

- 個人情報の安全管理のために、リスクの発生を予防するための措置等に関する事項（例えば「情報システム安全対策基準」「コンピュータウイルス対策基準」「コンピュータ不正アクセス対策基準」等を参考とする）

- h) 内部規程が従業員を拘束するに足りる一定の手続き
- i) 規程の制定・改廃、承認、周知等に関する事項
- j) 個人情報の各種管理記録（善管注意義務を果たしていることの証跡）等の文書管理

（2）内部規程の定期的見直し

医療機関は、事業の内容に応じて、内部規程の見直しを適宜実施すること。

（3）内部規程の体系

規程体系の一例を付録4に示す。規程体系は規模と組織形態により、部門ごとに作成し、その中で別途定めた共通事項の引用及びその部門での特殊事情を勘案した規定を加味する方法が適している場合もある。また、必要により詳細規程中に、より具体的な運用をさらに記述したマニュアル（手順書）が引用されることが望ましい。

4. 3. 4 計画書

A. JIS Q 15001 の要求事項

事業者は、内部規程を遵守するために必要な教育、監査などの計画を立案し、文書化し、かつ、維持しなければならない。

B. 医療機関としての解釈

（1）計画書の作成

個人情報を保護するためには、内部規程を遵守して従業員に行動させるための教育が不可欠である。また、内部規程どおりに運用を実施しているかをチェックするための監査が必要である。教育や監査などを効果的かつ効率的に実施するためには、計画書を策定する必要がある。教育の計画書を策定するためには、教育担当部署（担当者）が計画書を立案し、個人情報保護管理者の承認を得る必要がある。監査の計画書を策定するためには、監査責任者が計画書を立案し、代表者の承認を得る必要がある。

教育及び監査の規程の中で、計画項目を定めておくか、書式を定めておき、その内容を埋めることで必要な項目が充当されるような仕組みを取る必要がある。

実施計画書、改善報告書も合わせて決めておく必要がある。

a) 教育計画書に必要な項目

- 年間カリキュラム
- 研修の名称
- 開催日時
- 場所

- 講師
- 受講対象者及び予定参加者数
- 研修の概要
- 使用テキスト
- 任意参加か否かの別
- 予算

b) 監査計画書に必要な項目

- 監査テーマ
- 監査対象
- 目的
- 範囲
- 手続き
- スケジュール

(2) 他の計画との融合

これらの教育、監査は従来から医療機関で行われてきたものと統合して行って良い。
また、日勤、夜勤、準夜勤など医療機関特有の勤務体系も配慮し教育計画を立てる必要がある。

C. 最低限のガイドライン

最低年1回、事前に教育計画を策定し、内部規程を遵守するための教育を実施すること。

最低年1回、事前に監査計画を策定し、内部規程の遵守状況の確認のための監査を実施すること。

また、その実施記録を残すこと。

D. 推奨されるガイドライン

医療機関の内部で監査の独立性が確保できない場合は、外部に委託することを検討すること。

4. 4 実施及び運用

4. 4. 1 体制及び責任

A. JIS Q 15001 の要求事項

コンプライアンス・プログラムを効果的に実施するために役割、責任及び権限を定め、文書化し、かつ、個人情報に関連のある業務にかかわる役員及び従業員に周知しなければならない。

事業の代表者は、コンプライアンス・プログラムの実施及び管理に不可欠な資源を用意しなければならない。

事業の代表者は、この規格の内容を理解し実践する能力のある管理者を事業者の内部から指名し、コンプライアンス・プログラムの実施及び運用に関する責任及び権限を他の責任にかかわりなく与え、業務を行わせなければならない。

B. 医療機関としての解釈

(1) 個人情報保護管理者

事業の代表者は病院及び診療所の管理者（院長）にあたる。管理者は従業員から個人情報保護管理者を定めなければいけない。個人情報保護管理者は個人情報保護に対して十分な理解を持つ必要があり、法令で守秘義務が定められている職種の従業員などから選任すべきである。個人情報保護管理者は兼任でかまわないが、個人情報保護管理以外の業務の権限と責任とは無関係に個人情報保護に関する権限と責任を与える必要がある。例えば内科医員の一人を個人情報保護管理者に選任した場合、個人情報保護に関する権限や責任は医局長や内科部長の干渉をうけないことを定める必要がある。そして個人情報保護管理者とその権限及び責任をすべての従業員に周知しなければならない。

(2) 個人情報保護に必要な資源

病院または診療所の管理責任者は個人情報保護に必要な資源を用意しなければいけない。資源とは例えば必要要員、個人情報保管庫の鍵や入退室管理のための帳簿、不要になった個人情報を破棄するためのシュレッダーやディスク消去装置などが考えられる。

(3) 倫理委員会の設置

医療機関における個人情報保護は微妙な問題が数多く存在する。このような問題に対処するために可能であれば外部の有識者を含めた倫理委員会を設けるとよいであろう。個人情報保護だけでなく医療には診療上の必要性和倫理に微妙な問題が多く、そのような場面でも倫理委員会は重要である。臓器移植法やヒトゲノムの臨床研究のガイドラインなど、倫理委員会の存在や構成が指定されている法律・規範があるので、倫理委員会を構成する場合は参照するように。また診療所などの小規模な医療機関では単独で倫理委員会を設けるのは困難であるが、例えば地区医師会などで設けるなどの工夫が推奨される。

C. 最低限のガイドライン

医療機関の管理者は従業員のうち、個人情報保護に関して十分な理解を持つものから個人情報保護管理者を選任すること。

医療機関の管理者は個人情報保護管理者が職務を遂行するために必要な資源を整えなければならない。必要な資源は個人情報保護管理者と医療機関の管理責任者が合議の上で決定すること。

個人情報保護管理者はすべての従業員に個人情報保護に関する理念の理解と内部規程の遵守を求めること。個人情報保護管理者は従業員が理念を理解し、内部規程を遵守するために、理念及び内部規程の周知を図り、採用時及び年に1度以上は適切な教育を行わな

ればならない。

遵守しない従業員がいた場合、個人情報保護管理者は個別に遵守を求めることができ、それでも遵守しない場合は、医療機関の管理者に遅滞なく報告しなければならない。

従業員の内規の遵守違反及び個人情報保護管理者の義務不履行や不正行為に対して罰則規定を設けること。

D. 推奨されるガイドライン

個人情報保護管理者は法令で守秘義務が定められている職種の従業員から選任すること。

外部の学識経験者を含めた倫理委員会を構成し、個人情報保護と医療の必要性との間で問題が生じた場合に審議すること。倫理委員会についてはこのガイドライン以外にも臓器移植、ヒトゲノムの取扱い、疫学研究などに関するガイドラインやガイドライン案で規定されている。本ガイドラインでは外部の学識経験者を含める以外に特に構成等を規定しないが、他のガイドラインに関係する医療機関にあってはそれぞれのガイドラインでの倫理委員会の規程を満たす必要がある。また他のガイドラインにしたがって構成された倫理委員会であっても、外部の学識経験者が含まれている限り、本ガイドラインで規定する倫理委員会とみなしてよい。

4. 4. 2 個人情報の収集に関する措置

4. 4. 2. 1 収集の原則

A. JIS Q 15001 の要求事項

個人情報の収集は、収集目的を明確に定め、その目的の達成に必要な限度において行わなければならない。

B. 医療機関としての解釈

医療機関での情報収集目的は一義的には当該個人すなわち患者の健康の維持及び回復であるが、そのほかに一般的に以下のものがありうる。このような目的にまったく必要のない情報収集がないことを確認する必要がある。

(1) 患者さんの健康の維持と回復など直接的な利益が目的である場合

- 患者さんの診療や説明
- 患者さんの家族に対する説明
- 他の医療機関へ患者を紹介する場合、または患者の診療にあたって、他の医療機関の医師の意見を照会する場合
- 本人の調剤を現に行っている調剤薬局や本人が受診している他の医療機関からの照会に対する返答

(2) 病院事務あるいは経営上必要な場合

- 診療報酬の請求事務

- 医療機関の経営、運営のための基礎データ
 - 医療機関の上部組織への報告
 - 医療監視や医療指導監査への対応
- (3) 医療の向上への寄与
- 臨床治験
 - 臨床研究のためのデータ収集
 - 医師や看護婦、その他の医療従事者の教育や臨床研修
- (4) 行政上の業務への対応
- がん登録のような公益性の高い疫学調査の実施
 - 厚生労働省等の医療行政等にかかわる統計・調査、サーベイランス事業
 - 保健所など公的機関に対する保健医療及び公衆衛生上の報告
- (5) 保険業務への対応
- 労働者災害補償保険や自賠責の手続きなど
 - 一般の保険会社等からの問合せ
- (6) その他問合せ
- 患者さんの職場、学校等に対する情報提供
 - 警察からの問合せ
 - 裁判所からの問合せ

C. 最低限のガイドライン

コンプライアンス・プログラム作成にあたって診療情報の取得目的の中で、日常的に存在するものはすべて列挙する。そして収集する情報がこれらの目的にだけ使用されていることを定期的を確認すること。また、いずれの目的にも使用されない情報収集が行われていないか定期的を確認すること。これはコンプライアンス・プログラムの監査ではなく、コンプライアンス・プログラムの一環として定期的を確認することを意味している。ただし乳幼児及び小児で親権者による虐待の可能性がある場合はその親権者の同意や了解は必要ない。この場合は当然、法律に基づいて虐待の可能性を報告しなければいけない。

D. 推奨されるガイドライン

コンプライアンス・プログラム作成にあたっては、当該医療機関で過去に診療情報が使用された実績を詳細に調査し、すべて列挙すること。

収集情報を厚生労働省が作成した「電子保存された診療情報を交換するためのデータ項目セット (J-MIX)」のような適切で網羅的な項目セットを用いて項目別に分類し、収集された情報が既知の目的だけに使用されていることを常時確認する。また、いずれの目的にも使用されない不必要な情報収集が行われていないことを常時監視すること。

4. 4. 2. 2 収集方法の制限

A. JIS Q 15001 の要求事項

個人情報の収集は、適法、かつ、公正な手段によって行わなければならない。

B. 医療機関としての解釈

診療情報の収集は原則として当該個人から得られるもので、適法かつ公正と考えられる。しかし、次に列挙するものは適法性、公正性に配慮を必要とする。

- a) 意識障害・精神障害のある患者、乳幼児である患者で、情報を家族から得る場合。
- b) 意識障害・精神障害のある救急搬送患者で、情報を（家族でない）搬送員または当該患者の所持物等から得る場合。
- c) 生活環境に問題がある場合で、近隣の住民及び職場の人等から情報を得る場合。
- d) 検査等で、対象項目外で偶発的に発見した異常値や、測定上同時に得られてしまう値等。
- e) 紹介元や検診結果を問い合わせる場合。
- f) 当該個人から家族歴等の調査の目的で当該個人以外の情報を取得する場合。

これらの場合でも基本的には医療上の必要性が十分あれば、適法かつ公正と考えることができるが、特に上記の b) の所持物の検査などは医療の実施に最低限必要な範囲にとどめなければならない。意識の回復が期待できるが、事務手続きのために名前や住所が必要と言った場合には慎むべきで、緊急に連絡先が必要な場合などに限定することが求められる。f) に関しては個人情報保護の対象となる個人が当該患者以外であり、問題を含んでいる。ただ、家族歴は多くの場合医療の遂行上必須であり、また個々に対象個人の同意を得ることは極めて困難であるので、取得することはやむを得ないが、その扱いには十分な配慮が求められる。

C. 最低限のガイドライン

患者から情報を得る場合、十分な説明を行った上での患者による自発的な提供を原則とし、強要をしてはいけない。

意識不明で搬送された患者の所持物などの捜査は、可能な限り警察等にまかせるべきで、医療の遂行上やむをえない場合をのぞいて行ってはならない。また実施する場合はその必要性を出来る限り速やかに診療録等に記載すること。

当該患者以外の情報を患者から得る場合は、その情報の必要性を十分検討した後に行い、収集された情報の利用は当該患者の診療遂行に必須のものに限定する。

患者以外から当該患者に関する情報を取得する場合も必要性を十分検討した後に行い、可能であれば患者に取得情報の内容と取得状況の説明を行うこと。

意識障害、精神障害、乳幼児などで、説明による同意が困難な場合は、診療の遂行上の必要性を十分検討し、必要性を記録した上で情報の取得を行う。親権者、保護者が定まっ

ている場合はその了承を可能な限り得るようにすること。

D. 推奨されるガイドライン

C. に加えて患者に関するもの以外の情報を患者から得る場合で、対象個人の了承を得られない場合と患者以外から当該患者の情報を得る場合で当該患者の了承を得ることができない場合は、診療遂行上の必要性を複数の従業員が検証を行うこと。

4. 4. 2. 3 情報の収集の禁止

A. JIS Q 15001 の要求事項

次に示す内容を含む個人情報の収集、利用又は提供は行ってはならない。ただし、これらの収集、利用又は提供について、明示的な情報主体の同意、法令に特別の規定がある場合、及び司法手続き上必要不可欠である場合は、この限りでない。

- a) 思想、信条、及び宗教に関する事項。
- b) 人種、民族、門地、本籍地、身体・精神障害、犯罪歴、その他社会的差別の原因となる事項。
- c) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。
- d) 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。
- e) 保健医療及び性生活。

B. 医療機関としての解釈

(1) 診療遂行上からみて限度内の収集であることの確認

本項目は一般的な情報収集と保健医療福祉分野での情報収集でもっとも大きな違いが見られる事項である。人種、民族、身体・精神障害及び保健医療に関する情報収集は診療の遂行に関して必須であり、保健医療福祉分野では特別に扱う必要はないと考えられる。また思想、信条、犯罪歴でさえも精神疾患などでは収集目的の達成のために必要な場合がある。したがってこれらの禁止項目は保健医療福祉分野の場合、取得目的の範囲を超えた場合のみに適用されると考えるべきである。ただしこれらは特に個人情報保護に敏感な項目であるために挙げられたことに十分留意するべきで、これらの項目を収集する場合は特に利用範囲が診療の遂行のための限度内であることを確認する必要がある。

(2) 倫理委員会での方針決定

個人情報保護に敏感で医療の遂行上必要な情報は少なからず存在する。これらの情報収集には慎重でなければならないが、複雑な手続きを規定すると診療の遂行が困難になることもあり得る。このような情報は診療の専門性によってもことなるために一概に判断することは困難である。その医療機関の実態をよく把握し、日常的な情報収集で少しでも曖昧さがある場合はあらかじめ倫理委員会の方針を決めるなどの、説明可能な対策が求められ

る。

(3) 宗教に関する収集の事前通知と拒否

特殊な例として、宗教法人が運営する医療機関などで信者か否かを受診時に確認する場合がある。これも宗教に関する情報収集にあたる。医療面からの必要性は乏しく、安易に収集すれば個人情報保護の侵害にあたる。このような場合は、初診申し込み前に宗教に関する質問があることを通知し、回答を拒否できるようにするべきである。またホスピス等で本人の宗教によってケアが異なる場合のために情報を収集する場合がある。診療上の必要性はあると考えられるが、止むを得ないかどうかは判断が困難である。このような場合にも、事前に通知し、回答を拒否できるようにしておくべきである。

C. 最低限のガイドライン

以下のa～eの項目については、原則として情報を収集してはならない。ただし診療の遂行上情報の収集を避けられない場合はその理由が自明でない限り、その理由を診療録等に明記した上で収集すること。その場合も利用は診療上必要な範囲内にあることに特に注意しなければならない。診療上の理由が自明とは性生活そのものが健康上の問題である場合の性生活に関する情報や、思想、宗教、犯罪歴などが妄想などの精神症状に強く関連している場合であって、安易に自明と判断してはいけない。

- a) 勤労者の団結権、団体交渉及びその他団体行動の行為に関する事項。
- b) 集団示威行為への参加、請願権の行使、及びその他の政治的権利の行使に関する事項。
- c) 思想、信条、及び宗教に関する事項。
- d) 門地、本籍地、犯罪歴、その他社会的差別の原因となる事項。
- e) 性生活。

D. 推奨されるガイドライン

C.に加えてこれらの項目の情報収集を行う場合、診療上の必要性が自明でない場合、可能な限り事前に倫理委員会の了承を得る。事前に倫理委員会に諮ることが出来なかった場合は事後に倫理委員会に報告し、その際、不適と判断された場合は当該情報を抹消する。

例えば不妊外来での性生活に関する情報収集のように診療上の必要性があつて、かつ日常的に収集されることが予想される場合は、あらかじめ一括して倫理委員会等で検討を行い、必要性を明確にし、個人情報保護上の配慮を具体的に定めておく。このような過程を経た情報収集はその必要性と配慮がある前提で、個々に特別な手続きを経ずに収集することができる。

4. 4. 2. 4 情報主体から直接収集する場合の措置

A. JIS Q 15001 の要求事項

情報主体から直接に個人情報を収集する場合には、情報主体に対して、少なくとも、次に示す事項又はそれと同等以上の内容の事項を書面若しくはこれに代わる方法によって通知し、情報主体の同意を得なければならない。

- a) 事業者の内部の個人情報に関する管理者又はその代理人の氏名若しくは職名、及び所属並びに連絡先。
- b) 収集目的。
- c) 個人情報の提供を行うことが予定される場合には、その目的、当該情報の受領者又受領者の 組織の種類、属性及び個人情報の取扱いに関する契約の有無。
- d) 個人情報の預託を行うことが予定される場合には、その旨。
- e) 情報主体が個人情報を与えることの任意性及び当該情報を与えなかった場合に情報主体に生じる結果。
- f) 個人情報の開示を求める権利、及び開示の結果、当該情報が誤っている場合に訂正又は削除を要求する権利の存在、並びに当該権利を行使するための具体的な方法。

B. 医療機関としての解釈

(1) 包括的同意と個別同意

情報主体、すなわち患者から当該患者に関する情報を収集する場合の要求事項であり、それぞれ情報収集を行う前に患者に提示し、同意を得る必要がある。JIS Q 15001 の要求は項目毎の個別の同意か包括的な同意かについて言及はしていない。医療機関の健全な運営も含めて診療の遂行上必要な目的に関しては包括的な同意でよいと考えられるが、教育・研修や医学研究といった診療遂行上の必要性が薄い項目に関しては利用時に個別に同意を得るべきである。

直接診療に用いる場合や、診療報酬請求や病棟管理などの医療機関の経営や管理上の利用は本来目的であり、包括的な同意でよいと考えられるが、お見舞い客の案内に用いる入院名簿に掲載するといった利用目的は利用できなくても診療にも病院の経営・管理にも重大な障害とはならない。このような目的は患者に個別に拒否できるオプションを用意することが必要と考えられる。

(2) 客観的情報の削除・訂正は不可

また客観情報の訂正・削除には注意が必要である。要求されたからといって客観的な事実で診療上必要な事項は変更や削除はできない。

(3) 患者本人に理解能力がない場合の同意

乳幼児や意識障害、精神障害で本人に理解する能力がない場合は可能な限り親権者や保護者の了解または同意を得る必要がある。ただし乳幼児及び小児で親権者による虐待の可能性のある場合はその親権者の同意や了解は必要ない。この場合は当然、法律に基づいて虐待の可能性を報告しなければいけない。