3．5　電子署名

要求 (REQUIREMENT)	実装特性(IMPLEMENTATION FEATURES)	関連する既存規格番号
デジタル署名(デジタル署名が使用される場合、メッセージ完全性、非拒否、ユーザ認証の3つは必須。他はオプション) Digital signature (If digital signature is employed, the following three implementation features must be implemented: Message integrity, Non-repudiation, User authentication. Other implementation features are optional.)	属性を加える能力 Ability to add attributes.	3, 4, 10, 11, 13, 20
	署名能力の連続性 Continuity of signature capability.	3, 4, 11, 13, 14, 18
	副署 Countersignatures.	3, 4, 10, 11, 13, 14, 18
	独立している証明可能性 Independent verifiability	3, 4, 11, 13, 20
	相互運用性 Interoperability.	3, 4, 7, 8, 9, 13, 14, 48
	メッセージ完全性 Message integrity.	3, 4, 10, 11, 13, 14, 18
	複数署名 Multiple Signatures.	3, 4, 10, 11, 13, 20
	非拒否 Non-repudiation.	2, 3, 4, 10, 11, 13, 14, 42,
	移送可能性 Transportability	3, 4, 11, 13, 14, 18
	ユーザ認証 User authentication.	3, 4, 10, 11, 13, 20

3．6　関連する既存規格一覧表

番号は、表3.1から表3.5の関連する既存規格番号で引用されている。

1. ANSI X3.92 Data Encryption Standard
2. ANSI X9.30 Part 1: Public Key Cryptography Using Irreversible Algorithms: Digital Signature Algorithm
3. ANSI X9.30 Part 2: Public Key Cryptography Using Irreversible Algorithms: Secure Hash Algorithm (SHA-1)
4. ANSI X9.31 Reversible Digital Signature Algorithms
5. ANSI X9.45 Enhanced Management Controls Using Digital Signatures and Attribute Certificates
6. ANSI X9.52 Triple DES Modes of Operation
7. ANSI X9.55 Extensions to Public Key Certificates and CRLs
8. ANSI X9.57 Certificate Management

9. ANSI X9.62 Elliptic Curve Digital Signature Algorithm (draft)

10. ANSI X12.58 Security Structures (version 2)

11. ASTM E 1762 Standard Guide for Authentication of Healthcare Information

12. ASTM E 1869 Draft Standard for Confidentiality, Privacy, Access and Data Security Principles

13. ASTM PS 100-97 Standard Specification for Authentication of Healthcare Information Using Digital Signatures

14. ASTM PS 101-97 Security Framework for Healthcare Information

15. ASTM PS 102-97 Standard Guide for Internet and Intranet Security

16. ASTM PS 103-97 Authentication & Authorization Guideline

17. CEN European Pre-Standard

18. FDA Electronic Records-Electronic Signatures-Final Rule

19. FIPS PUB 112 Password Usage

20. FIPS PUB 196 Entity Authentication Using Public Key Cryptography

21. FIPS PUB 46-2 Data Encryption Standard

22. IEEE 802.10: Interoperable LAN/MAN Security (SILS), 1992-1996 (multiple parts)

23. IEEE 802.10c LAN/WAN Security-Key Management

24. IETF ID Combined SSL/PCT Transport Layer Security Protocol

25. IETF ID FTP Authentication Using DSA

26. IETF ID Secure HyperText TP Protocol (S-HTTP)

27. IETF ID SMIME Cert Handling

28. IETF ID SMIME Message Specification

29. IETF RFC 1422 Privacy Enhanced Mail: Part 1: Message Encryption and Authentication Procedures

30. IETF RFC 1424 Privacy Enhanced Mail: Part 2: Certificate-Based Key Management

31. IETF RFC 1423 Privacy Enhanced Mail: Part 3: Algorithms, Modes, and Identifiers

32. ISO/IEC 9798-1: Information Technology - Security Techniques-Entity Authentication Mechanisms - Part 1: General Model

33. ISO/IEC 9798-2: Information Technology - Security Techniques-Entity Authentication

Mechanisms - Part 2: Entity Authentication Using Asymmetric Techniques

34. ISO/IEC 9798-2: Information Technology - Security Techniques-Entity Authentication Mechanisms - Part 2: Entity Authentication Using Symmetric Techniques

35. ISO/IEC 10164-4 Information Technology - Open Systems Connection - System Management: Alarm Reporting Function

36. ISO/IEC 10164-5 Information Technology - Open Systems Connection - System Management: Event Report Management Function

37. ISO/IEC 10164-7 Information Technology - Open Systems Connection - System Management: Security Alarm Reporting Function

38. ISO/IEC 10164-8 Information Technology - Open Systems Connection - System Management: Security Audit Trail Function

39. ISO/IEC 10164-9 Information Technology - Open Systems Connection - System Management: Objects and Attributes for Access Control

40. ISO/IEC 10181-2 Information Technology - Security Frameworks in Open Systems - Authentication Framework

41. ISO/IEC 10181-3 Information Technology - Security Frameworks in Open Systems - Access Control Framework

42. ISO/IEC 10181-4 Information Technology - Security Frameworks in Open Systems - Non-repudiation Framework

43. ISO/IEC 10181-5 Information Technology - Security Frameworks in Open Systems - Confidentiality Framework

44. ISO/IEC 10181-7 Information Technology - Security Frameworks in Open Systems - Security Audit Framework

45. ISO/IEC 10736 Information Technology - Telecommunications and Information Exchange Between Systems - Transport Layer Security Protocol (TLSP)

46. ISO/IEC 11577 Information Technology - Telecommunications and Information Exchange Between Systems - Network Layer Security Protocol (NLSP)

47. NIST Generally Accepted Principles and Practices for Secure Information Technology Systems

48. NIST MISPC Minimum Interoperability Specification for PKI Components Version 1

49. PKCS #7 Cryptographic Message Syntax Standard Version 1.5 or later

50. PKCS #11 Cryptoki B A Cryptographic Token Interface

51. RFC 1510 Kerberos Authentication Service

52. RFC 2104 HMAC:Keyed-Hashing for Message Authentication

53. For the Record - Protecting Electronic Health Information

54. ANSI X9.42 Management of Symmetric Keys Using Diffie-Hellman

55. ANSI X9.44 Key Transport Using RSA

以上

E.結論

米国で成立したＨＩＰＡＡ法の背景を述べると共に、その個人情報保護ガイドラインの中の個人の同意を得ないで情報が利用・開示できるとした部分について考察を加えた。

平成１２年度厚生科学研究補助金（特別研究事業）

分担研究報告書

個人情報保護法に関する研究

分担研究者　　桐生康生（(財）医療情報システム開発センター）

研究要旨　　本研究では、現在、国会に提出されている個人情報保護法案について医療機関の視点から概要をまとめるとともに、その検討課題等を整理した。

本法の医療分野への適用を想定した場合に、利用目的をどの程度まで詳細にするべきか等多くの混乱を招く恐れがあり、法律では明確にされていない詳細な事項等について検討する必要がある。

A．研究目的および方法

現在、個人情報保護法案が提出されている。患者の個人情報を扱う医療機関においては、個人情報保護法の成立により、どのような対応をしなければならないかが大きな関心事となっている。

本研究では、個人情報保護法について、医療分野、特に医療機関の視点から概要をまとめ、医療分野における本法適用時の検討課題、問題点等を整理した。

B．研究結果および考察

1　個人情報保護法の概要

1－1　特徴・留意事項

ここでは本法を理解するうえで重要な視点等について述べる。

（1）一般法

本法は、個人情報保護に関する一般法（通則法）であり、特定の分野・領域を対象とした法律ではない。個別の分野・領域について法律（個別法）が必要か否かは国が定める予定の基本指針（第１２条）で定められることになると考えられるが、医療分野について個別法が定められるか否かは 2001 年４月現在明らかになっていない。

（2）情報を視点としたルール

従来は職種ごとに守秘義務の規定があったが、本法では職種を問わず「個人情報」に関してその取り扱いのルールを定めたものである（例：医師（刑法、医師法））。

もちろん、従来の職種ごとに守秘義務は今後も適用される。

（3）自己情報のコントロール権

法律には明記されていないが、個人情報はその本人にコントロール権があるとする自己情報のコントロール権の考えに基づいて定められている。コントロール権により、本人からの情報開示、訂正、利用停止等の要求が導かれる。

（4）個人情報の範囲

本法では、「個人情報」を「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等により特定の個人を識別することができるもの（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。）」とされている（第２条第１項）。

従って、既に死亡した者の情報は本法の保護対象外である。

（5）利用目的

個人情報を扱う上で利用目的を重視している。そして、利用目的に応じて、利用目的の公表、本人への通知、本人の同意等が必要とされている。

（6）本人への情報開示

(1) 生命、身体、財産等の侵害の恐れのある場合、(2) 業務の適正な実施に著しい支障を及ぼす恐れのある場合等を除き、本人の要求に応じて個人情報を開示する義務が定められている（第

３０条)。

これにより、従来から問題となっていたカルテ開示に関して、開示が義務づけられたことになる。ただし、死亡した患者のカルテの開示は本法律の対象外である。

（７）個人情報取扱事業者

個人情報を取扱う者のうち国、地方公共団体、小規模事業者、個人等を除く者を「個人情報取扱事業者」と定義（第２条）し、その守るべき義務等（第２０条から４１条、４７条、４８条）を定めている。多くの医療機関は個人情報取り扱い業者に該当すると考えられる。

（８）認定個人情報保護団体

個人情報取扱事業者の個人情報の適正な取扱いの確保を目的として、本人からの苦情の処理や事業者への情報提供等の業務を行う団体として「認定個人情報保護団体」を設けている。

（９）罰則規定

違反者に対する罰則規定が設けられた（第６１条から６４条)。

（１０）国の基本指針

本法に基づき、国は基本指針を策定することになっている（第１２条)。その内容は、(1) 施策の推進に関する基本的な方向、(2) 国が講ずべき措置、(3) 地方公共団体が講ずべき措置、(4) 独立行政法人および特殊法人が講ずべき措置、(5) 個人情報保護取扱事業者および認定個人情報保護団体が講ずべき措置、(6) 苦情の円滑な処理に関すること等を定めることとなっているが（第１２条)、2001 年４月現在具体的な内容は明らかになっていない。

１－２各章の概要

本法は、７章と附則から構成されている。各章の概要は以下の通りである。

（１）第１章　総則

この章では、この法律の目的と定義が書かれている。目的は前述した通りである。定義に関しては「個人情報」「個人情報データベース等」「個人情報取扱事業者」「個人データ」「保有個人データ」「本人」について定められている（第２条)。なお、「認定個人情報保護団体」については第４５条で定められている。

（２）第２章　基本原則

この章では、個人情報を取り扱う上での５つの基本原則を定めている。基本原則は、「利用目的による制限（第４条)」「適正な取得（第５条)」「正確性の確保（第６条)」「安全性の確保（第７条)」「透明性の確保（第８条)」である。

（３）第３章　国及び地方公共団体の責務等

この章には、国及び地方公共団体の責務が書かれている。国は、総合的な施策を策定・実施し、また、必要な法制上の措置等をとる責務がある（第９条、１１条)。地方公共団体は、必要な施策の策定・実施する責務がある（１０条)。

（４）第４章　個人情報保護に関する施策等

この章には、第３章の国、地方公共団体の責務を踏まえ、国および地方公共団体が行うべき施策等が書かれている。具体的には、国の施策については、個人情報の保護に関する基本指針を策定（第１２条)、(2) 地方公共団体等への支援（第１３条)、(3) 苦情処理のための措置（第１４条)、(4) 個人情報の適正な取扱いを確保するための措置（第１５条）を定めている。地方公共団体の施策については、苦情処理のあっせん等（第１８条）必要な措置を講ずることとされている。

（５）第５章　個人情報取扱事業者の義務等

この章には、個人情報取扱事業者の義務（第２０条から第４１条）および認定個人情報保護団体（第４２条から第５４条）について定められている。これらの詳細は後述する。

個人情報取扱事業者には、(1) 利用目的の特定、(2) 利用目的の公表、本人への通知、本人の同意等、(3) 情報セキュリティ対策、(4) 従業者、外部委託者の監督、(5) 第３者への情報提供の制限、(6) 本人からの開示、訂正、利用停止等の要求への対応、(7) 苦情処理、(8) 個人情報の取扱いに関する国への報告等が義務づけられる。

（７）第６章　雑則

この章には、第５章の義務規定の除外規定（第５５条)、国の事務の代行（第５７条)、大臣の権限の委任（第５７条)、施行状況の公表（第５８条）等が定められている。

除外規定のうち医療分野で特に重要なのは、大学等の学術研究機関が学術研究目的で個人情報を取り扱う場合は第５章の義務規定が除外さ

れることである（第５５条第２号）。

（７）第７条　罰則

この章には罰則が定められている。医療機関の視点から見ると、国からの是正命令に従わなかった場合（第３９条第２、３項）および国への報告が不適切な場合（第３７条）に対して罰則（第６１、６２条）が科されることになる。

（８）附則

附則では、法律の施行日、経過措置等が定められている。

２　今後の検討事項等

本法が医療分野に適用された場合を想定すると以下のような検討事項が考えられる。

２－１　どの程度の規模の医療機関が個人情報保護取扱事業者（第２条第３項）に該当するか

小規模（取り扱う情報量が少ない）医療機関は個人情報保護取扱事業者から除外されるとされている（第２条第３項）が、どの程度の規模か明らかになっていない。また、患者情報の中には家族歴も含まれることから１カルテ１個人情報とは限らないため、情報量の正確な算定は困難である。

２－２　どの程度までが個人情報の範囲か（第２条第１項）

本法の個人情報の定義は「氏名、生年月日その他の記述等により特定の個人を識別することができるもの」とされているが、氏名、生年月日以外にどのような項目が該当すると考えれば良いか。また、組織片等から遺伝情報が入手可能であることを考えると組織片等も個人情報として扱うべきか。

２－３　利用目的にはどのようなものがあるか、また、どの程度詳細に特定しなければならないか（第２０条）

２－４　安全管理（第２５条）とは具体的にはどのような措置を講ずれば良いか

２－５　どの程度の利用目的が「利用目的が明らか」に該当するか（第２３条４２項４号）

患者情報は、診療目的に利用するのは明らかであると思われるが、どこまでが診療目的の利用かは不明確である。

２－６　従業者、委託先への監督は何をどのようにどの程度行うべきか（第２６，２７条）

２－７　「本人が容易に知り得る状態」（第２８条２項、２８条４項３号）とはどういういう状態か、また、「本人が知り得る状態」（第２９条）とどう異なるか

２－８　利用目的の「公表」「あらかじめ公表」（第２３条）とはどのように行うのか、また、両者はどう異なるか

２－９　目的外利用（第２１条）とはどの程度のことが該当するか

２－１０　開示／非開示（第３０条）、利用目的の通知／非通知（第２９条）等について何を判断基準にすれば良いか

２－１１　家族からの開示要求等代理人からの要求（第３４条第３項）はどのように政令で定められるか

代理人の条件、手続き、本人の同意等まで詳細に政令で定められるのか。特に、小児、高齢、意識障害者等本人の同意が得られない場合に関しても一定の方針が出されるのか。

２－１２　苦情処理の体制整備や処理方法（第３６条）はどのようにすれば良いか

２－１３　第５５条の除外規定（学術研究機関における学術研究目的の利用）の範囲はどの程度か

２－１４　行政目的の範囲はどの程度か（第２１条３項４号）

医療機関は、行政から患者情報の提供を求められる場合があるが、医療機関からはそれらが法令に定められているものか否かが明確にはわからない。どの程度まで提供要求の根拠を確認して、どのような判断基準で提供の要否を判断すれば良いか。

２－１５　開示の方法はどのように政令で定められるか（第３０条）

以上のように、個人情報保護法を現在の診療の現場にそのまま適用した場合には多くの混乱を招く恐れがあり、医療現場に即した詳細な事項の検討等が必要である。

Ｃ．健康危険情報

特になし

D．研究発表／知的財産権の出願等

特になし

平成１２年度厚生科学研究費補助金（特別研究事業）

分担研究報告書

医療機関における個人情報保護のためのガイドライン

分担研究者　　山本隆一（大阪医科大学医療情報部）

研究要旨　　日本における診療の場面における個人情報保護のガイドラインを現在国会に上程中の個人情報保護法案との関連を考慮しつつ作成した。これは、今後のガイドラインのための一つの資料とされるべきもので、まだ完成されたガイドラインではない。

A.研究目的

本研究の目的は、ＨＩＰＡＡ法なども参考にしつつ、現在国会上程中の個人情報保護法との関連で、日本における診療に関連した個人情報保護ガイドラインを検討することを目的としている。

B.研究方法

ＨＩＰＰＡ法などを参考にしつつ、個人情報保護法の条文と現在の医療の実際の場面との対応を考慮した。

C.研究結果及びD.考察

以下にガイドラインの骨格を示すが、これは今後の議論の一つの材料となるべきものであり、最終のガイドラインではない。

１）はじめに

診療において個人情報保護が重要なことは当然であり、これまでも関係者の間では十分に配慮されてきた。しかしこのたび個人情報保護に関する法律が制定されようとしており、医療以外の分野でも個人情報保護への関心は高まりつつある。また現代の医療は患者を中心として直接受診している医療機関内の多くの職種の人が協力して行われることが一般的であり、さらに当該医療機関外の機関や人の協力も日常的に行われている。さらに医療の基礎である医学研究や公益的な目的で実施される調査なども直接患者情報を扱う場合があり、個人情報保護に関しては適切な配慮が極めて重要である。

一方で診療情報の電子化は医療のコスト・パフォーマンスを上げるために必須であり、近年急速に進行している。電子化の利益は経済的な効果だけではなく、個人の健康歴の一貫的で有機的な管理や、すばやい疫学的調査が可能になり、患者本人および国民の公益に資するところが大きく、今後ますます発展していくことは確実視されている。電子化の利点は主に情報の可用性の向上に由来するが、可用性の飛躍的な向上に伴って従来にはない、個人情報保護への配慮も求められる。

これまで診療における個人情報保護は医療専門職の身分法にある守秘義務や、世界医師会、日本医師会などが制定した倫理綱領を基礎に医療従事者および医療機関の責任で守られてきた。しかし、前述した個人情報保護の法制化や診療情報の電子化に加えて、医療の透明性が求められているところであり、この機会に診療における個人情報保護ガイドラインを作成し、公表することは意味が大きいと考えられる。

２）対象範囲

本ガイドラインは個人情報保護に関する法律と既存の医療職関連法規を基礎に作成した。自治体には独自の個人情報保護条例を制定しているところもあるが、それらは勘案していない。また個人情報保護に関する法律では国および公共機関と独立行政法人は対象外となっているが、このガイドラインでは区別していない。またガ

イドラインの一部は医療機関だけではなく、医療機関と業務協力関係にある一般の企業・機関も対象としている。

なお、個人情報保護に関する法律では第５５条で適用除外事業者として、「大学その他の学術研究を目的とする機関若しくは団体又はそれらに属する者　学術研究の用に供する目的」を挙げている。大学病院は大学の組織であり、事業者としてはこれに相当するが、適用を除外されるためには、扱う情報が専ら、学術研究の用に供する目的でなくてはならない。大学病院でも通常の診療情報は専ら、学術研究の用に供する目的のために取得されるとは言いがたく、この法律の適用になる可能性が高い。また専ら、学術研究の用に供する目的で取得された場合でも、個人情報保護に努め、苦情処理など、個人情報保護に必要な措置を自ら講じることが求められている。したがって本ガイドラインに従った運用が求められる。

3）無名化

診療情報は当該個人の健康の回復や維持など自明の利用目的以外に、学術研究や教育およびその他の公益目的に利用されており、これは国民の健康や福祉の改善に重要な役割を果たしている。個人情報保護に関する法律でも真に公益的な利用は可及的に合意を得る努力をすることを前提に原則として許されている。しかしたとえ真に公益的な利用目的であっても不用意に個人情報保護の理念に反した利用は慎まなければならないことも自明である。公益的利用に用いる場合でも、個人が識別できる情報を用いるのはやむを得ない場合に限定するべきで、可能な限り個人識別情報を排除して無名化するべきである。紙の診療録のように情報の分離が困難な場合、無名化は困難であるが、電子化された場合は適切に設計されていれば比較的容易にできる場合が多い。無名化された情報は扱いも容易であり、システムの設計も含めてこのような点に配慮すべきであろう。

4）同意を得ることが困難な診療情報

医療機関では死者やすでに通院を中止しているなど、個々に同意を得ることが困難な診療情報が利用されることがある。診療報酬請求、診断書発行、監査、教育、研究などの利用目的が考えられる。このような利用に関しては可能な限り事前に同意を得ておくべきであるが、それが不可能な場合は外部の人を含めた倫理委員会などで了承を得ることが必要である。

ガイドライン

1）用語

個人情報とは個人が容易に識別できる一体の情報であり、他の情報と照合することで容易に個人が識別できる場合を含んでいる。例えば患者 ID と検査項目名、検査値だけが記録された情報は、患者 ID と患者本人を結びつける情報がない場合は個人情報ではないが、ID と患者本人を結びつける情報が入手可能な場合は個人情報として扱わなければならない。診療現場では患者から発生したか、患者に関連する**診療情報**はすべて個人情報として扱う必要がある。

個人情報データベースとは個人情報の集積で検索可能なものを指す。個人情報保護に関する法律ではコンピュータの使用を前提とした一般的なデータベース以外に手作業で検索可能なものも含むとしており、診療現場では**紙のカルテ**や**各種伝票**、**帳票**、**報告書**なども含まれると考えられる。

個人情報取扱い業者とは個人情報データベースを扱う業者であり、すべての**医療機関**はこれに相当すると考えられる。

提携事業者とは医療機関ではなくて、医療機関が個人情報を含む診療情報を業務上で提供または交換する事業者。例えば検査会社や診療報酬算定業者など。

2）体制

医療機関は個人情報保護を達成するための体制を整備するべきである。大規模な医療機関では院内に個人情報保護責任者と苦情処理担当者を設置し、次章のポリシーおよび運用規程に明記すべきである。小規模な医療機関では個人情報保護を目的とする民間団体の対象事業者となり、その作成する指針に従うべきである。

3）ポリシーと運用規程

医療機関は個人情報保護に対する理念と後述する利用目的を含む情報の扱いの概要や苦情処理の方法などの基本方針をさだめて個人情報保護に関するポリシーとして文書化し公開すべきである。この場合公開とは受診患者ならびに受診しようとする患者にとって容易にアクセスできることを意味し、例えば院内のよく見えるところに掲示し、パンフレットを用意するなどを指す。またポリシーに従って診療情報の運用規程を定め、要求に応じて開示すべきである。

4）医療機関における個人情報保護の細目

4－1．利用目的の明確化と通知

医療機関は診療情報の利用目的を明確にしなければならない。また当該本人にとって自明でない利用目的は容易に当該本人が認識できる方法で通知しなければならない。誰でも見ることができ、なおかつ注意を引き易い場所に掲示するか、個々に説明文書を渡すなどの方法をとる必要がある。

一般に医療機関では下記のような利用目的が考えられる。A、B、Cは医療機関で情報を取得する場合自明の利用目的であり、通知しなくてもかまわない。またD．の法令で定められた利用に関しては通知しなくてもかまわない。

A．　当該本人の健康回復および健康維持。
B．　診療報酬請求の作成のための利用。
C．　病院管理などの医療機関の健全な運用のための利用
D．　法令で定められた届け出などのための利用
E．　医学生、研修医などの教育のための利用
F．　臨床医学研究および疫学的研究のための利用
G．　各種監査における利用

利用目的を変更した場合は本人に通知するか公表しなければならない。ただし、国の機関又は地方公共団体が法令の定める事務を遂行することに対して協力する必要がある場合であって、利用目的を本人に通知し、又は公表することにより当該事務の遂行に支障を及ぼすおそれがあるときを除く。

4－2．目的外利用の制限

個別に本人に同意を得ることなく、診療情報の目的外利用はしてはならない。ただし以下の場合を除く。

A．　法令に基づく場合
B．　人の生命、身体または財産の保護のために必要がある場合で、本人の同意を得ることが困難なとき
C．　公衆衛生の向上又は児童の健全な育成のために必要がある場合で、本人の同意を得ることが困難なとき
D．　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

4－3．適正な取得

ポリシーの掲示だけでなく、可能な限り説明し同意を得て情報を収集するべきである。意識障害などで同意を得られない場合は、その事情を客観的に診療録に記述する。また未成年者で本人が説明を理解する能力がない場合は親権者または法的な後見人に説明し同意を得ることに勤めなければならない。

4－4．正確性の確保

診療データの多くはある時点の情報であり、経時的に変化する場合、その時点でのあらたな情報が発生する。このような情報の正確性を確保するために、一般的な精度管理に勤めなければならない。また例えば病名のような持続する状態を示す情報は適切に転帰を記載するなどの状態を正確に保つことにつとめなければならない。

4－5．安全管理と従業者の監督

安全管理は診療情報データベースサーバやカルテ倉庫のような物理的な場所の安全管理と、搬送機やネットワーク上で稼動する連携アプリケーションなどの情報の移転の安全管理、および情報にアクセスする従業員の安全管理からなる。

物理的な場所の安全管理は漏水、浸水、地震などによる情報の破損に備える必要がある。可

能であれば地下や１階は避け、２階以上で保管するべきである。やむを得ない場合は十分な防水対策等を施す必要がある。また入退出管理は必須であり、操作記録も備える必要がある。また必要に応じて記録やデータを管理場所から持ち出す場合は運用上自明の場合を除き、所在を明らかにする必要がある。

情報の移転の安全管理は紙の媒体の場合、落下を防止し、また容易に第３者が診療情報を観察できるような形態で移転してはならない。診察室などでも現に診察中の患者以外の診療情報が容易に観察できるような形で放置してはならない。ローカルエリアネットワークを用いている場合は、ネットワーク接続機器を正しく管理するとともに、不正なアプリケーションやライブラリを動作させてはならない。

従業員の安全管理は正確に利用者登録を行い、利用者認証を徹底し、アクセス管理をただしく行うことからなる。またシステムとしてのアクセス管理だけで効率的な運用と安全確保の両立は難しく、運用規程をさだめ遵守することと監査が重要である。

４－６．提携業者の監督

提携業者に診療情報を提供する必要がある場合は、あらかじめ当該本人にその旨を掲示したポリシー内などで告知しておくこと必要がある。さもなければ提携業者とはみなされない。

提携業者が当該医療機関と同等以上の個人情報保護対策を講じていることを確認し、その旨を明記した契約を行う必要がある。契約後も適切な監督を行う必要があり、定期的に報告を求めるか、監査することが望ましい。

４－７．第三者提供の制限

第三者への診療情報の提供はポリシーでの掲示などで周知をはかった公益的目的以外は原則として、してはならない。ただし以下の場合を除く。

Ａ．　法令に基づく場合

Ｂ．　人の生命、身体または財産の保護のために必要がある場合で、本人の同意を得ることが困難なとき

Ｃ．　公衆衛生の向上又は児童の健全な育成のために必要がある場合で、本人の同意を得ることが困難なとき

Ｄ．　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

個人識別不可能な情報は対象外であるが、識別不可能であることを厳格に確認する必要がある。医療機関や保健機関であつかう情報は住所や年齢など偏りが大きいものもあり、一見個人識別につながらない情報でも相当程度に限定できる場合がある。また項目の組み合わせで強く限定できる場合があることに留意しなくてはならない。

本人の同意を得ており、本人の求めによって中止でき、以下の事項を本人が承知している場合は第三者に提供可能である。

Ａ．　第三者への提供を利用目的とすること。

Ｂ．　第三者に提供される個人データの項目

Ｃ．　第三者への提供の手段または方法

Ｄ．　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

各種保険の診断書などが上記の第三者へ提供することができる場合に相当する。なお、死亡診断書のように本人の同意が不可能な場合は、遺族または家族を代表するものが求める場合、および遺族または家族を代表するものの同意を得て提供すべきである。

４－８．開示

本人から、診療情報の開示を求められたときは、別に政令で定める方法で遅滞なく診療情報を開示しなければならない。ただし以下の場合を除く。

Ａ．　本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

Ｂ．　当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合

Ｃ．　他の法令に違反することとなる場合

以上の理由により開示しないことを決定した場合は、遅滞なく本人にその趣旨を伝えなければならない。また開示しない理由を明らかにするようにつとめなければならない。

医療機関は開示を請求するための手続きを定めることができる。手続きを定めた場合、開示を請求するものはこの手続きに従って請求しなければならない。開示を請求する手続きは請求者に過度の負担をかけるものであってはならない。また開示に必要な手数料を定めることができるが、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

開示請求は政令で定める代理人によってもおこなうことができる。

４－９．訂正等

本人から当該本人の診療情報が事実出ないという理由で理由によって訂正（削除および追加を含む）があった場合は利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有診療情報の内容の訂正等を行わなければならない。ただし診療情報の多くは客観的な情報であり、このような情報は本人の求めであっても根拠なく変更してはならない。訂正を行った場合は訂正の履歴が確認できるように訂正を行ったこと自体を記録するとともに、その理由も記録することがのぞましい。また訂正の事実と内容、訂正を行わなかった場合はその趣旨を本人に通知しなければならない。訂正をおこなわなかった場合にはその理由を明らかにするようにつとめなければならない。

４－１０．利用の停止

診療情報が個人情報保護に関する法律の理念に違反して取り扱われているという理由で本人から診療情報の利用の停止を要求された場合で、その求めに理由があることが判明し、本人および第三者の生命、身体、財産を害する恐れのない場合は、違反を是正するために必要な限度で、遅滞なく、当該診療情報の利用停止等を行わなければならない。ただし、当該診療情報の利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

利用の停止を行った場合、および利用の停止を行わなかった場合は本人に遅滞なく通知し、利用の停止をおこなわなかった場合には理由を明らかにすることにつとめなければならない。

４－１１．苦情の処理

医療機関は個人情報保護に関しての苦情の適切かつ迅速な処理に努めなければならない。またそのために担当者を明確にし、窓口を設けるなどの体制を整備しなければならない。

５）認定個人情報保護団体

個人情報保護に関する法律では個人情報保護団体が主務大臣の認可を受けて、苦情の処理、対象事業者への個人情報保護に関する情報の提供、指針の作成などを行うことができる。小規模な医療機関で苦情の処理などを行うことが困難な場合は個人情報保護団体の対象業者となることで、負担を軽減することができる。

E.結論

日本における医療の現場におけるガイドラインの案を作成した。

研究成果の刊行に関する一覧表

書籍

著者氏名	論文タイトル名	書籍前提の編集者名	書　籍　名	出版社名	出版地	出版年	ページ

雑誌

発表者氏名	論文タイトル名	発表誌名	巻　名	ページ	出版年