クリントン政権、個人の医療情報保護に関する規則を公布

Vol. 5, No. 5　December 20, 2000
Health and Welfare Department
岩屋孝彦（Takahiko Iwaya）
天池麻由美（Mayumi Amaike）

本日、クリントン大統領は、連邦政府としては初めて個人の医療情報を保護するための規則を公布した。1996年に制定された医療保険改革法で医療情報の保護に関する連邦法の制定等が義務づけられ、これまで議会や政府が規制案の作成に取り組んできたが、法律を制定することはできず、４年の歳月を経てようやく連邦保健福祉省規則が公布されることとなった。

ヘルスケア分野では、かつて、個人の医療情報はかかりつけ医によって管理されていたが、マネジドケアの普及により、こうした情報はコンピューターで管理され、医師や病院といった医療提供者と保険会社の間で瞬時に交換されている。効率よく情報が提供されるといった利点がある一方、簡単に個人の情報が漏洩することを心配する声も多い。実際、コンピューターに保存された数千人の患者の情報がハッカーによって引き出された事件も起こっており、個人情報のプライバシー保護を求める声が高まっていた。

連邦保健福祉省の発表によれば、本日公布された規則は、書類や口頭でのやりとりを含む全ての医療情報を保護の対象としており、治療や支払い申請といった一般的な手続きに必要な医療情報の使用（routine use）についても、その都度、患者の同意書が必要とされることとなった。また、その他の主な内容としては、①合意を得ずに個人の医療情報を使用または開示することを制限する、②消費者本人が医療記録を閲覧する権利や、本人以外の誰が当該記録にアクセスしたかを知る権利を保障する、③特別な例を除いて医療情報の開示を必要最低限にとどめるよう規制する、④不適切な医療情報の使用や開示に対して民事罰（civil sanctions）または刑事罰（criminal sanctions）を科す、⑤研究等を目的とする医療情報へのアクセスに関し、新たに規則を設けるといったことが含まれている。

今回は、個人の医療情報の保護に関する規制の状況、議会および政府の規制への取組み、規則の主な内容、関係者の反応についてレポートする。

１．個人情報の保護に関する規制の状況――情報を「知る」権利だけでなく「保護」を求める声が活発に――

個人情報の取扱いに関する連邦法としては、1974年に制定されたFederal Privacy Actが挙げられる。同法は、政府が保有する個人情報を本人が知る権利、当該情報がどのように利用されるのかを本人が知る権利、個人が当該情報を閲覧する権利を有することを前提に、公平な情報の使用について定めたものである。

http://www.jmari.med.or.jp/

Federal Privacy Act の制定から 25 年以上が経過し、人々やヘルスケアシステムを取り巻く環境は変化しており、知る権利だけでなく個人情報の保護を求める声が高まっている。一昔前、カルテに書き込まれた患者の情報はかかりつけ医のオフィスに保存されていたが、マネジドケアの普及により医療の供給体制に変化が起こり、現在では患者の情報はコンピューターで管理され、提携する保険会社、医師、病院等の間で瞬時に情報交換が行われている。コンピューターの導入により情報交換が効率よく行われるようになったという利点があるものの、個人情報の漏洩を懸念する者は少なくない。実際、ワシントン大学病院のコンピューターに保存されていた 5,000 人以上の患者の情報がハッカーによって盗まれたという事件が最近明るみになった[1]。

また、今日ではインターネットを利用してヘルスケア分野のサイトにアクセスする消費者も多いが、インターネット上での個人のプライバシーが守られていないとの批判が上がっている。現在、個人情報の保護に関する各ウェブサイトの方針はまちまちであるほか、個人情報の保護に関する方針を打ち出しているものの実際にはきちんと守られていないといった報告がされている[2]。

個人情報の保護に関する連邦法は存在しないため、州法による規制が行われているが、一つのマネジドケア企業が複数の州にまたがってビジネスを展開していることや、コンピューターを使って簡単に州内外で情報交換が行われている現状を考慮すると州法による規制だけでは不十分であり、こうした状況からも連邦レベルでの規制が求められていた。

２．医療保険改革法下での個人情報保護の動き

1996 年 8 月に制定された医療保険改革法（Health Insurance Portability and Accountability Act of 1996: HIPAA）は、医療情報の保護に関し同法の制定から一定期限内に以下のことを実施するよう義務づけている。

- 1 年以内に連邦保健福祉省長官は個人の医療情報の保護に関する提言を議会に提出すること。
- 3 年以内に連邦議会は医療情報の保護に関する法律を成立させること。同期限内に法律が成立しなかった場合、同法の制定から 3 年半以内に保健福祉省が規則を公布すること。

①議会の動向――HIPAA が定めた期限内に個人の医療情報の保護に関する法律を成立できず――

[1] 本年 12 月 1 日付け、Wall Street Journal 紙による。

[2] 本年 2 月、California HealthCare Foundation（カリフォルニア州内の保健医療分野の状況改善やアクセス向上を目指す団体）は、保健医療関連情報を提供する各サイトを対象にプライバシー保護に関する方針の有無や、その遵守状況についての調査結果を発表した。その結果によれば、調査対象となった 21 サイトのうち、19 サイトがプライバシー保護に関する方針を打ち出しているものの、大部分のサイトではプライバシーが十分に保護されていない実態が明らかにされている。特に、複数のサイトに共通する問題として、サイト運営者やバナー広告の広告主が、利用者のアクセス履歴を割り出したり、利用者の個人情報まで引き出すことが可能となっているといったシステム上の問題が指摘されている。

http://www.jmari.med.or.jp/

昨年、「医療情報のプライバシーと保護に関する法律（Medical Information Privacy and Security Act）」が上下院にそれぞれ提出された[3]ものの審議には至らず、HIPAA が定めた 1999 年 8 月 21 日の期限を過ぎた現在も、議会は医療情報の保護に関する法律を成立させていない。

なお、医療情報の保護に関連する最近の議会の動向として、本年 6 月、下院では Medical Financial Privacy Protection Act[4]が提出された。本法案は、支払い機関による患者の健康に関する情報の取扱い等について、患者本人がこうした情報の使用や公開に関する管理が行えるよう消費者の権限を保障する内容となっている。本法案については、共和党議員の支持が少ないことや業界団体が反対を唱えていることから議会での成立は難しいと考えられている。

②連邦保健福祉省の取組み――97 年には医療情報の保護に関する提言を提出。99 年には規則案を公表――

前述の HIPAA に従い、1997 年、Shalala 長官は個人の医療情報の保護に関する提言をまとめ議会に提出した。本提言は 5 項目から成り立っており、その主な内容は以下のとおりである[5]。

- 消費者の権限（Consumer Control）
  消費者本人の医療記録を閲覧する権利、医療に関する記録が誤っていた場合に修正を要求する権利、健康に関する記録の開示について知る権利を保障する。
- 消費者の権利に関する保護（Accountability）
  患者のプライバシー侵害に対して懲罰を科す。（例えば、civil monetary penalties で最高 2 万 5 千ドルの罰則金。侵害の内容いかんでは刑法で罰し、①個人の医療情報を不当に公開もしくは入手した場合、最高 5 万ドルの罰金と 1 年間の懲役、②本人を装って医療情報を入手した場合、最高 10 万ドルの罰金と最高 5 年の懲役、③利益目的等で個人の医療情報を販売もしくは使用した場合、最高 25 万ドルの罰金と最高 10 年の懲役を科す。）
- 公共の利益に関する責務（Public Responsibility）
  公衆衛生の維持、医療に関する研究、医療の質の向上、医療に関する不正行為の取締といった特定の公共の目的・利益に基づいて個人の医療情報が必要とされる場合、本人の同意なしに使用することを認める。
- 情報の流用からの保護（Boundaries）
  個人の医療情報は、特別な例を除いて、治療と医療費の支払目的のみで使用されるべきであり、その他の目的（例：雇用、解雇、昇進に関する判断材料）に用いられてはならない。また、生命保険の契約にあたりこうした情報が使用されてはならない。

---

[3] H.R.1507、S.573。法案内容については、連邦議会のウェブサイト（http://thomas.loc.gov/）を参照されたい。
[4] H.R.4585。法案内容については、連邦議会のウェブサイト（http://thomas.loc.gov/）を参照されたい。
[5] 本提言については、連邦保健福祉省のウェブサイト（http://www.hhs.gov/news/press/1999pres/991029a.html）を参照されたい。

http://www.jmari.med.or.jp/

・ 情報の保護（Security）
　個人の医療情報の使用を委託された機関は、当該情報が不当に使用されたり開示されないようにしなければならない。

また、個人の医療情報の保護に関する法律が期限内に議会で成立しなかったため、保健福祉省は規則案の作成に取り掛かった。昨年 11 月に公表された規則案の概要は別紙[6]のとおりであるが、その内容は上記の提言に基づいており、消費者本人が医療記録を閲覧する権利や、当該記録の内容が正確でない場合に訂正を要求する権利を保障しているほか、保険会社や医療提供者による個人の医療情報の使用または開示に際しての制限を定めている。

３．公布された規則の主な内容

本日公布された規則の原文は未だインターネット上で公開されていないが、連邦保健福祉省の発表[7]によれば、その主な内容は、①合意を得ずに個人の医療情報を使用または開示することを制限する、②消費者本人が医療記録を閲覧する権利や、本人以外の誰が当該記録にアクセスしたかを知る権利を保障する、③特別な例を除いて医療情報の開示を必要最低限にとどめるよう規制する、④不適切な医療情報の使用や開示に対して民事罰（civil sanctions）または刑事罰（criminal sanctions）を科す、⑤研究等を目的とする医療情報へのアクセスに関し、新たに規則を設ける、といったものになっている。

２．②の規則案では、電子ファイル化された医療記録や情報の一部が電子形態で保存された文書が対象とされていたが、最終版では、書類や口頭でのやりとりを含む全ての医療情報が対象とされている。また、案の段階では、治療や支払い申請といった一般的な手続きに必要な医療情報の使用（routine use）については患者の同意なく使用を許可するものとされていたが、公布された規則では、こうした使用についても、その都度、患者の同意書が必要とされることとなった。

なお、生命保険会社や従業員向け福利厚生プログラム等による医療情報の使用や再利用について現行法では規制できないため、議会はこうした点について法律を制定する必要があると連邦保健福祉省の Shalala 長官は話している。

４．関係者の反応

米国健康保険協会会長の Charles N. Kahn III 氏は、「保険者と保険会社は、消費者の医療情報が保護されるべきであると強く思っているが、本規則は、煩雑かつコスト負担の大きい規制である。」と話している。一方、プライバシーに関する専門家は、企業への潜在的なコスト負担増よりも、現在、消費者が直面している問題の方がずっと深刻であ

[6] 本年 2 月 17 日、下院歳入委員会の下部機関である保健委員会（Subcommittee on Health）で、患者の医療記録に関するプライバシー保護について証言した連邦保健福祉省の Dr. Margaret A. Hamburg（Assistant Secretary for Planning and Evaluation）の付属資料。規制案の原文については、連邦保健福祉省のウェブサイト（http://aspe.hhs.gov/admnsimp/nprm/pvclist.htm）を参照されたい。
[7] 連邦保健福祉省のウェブサイト（http://www.hhs.gov/news/press/2000pres/20001220.html）を参照されたい。

http://www.jmedj.or.jp/

ると指摘し、うつ病やアルコール中毒等の病歴を雇用主に見つかるのをおそれて、医師に病歴を明らかにしない患者や、治療を勝手に中断してしまう患者が存在していることを問題の例として挙げている。

なお、大統領に選出された Bush 氏は、選挙綱領（campaign platform）で医療情報のプライバシー保護に関する規制の実施を掲げているが、現在のところ本規則に関する反応は示していない。

http://www.imi.med.or.jp/

（別紙）個人の医療情報の保護に関する規則案の概要

Proposed Standards for Privacy of Individually Identifiable Health Information Statutory Requirement

Statutory Requirement

Section 264 of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, enacted August 21, 1996, requires that, if legislation establishing privacy standards is not enacted "by the date that is 36 months after the date of the enactment of this Act, the Secretary of Health and Human Services shall promulgate final regulations containing such standards not later than the date that is 42 months after the date of the enactment of this Act."

The statutory deadline for Congress to enact legislation was August 21, 1999. Absent legislation, HHS has developed its proposed rule.

Overview

The proposed rule would:

- allow health information to be used and shared easily for the treatment and for payment of health care;
- allow health information to be disclosed without an individual's authorization for certain national priority purposes (such as research, public health and oversight), but only under defined circumstances;
- require written authorization for use and disclosure of health information for other purposes, and
- create a set of fair information practices to inform people of how their information is used and disclosed, ensure that they have access to information about them, and require health plans and providers to maintain administrative and physical safeguards to protect the confidentiality of health information and protect against unauthorized access.

Scope

a. Entities covered by the proposed rule

- Health care providers who transmit health information electronically
- Health plans

http://www.imeji.med.or.jp/

- Health care clearinghouses

b. Health information covered by the proposed rule ("Protected health information")

- Protection would start when information becomes electronic, and would stay with the information as long as the information is in the hands of a covered entity.
- Information becomes electronic either by being sent electronically as one of the specified Administrative Simplification transactions or by being maintained in a computer system.
- The paper progeny of electronic information is covered; the information would not lose its protections simply because it is printed out of the computer.
- HIPAA protects the information itself, not the record in which the information appears.
- The information must be "identifiable." If the information has any components that could be used to identify the subject, it would be covered.

General rules

We propose that covered entities be prohibited from using or disclosing health information except: as authorized by the patient, or as explicitly permitted by the regulation. The regulation would permit use and disclosure of health information without authorization for purposes of health care treatment, payment and operations, and for specified national policy activities under conditions tailored for each type of such permitted use or disclosure.

○ The amount of information to be used or disclosed would be restricted to the minimum amount necessary to accomplish the relevant purpose, taking into consideration practical and technological limitations.

- There would be exceptions for situations in which assessment of what is minimally necessary is appropriately made by someone other than the covered entity (e.g., such as when an individual authorizes a use or disclosure of information, or when the disclosure is mandatory under another law).

- We would allow covered entities to rely on requests by certain public agencies in determining the minimum necessary information for certain disclosures.

- Under the principle of minimum necessary use, if an entity consists of several different components, the entity would be required to create barriers between components so that information is not used or shared inappropriately.

http://www.jmaj.med.or.jp/

○ To encourage covered entities to strip identifiers from health information when it is possible to do so, we would permit a covered entity to use and disclose such de-identified information in any way, provided that:

- it does not disclose the key or other mechanism that would enable the information to be re-identified, and

- it has no reason to believe that such use or disclosure will result in the use or disclosure of protected health information (e.g., because the recipient has the means to re-identify the information).

○ We would treat the key to coded identifiers the same as the information to which it pertains. A covered entity could use or disclose a key only as it could use or disclose the underlying information.

○ We would permit covered entities to disclose protected health information to persons they hire to perform functions on their behalf, where such information is needed for that function. These "business partners" would include contractors such as lawyers, auditors, consultants, health care clearinghouses, and billing firms, but not members of the covered entity's workforce.

○ Except where the business partner is providing a treatment consultation or referral, we would require covered entities to enter into contracts with their business partners and would require the contracts to include terms to ensure that the protected health information disclosed to a business partner remains confidential. Business partners would not be permitted to use or disclose protected health information in ways that would not be permitted of the covered entity itself. We use the contract as a tool for protecting information, because the HIPAA does not provide legislative authority for the rule to reach many such business partners directly.

○ The uses and disclosures permitted by this rule would be exactly that -- permitted, not required. For disclosures not compelled by other law, providers and payers would be free to disclose or not, according to their own policies and principles. At the same time, nothing in this rule would provide authority for a covered entity to refuse to make a disclosure mandated by other law.

○ Only two disclosures would be required by this proposed rule: disclosure to the subject individual pursuant to the individual's request to inspect and copy health information about him or her, and certain disclosures for the purposes of enforcing the rule.

http://www.jmari.med.or.jp/

○ Health information covered by the proposed rule generally would remain protected for two years after the death of the subject of the information, subject to certain exceptions.

Disclosures without authorization for health care treatment, payment, and operations

- Covered entities could use and disclose protected health information without authorization for treatment, payment and health care operations. This would include purposes such as quality assurance, utilization review, credentialing, and other activities that are part of ensuring appropriate treatment and payment.

- Individuals generally could ask a covered entity to restrict further use and disclosure of protected health information for treatment, payment, or health care operations, with the exception of uses or disclosures required by law. The covered entity would not be required to agree to such a request, but if the covered entity and the individual agree to a restriction, the covered entity would be bound by the agreement.

Uses and disclosures with individual authorization

- Covered entities could use or disclose protected health information with the individual's authorization for almost any lawful purpose.

- We would prohibit covered entities from conditioning treatment or payment on the individual agreeing to disclose information for other purposes, and require the authorization form to state this prohibition.

- While the provisions of this proposed rule are intended to make authorizations for treatment and payment purposes unnecessary, some States may continue to require them. Generally, this rule would not supersede such State requirements. However:

  ● the rule would impose a new requirement that such State-mandated authorizations must be physically separate from an authorization for other purposes described in this rule.

  ● the authorization would have to meet the rule's requirements for the content of such authorizations (although a state law could require that an authorization

http://dpi.mei.med.or.jp/

contain additional provisions).

- We would require authorizations to specify the information to be disclosed, who would get the information, and when the authorization would expire. If an authorization is sought so that a covered entity may sell or barter the information, the covered entity would have to disclose this fact on the authorization form.
- Use or disclosure of information by the covered entity inconsistent with the authorization would be unlawful.

- Individuals could revoke an authorization.

Permissible uses and disclosures for purposes other than treatment, payment and operations

- Covered entities could use and disclose protected health information without individual authorization for the following national priority activities:

  - Oversight of the health care system, including quality assurance activities;
  - Public health, and in emergencies affecting life or safety;
  - Research;
  - Judicial and administrative proceedings; Law enforcement;
  - To provide information to next-of-kin;
  - For identification of the body of a deceased person, or the cause of death;
  - For government health data systems;
  - For facilities' (hospitals, etc.) directories;
  - To financial institutions, for processing payments for health care; and
  - In other situations where the use or disclosure is mandated by other law, consistent with the requirements of the other law.

- Specific conditions would have to be met in order for the use or disclosure of protected health information to be permitted. These conditions are tailored to the need for each specific category listed above and to the types of organizations involved in such activities.

Individual rights

The proposed rule would provide several basic rights for individuals with respect to protected health information about them. Individuals would have:

http://www.imari.med.or.jp/

- The right to receive a written notice of information practices from health plans and providers. The notice must describe the types of uses and disclosures that the plan or provider would make with health information (not just those uses and disclosures that could lawfully be made). When plans and providers change their information practices, they would also have to update the notice. Plans and providers would be required to follow the information practices specified in their most current notice.

- The right to obtain access to protected health information about them, including a right to inspect and obtain a copy of the information.

- The right to request amendment or correction of protected health information that is inaccurate or incomplete.

- The right to receive an accounting of the instances where protected health information about them has been disclosed by a covered entity for purposes other than treatment, payment, or health care operations (subject to certain time-limited exceptions for disclosures to law enforcement and oversight agencies).

Administrative requirements and policy development and documentation

This proposed rule would require providers and payers to develop and implement basic administrative procedures to protect health information and the rights of individuals with respect to that information.

- Covered entities would be required to maintain documentation of their policies and procedures for complying with the requirements of the proposed rule. The documentation must include a statement of the entity's practices regarding who would have access to protected health information, how that information would be used within the entity, and when that information would or would not be disclosed to other entities.

- Covered entities would be required to have in place administrative systems, appropriate to the nature and scope of their business, that enable them to protect health information in accordance with this rule. Specifically, covered entities would be required to:

  - designate a privacy official;
  - provide privacy training to members of its workforce;
  - implement safeguards to protect health information from intentional or accidental

http://www.jmari.med.or.jp/

misuse;

- provide a means for individuals to lodge complaints about the entity's information practices, and maintain a record of any complaints; and
- develop a system of sanctions for members of the workforce and business partners who violate the entity's policies.

Scalability

We propose privacy standards that covered entities must meet, but leave the detailed policies and procedures for meeting these standards to the discretion of each covered entity.

- We intend that implementation of these standards be flexible and scalable, to account for nature of each covered entity's business, and the covered entity's size and resources. We would require that each covered entity assess its own needs and implement privacy policies appropriate to its information practices and business requirements.
- The preamble to the proposed rule will include examples of how implementation of these standards are scalable.

Preemption

Pursuant to HIPAA, this rule will preempt state laws that are in conflict with the regulatory requirements and that provide less stringent privacy protections, with specified exceptions for certain public health functions and related activities.

Enforcement

- Under HIPAA, the Secretary is granted the authority to impose civil monetary penalties against those covered entities which fail to comply with the requirements of this regulation.

- HIPAA also established criminal penalties for certain wrongful disclosures of protected health information. These penalties are graduated, increasing if the offense is committed under false pretenses, or with intent to sell the information or reap other personal gain.

http://www.jmaj.med.or.jp/

- Civil monetary penalties are capped at $25,000 for each calendar year for each standard that is violated.

What this proposed rule does not do

- The HIPAA limits the application of our proposed rule to the covered entities. It does not provide the authority for the rule to reach many entities that receive health information from these covered entities, so the rule cannot put in place appropriate restrictions on how such recipients of protected health information may use and re-disclose such information.
- Any provider who maintains a solely paper information system cannot be subject to these privacy standards.

- There is no statutory authority for a private right of action for individuals to enforce their privacy rights.

http://www.imari.med.or.jp/