定 教育 就業規則・外注契約書での義務・責任と罰則
- ⑦ 患者への公表・同意書

#### (8) 安全対策

- ① 物理的安全対策 入退館の管理 盗難・盗撮防止の物理的保護 防犯カメラ
- ② 技術的安全対策 利用者の識別及び認証機能 iD・パスワード  
不正ソフトウェア対策 セキュリティソフト
- ③ 情報の区分管理 アクセス権限の管理 職務権限と情報を区分し職務と人的安全対策 応じたアクセス範囲の限定 守秘義務契約
- ④ 情報の破棄 破棄の基準 破棄の手続きと手順 権限者の特定 管理規定
- ⑤ 情報と機器の持ち出し  
持ち出しの基準 持ち出しの手続きと手順 許可権限者の特定 管理規定
- ⑥ 災害時と非常時  
何が起きた時, 誰が何をするかの計画の策定 周知

#### (9) 外部との医療情報交換する場合の安全管理

- ① 通信経路における安全性 誤送信・なりすまし・盗聴・改ざん等の対策  
解錠キーの設定や介入限界の設定等 セキュリティ
- ② 専用線, 公衆網 (ISDN ダイヤルアップ インターネット), IP通信網, モバイルによるインターネットによる通信の安全性
- ③ 患者同意, 通信の相手方の確認等の手順 手続き等のマニュアル 接続できない場合の措置等
- ④ 患者等の個人情報対象者からのインターネットによる申請と申請者本人への送信について, 予め規則で定めておく。公衆通信利用にともなうリスクについて免責同意条項等④患者等の個人情報対象者からのインターネットによる申請と申請者本人への送信について, 予め規則で定めておく。公衆通信利用にともなうリスクについて免責同意条項等

(10) 電子保存の要求事項

- ① 内部保存か外部保存か
- ② 保存データの障害等に対する真正性・見読性, 保存性の確保
- ③ 監査 媒体の劣化・陳腐化対策 データ形式の標準性 責任

(11) 診療録及び診療諸記録を外部に保存する際の基準

- ① 保存場所・方法・管理体制の説明責任 委託側と受託側の責任範囲 定期的監査・改善
- ② 守秘義務 アクセス禁止 漏えい等の事後責任の明確化 契約終了時の処理
- ③ 利用性の確保 数年後の求説明・問い合わせ, 訴訟, 監査等での見読性
- ④ 患者への外部保存していることの揭示 責任の所在(病院)の説明

(12) 診療録等をスキャナ等により電子化して保存する場合について

- ① 保存マニュアル 保存の目的 保存する範囲 誰が決めるか
- ② 電子カルテとの連結(データベース化)の可否

(13) 運用管理について

- ① 管理者の指名 管理者の職務と権限 監査 アクセス権者の範囲・指名 アクセス権者の権限の範囲
- ② 基本データセット, 標準用語, コードセット, 用語集  
患者情報, 症状所見, 病名, 検査項目, 処置項目, 薬品名, 画像情報等の標準化
- ③ 国際的な標準規格への準拠

(14) 情報システムの安全管理と法的責任

- ① 法的責任 刑法の医療専門職の守秘義務, 診療契約上の義務, 個人情報保護法上の義務に対する対応としての安全管理責任
- ② 制度上の要求事項  
個人データの漏えい, 滅失・き損の防止その他のデータの安全管理のための従業者の監督, 委託先の監督
- ③ 方針の制定と公表 個人情報保護に関する方針を定め公表する。