- 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・プラ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に確認すること。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に確認すること。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に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で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って、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。

C．最低限のガイドライン

患者の状態が許す限り、初診時に以下ａ～ｉの項目を記載した文書を手渡すか、見やすいところに掲示し、内容を理解し、同意したことを確認すること。例えば初診申し込み用紙などに同意した趣旨を確認できる記載を行う。

意識障害、精神障害、乳幼児などで、本人に理解能力がない場合で、親権者や保護者が定まっている場合は可能な限り親権者や保護者に提示し同意を得ること。

親権者や保護者が複数いて、意見に相違がある場合は原則として不同意を優先する。ただし、患者や第三者の人命にかかわる場合や、身体に重大な損傷をあたえることが予想される場合は同意を優先してよい。その場合、優先した理由を速やかに診療録等に記載すること。患者が乳幼児及び小児で親権者に虐待の疑いがある場合は虐待のある親権者の同意は必要としない。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。

以下に収集時、患者に通知する内容の留意点を述べる。

ａ）医療機関の個人情報保護管理者の氏名と連絡方法。苦情の連絡先が異なる場合にはそれも記載。

ｂ）４．４．２．１で列挙した取得目的のなかで診療目的及び医療機関の健全な管理のためのものを挙げ、初診時の了解を持って取得及び利用に同意したこととする項目。さらにこれらの項目のうち、特定の目的に限って患者が拒否した場合に利用しないものがある場合はその項目。

ｃ）４．４．２．１で列挙した取得目的のなかで利用時に個別に同意を得るか、同意が得られない場合はその目的で利用しないもの。

ｄ）４．４．２．１で列挙した取得目的の中で法律に基づくもの。

ｅ）４．４．２．１で列挙した取得目的の中で公益性が強く、初診時の了解を持って取得及び利用に同意したこととする項目。さらにこれらの項目のうち、特定の目的に限って患者が拒否した場合に利用しないものがある場合はその項目。

ｆ）外注検査のように契約をおこなった外部機関への情報の提供の有無と個人情報保護に関する契約内容の要約

ｇ）当該医療機関が診療の遂行上、必要と認め、患者が情報の提供または利用を拒否した場合に診療が十分行われない可能性があること。

ｈ）開示を求める方法と費用、及び開示を拒否する場合の理由。訂正を求められた場合に応じる条件。

ｉ）一括して削除を求められた場合に要求に応じない条件。（医師法、医療法、療養担当規則等で規定された保存期間など。）

４．４．２．５　情報主体以外から間接的に収集する場合の措置

A．JIS Q 15001 の要求事項

情報主体以外から間接的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、4.4.2.4 のａ）～ｄ）及びｆ）に示す事項を書面又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。ただし、次に示すいずれかに該当する場合は、この限りではない。

ａ）情報主体からの個人情報の収集時に、あらかじめ自己への情報の提供を予定している旨　4.4.2.4のｅ）に従い情報主体の同意を得ている提供者から収集を行う場合。

ｂ）情報処理を委託するなどのために個人情報を預託される場合。

ｃ）情報主体の保護に値する利益が侵害されるおそれのない収集を行う場合。

Ｂ．医療機関としての解釈

患者の家族、職場や近隣の人々、検診記録、紹介元、ケースワーカ、ソーシャルワーカー、搬送を担当した救急隊員、警察等から情報を得る場合で、原則として当該患者に通知の上で同意を得る必要がある。しかし医療の現場では種々の事情で同意を得ることが難しいことがある。意識障害がある場合や、本人が虚偽を述べている場合などがこれにあたる。このような場合は診療の遂行上の必要性が重要で、これを確認して行わなければならない。

また検査センターで発生する情報も広い意味で患者以外から情報を収集することに相当する。この場合は要求事項の例外のａに相当すると考えられる。すなわちあらかじめ包括的に同意を得ておかなければならない。

Ｃ．最低限のガイドライン

患者本人以外から当該患者の情報を得る場合、原則として事前に本人の同意を得る必要がある。口頭で説明し、同意を確認した上で情報を収集し、事後に収集情報を本人に開示しておくことが求められる。

情報提供者が本人への開示を拒否した場合、診療の遂行上の必要性が大きい場合に限って、その情報を利用することができる。診療の遂行上の必要性がないか、その情報がなくても診療の遂行が可能なほど小さい場合は、直ちにその情報を破棄しなければならない。

意識障害・精神障害・乳幼児等で本人の同意が得ることができない場合、診療の遂行上の必要性を十分検討し、その必要性を診療録等に記載した上で情報の収集を行うこと。緊急事態等で事前の記載が不可能な場合は可及的速やかに事後に記載する。また親権者や保護者が定まっている場合は可能な限り親権者や保護者の同意を得ること。ただし患者が乳幼児または小児で親権者による虐待が疑われる場合は、その親権者の同意は必要ない。

本人が虚偽を申し立てている可能性が強い場合で、診療の遂行上の必要性が高い情報である場合も本人の同意なく情報を収集し利用することができる。この場合も本人が虚偽を申し立てていると判断した理由、及びその情報が診療の遂行上必要である理由を診療録等に記載しなければならない。

D．推奨されるガイドライン

C．に加えて診療の遂行上の必要性、及び本人が虚偽を申し立てていると判断した根拠などを複数の従業員が判定する。

４．４．３　個人情報の利用及び提供に関する措置

４．４．３．１　利用及び提供の原則

A．JIS Q 15001 の要求事項

個人情報の利用及び提供は、情報主体が同意を与えた収集目的の範囲内で行わなければならない。なお、次に示すいずれかに該当する場合は、情報主体の同意を必要としない。 a）法令の規定による場合。 b）情報主体及び・又は公衆の生命、健康、財産などの重大な利益を保護するために必要な場合。

B．医療機関としての解釈

診療情報の利用を原則としてあらかじめ同意を得た範囲に限定するもので、同意は包括的なもの、個別のものがある。例外のａ）の例として、感染症予防法による保健所への報告や児童虐待防止法による報告などがある。ｂ）は緊急避難に相当するものである。

C．最低限のガイドライン

診療情報の利用は原則として事前に同意を得た範囲で行わなければならない。意識障害、精神障害、乳幼児などで同意を得ることが困難な場合は診療遂行上の必要性を検討した上で、必要性を記載し、利用を行うこと。また可能な限り親権者等の同意を得る。ただし患者が乳幼児または小児であって親権者による虐待が疑われる場合は、その親権者の同意は必要としない。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。

情報の利用が法令による場合は同意を必要としない。

患者及び公衆の生命、健康、財産に重大な損害を防止するために利用する場合で、あらかじめ同意を得ることができない場合は同意を必要としない。

D．推奨されるガイドライン

法令による利用であってもその利用を通知しておくことが望ましい。また、緊急避難的利用の場合も、事後にその利用を通知しておくことが望ましい。

４．４．３．２　収集目的の範囲外の利用及び提供の場合の措置

A．JIS Q 15001 の要求事項

情報主体が同意を与えた収集目的の範囲外で個人情報の利用及び提供を行う場合は、少なくとも、4.4.2.4 のａ）～ｄ）及びｆ）に示す事項を書面又はこれに代わる方法によって

情報主体に通知し、事前の情報主体の同意の下に行わなければならない。

Ｂ．医療機関としての解釈

あらかじめ同意を得た範囲外での情報提供を行う場合は、原則、患者の同意を必要とする。ただし診療情報では公益目的及び行政的な目的のために法令に基づいて情報の提供が行われる場合は同意を必要としない。

民間保険会社等の求めに応じて診断書や意見書を作成する場合、学校や職場からの病状問い合わせ、警察等からの問い合わせ、医学教育及び研修への利用、外部評価機関の評価のための診療情報の閲覧などであらかじめ同意を得ていない場合がこの項に相当する。行政機関による医療監視や裁判所の命令による利用、感染症予防法等による情報提供は法令に基づくためにかならずしも同意は必要としない。公益目的による除外は慎重に判断しなければならない。当該個人情報の提供がおこなわれなければ公益を大きく損なう場合だけに限定するべきである。

患者が意識障害、精神障害、乳幼児等で、同意を得られない場合がある。この場合新たに発生した情報提供が診療の遂行上の必要性が高い場合や公益性が高い場合は提供を行うことができると考えるべきである。また親権者、保護者が定まっている場合は可能な限り親権者または保護者の同意を得る必要がある。本人（親権者、保護者を含む）の同意を得ることができなくて、診療の遂行上の必要性がなく公益性も低い場合は予め同意を得た収集目的範囲外での個人情報の提供してはならない。

Ｃ．最低限のガイドライン

あらかじめ同意を得た範囲外で情報提供を行う場合、患者本人の同意を得なければならない。患者本人が意識障害、精神障害、乳幼児等で同意を得ることが困難な場合で親権者や保護者が定まっている場合、親権者や保護者の同意を得なければならない。

本人の生命、健康、財産及び公衆の生命、健康、財産に重要な利益がある場合は同意を得なくてもよい。

４．４．４　個人情報の適正管理義務

４．４．４．１　個人情報の正確性の確保

Ａ．JIS Q 15001 の要求事項

個人情報は、収集目的に応じ必要な範囲内において、正確、かつ、最新の状態で管理しなければならない。

Ｂ．医療機関としての解釈

本条は、4．3．1 で特定された個人情報に関して誤った情報や古い情報によって個人の利益が侵害されることを防ぐため、利用目的に応じて必要な範囲において、正確かつ最新

の状態で管理することを求めるものである。特定された個人情報に関し正確性に対するリスクを認識し、その対策を規程化する。データの誤りは、誤った指示、誤処理、誤操作、機器等の故障等によっても発生するのでその原因を除去することにより防止しなければならない。

（1）入力時のチェック

医療情報システムへの入力時、確定操作前に入力データに誤りがないか、転記ミスがないかを十分チェックする習慣及びチェックできるシステムにする必要がある。

（2）変更の時間的ズレによる正確性の喪失

また、「記録の遅れ」、あるいは「住所・姓名等の変更が迅速に反映されないため」、正確性が喪失される場合がある。

住所変更､保険証区分等の変更や診療録等の記載の訂正に対して誰が変更を行えるのか、またその変更や訂正に対する履歴はどのように管理するのかを規程化する必要がある。

（3）システムによる正確性確保とその検証

医療情報システムは指示書に基づく処理、システムに組込まれたデータの日付や、件数チェック、運用の自動化等により正確性が確保される。また処理結果の確認、実施記録の保管、指示書とオペレーションログの検証等が行われ正確性が検証される。

C．最低限のガイドライン

まず、４．３．１で特定された個人情報に対して各責任部門で正確性に関するリスク分析を行うことを規程化すること。すなわち、正確性をそこなうどのような脅威があるか、その発生確率と発生した場合の重大性を評価し、予防対策及び発生時の対策を立てる。リスク分析及びその対策を誰が何時どのように行うのか規程化すること。本分析はつぎの安全性のリスク分析と同時に行っても良いが分析の視点は正確性と安全性とは分けて行う必要がある。

- 正確性に関する技術的対策は以下の項目をシステムに合せて実施すること。
- 用語・コードのマスターの種別あるいはバージョン管理を適正におこなうこと。
- 患者名により各データの所在管理が確実におこなわれる機構をもつこと。
- 住所変更や保険区分等の変更があった場合に変更が可能でなお変更履歴がのこること。
- 入力の確定操作後は変更が出来ない機構であること。
- 正確性に関する管理規程は、以下の項目を必要に応じ規程化すること。

運用管理　：データ利用、ジョブ処理、ファイル取扱、機器操作等、に関する規定

入出力管理：入力処理、出力処理、本人確認方法、記録事項変更確認方法、誤データ更新方法に関する規定

データ管理：データ保管、バックアップ、廃棄等に関する規定

委託先管理：自施設と同じ管理レベルの正確性の確保を委託先に要求する規定

D．推奨されるガイドライン

論理的にありえない入力を行った時は警告を発生する機能をシステムとして付加することが望ましい。特に正確性を要するデータやインデックスは２重化が望ましい。確実に本人が署名を行ったことの確認が必要な場合は電子署名の手段により、データの正確性をデジタル的に確認できるシステムの導入を推奨する。データの前後関係の必要なデータに対しては証拠性のあるシステムによるタイムスタンプをつける等の時刻管理を行えることが望ましい。

４．４．４．２　個人情報の利用の安全性の確保

A．JIS Q 15001 の要求事項

個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざん及び漏えいなど）に対して合理的な安全対策を講じなければならない。

B．医療機関としての解釈

（1）合理的な安全対策

「合理的」という意味は、脅威が発生した場合の損失や平常時の対策状況に対する社会的評価を配慮して経済的に実行可能な最良の技術及び運用方法の適用に配慮することである。その為に 4．3．1 で特定された個人情報ごとに以下のことを技術的に配慮した医療情報システムの導入及び管理規程の作成、及びそれに基づいた運用が必要である。

（2）リスク顕在化の予防と発生時対策

安全対策は、一つの方法のみで十分というわけではなく、総合的な検討が求められる。安全性の確保に対する対策は漫然と実施するのではなく、4．3．1で特定した個人情報を施設の部門別に特定し、その部門での収集、提供・預託、委託、利用、破棄、処理の各場面で、リスクすなわち脅威と脆弱性を明確に評価し、そのリスクに対するさまざまな予防措置を検討し、その中で医療機関が取り得る最良の措置を講じることにより、そのリスクの顕在化を防止する。脅威としては、故意及び過失や災害等が考えられる。また、内部や外部からのものが考えられる。

また、予防対策おこなったにもかかわらずリスクが顕在化した場合の是正措置も必要である。この場合、顕在化を誰がどのレベルでチェックし、誰に連絡し、誰が対策を行うのか等責任体制の確立が重要である。これにより、リスクが発生しても最低限の損失にとどめることができる。

（3）内部の脅威に対する抑制

一般的に、個人情報の漏えい事例は内部のものによって行われることが多いので医療施設でもその脅威に対する観点も入れた対策が必要である。特に内部のものが安全性を脅か

す誘惑にかられないようにするためにもアクセスログを取っていることや個人認証を行っていることを周知させるような明確な規制が有効である。

（４）一覧機能、検索機能、コピー機能の制限

特に患者データを一覧表として表示できる機能、患者名等から診療データを検索できる機能のアクセス制限や表示データ等のＦＤ等へのコピー制限機能が重要である。また、アクセス可能者が患者同意のとれた範囲で運用できるための機能が必要となる。

（５）紙データや検体の授受を含めた管理

また、コンピュータ内のデータのみでなく記入用紙あるいは出力用プリント・オーダ伝票あるいは診療録等の紙データの閲覧及び移動時の取扱いも管理規程を定め、入退出者を監視したり、第三者に見読されるような不用意な場所への放置や搬送防止策により紛失や第三者への漏えいを防止しなければならない。

また、臨床検査データ等の外部への検査依頼時も検体等の授受やレポートの授受に関しても安全性に対して委託業者も含めた形で管理規程を定めておく必要がある。

（６）個人用コンピュータの管理

医師が個人データを自己の研究用または主治医としての診療の必要からパーソナルコンピュータにデータベース化している場合も禁止するか適正運用管理の為の規程化を行っておく必要がある。

Ｃ．最低限のガイドライン

（１）合理的な技術及び運用対策

個人情報に対する安全性の確保のための技術的及び、運用管理対策を規程化すること。予防対策としては、不正アクセス、紛失、改ざん、及び漏えい等の様々なリスクから安全を確保することである。

まず、４．３．１で特定された個人情報に対して各責任部門で安全性に関するリスク分析を行うことを規程化する。すなわち、安全性を損なうどのような脅威があるか、その発生確率と発生した場合の重大性を評価して対策を立てる。誰がいつどのように行うのかを規程化する。技術的な対策として下記のような対応策が上げられる。適切なものを選択し、規程化すること。

① 不正アクセスへの対応：
- ・アクセス制御
- ・外部からの接続の遮断
- ・アクセスログの取得
- ・アクセスログの定期的チェック機構

② 紛失への対応：
- ・鍵の掛かる場所への保管
- ・鍵の特定者（部門の管理者等）の管理

・授受の記録
・バックアップ

③　改ざんへの対応：
・アクセスの制御
・データ（伝送データを含め）改ざん防止(暗号化等)措置
・アクセスログの取得
・ウイルスチェックの自動化

④　破壊への対応：
・外部からの接続の遮断
・バックアップ
・ウイルスチェック

⑤　漏洩への対応：
・個人情報へのアクセス制御
・鍵の掛かる場所への保管
・鍵の特定者（部門の管理者等）の管理
・データ（伝送データを含め）改ざん防止(暗号化等)措置
・不正ソフトのチェック

また安全性の確保に関する予防対策に対する管理規程項目は、次の通りである。そのシステムにあった適切なものを選択すること。

①　入退管理：
・建物、室への入退制限、チェック、記録の実施規定
・機器及び媒体等の搬出入や授受記録に関する規定、監視人の規定

②　アクセス管理：
・情報システム利用時の権限、識別情報、ID、パスワードの付与、チェック、記録の実施規定
・データへのアクセスに関する規定

③　データ管理：
・データ保管、バックアップ、廃棄等に関する規定・不正ソフトウエア、ウイルスチェック管理に対する規定

④　委託先管理：
・自施設と同じ管理レベルの安全性確保を委託先に要求する規定

（２）廃棄時の安全性

個人情報の漏えい事例には、破棄時の漏えいが多くみられることから、廃棄にあたっても、電子ファイルの場合は２重書き消去、あるいは、個人情報が打ち出された紙の場合は破砕処理あるいは溶解処理などによって、破棄されたデータが他者に流出することのない

よう留意することが必要である。

（3）リスク発生時の是正措置

予防措置を講じていたにもかかわらず、個人情報に対するリスクが顕在化する場合も、可能性としては残されている。そのため、是正措置も予め検討して講じる必要がある。是正措置についても、医療機関が取り得る最善の方法を検討しておかなければならない。なお、是正のための技術的な措置は、前述の予防措置の検討に包含される場合が多く、例えば、アクセスログの取得、バックアップの作成等はこれに当たる。また、漏えい等が起こったときの患者への対応、関係機関、マスコミ等への対応等の規定も必要である。

（4） 電子保存（フィルムレス・ペーパレス）への対応

また､保存義務のある診療録等を電子媒体に保管して保存義務を果たす場合は平成11年4月22日付けの厚生省（当時）3局長連名通知に従って3基準である真正性、見読性、保存性及びその留意事項を満足させなくてはならない。その為には通知に付属したチェックリストを参考にして対策をたてることを推奨する。

D．推奨されるガイドライン

安全性の基準としては、すでに国際的には、国際規格 ISO/IEC17799－2000（Information technology- Code of practice for information security management 情報技術－情報セキュリティマネージメント実施基準）があり、JIS 規格は JIS X 5080 である。この認証のためのシステムとして、(財）日本情報処理開発協会が「情報セキュリティマネジメントシステム適合性評価制度」を実施しており、この評価制度を受けるか、これに準じたマネジメントシステムを構築することが推奨される。

インターネットとの結合がある場合はアクセスログの解析を定期的またはリアルタイムで実施し異常なアクセスがあったときは警告を発生し、ネットワークを切断する機能の付加が望ましい。

不正ソフトウエアを自動的に監視し活性化しない機構を備えることが望ましい。

秘密鍵等のシステム内での保管はハードウエアセキュアモジュールへの格納が望ましい。

４．４．４．３　個人情報の委託処理に関する措置

A．JIS Q 15001 の要求事項

事業者が、情報処理を委託するなどのために個人情報を預託する場合は、十分な個人情報の保護水準を満たしている者を選定する基準を確立しなければならない。また、契約によって、次に示す内容を規定し、その保護水準を担保しなければならない。

B．医療機関としての解釈

医療機関が検査や医事会計の外注を行うことは、当然のこととなってきており、外注に際しての個人情報保護をどうするのかは重要な事項である。

（1）委託先評価基準

まずは、個人情報保護に関する評価基準を明確にする必要がある。もちろん、プライバシーマークを取得している業者が好ましいといえるだろう。しかし、プライバシーマークを有さない業者であっても、個人情報の保護に努めているものもいるので、次のような項目で明確な評価基準が必要になる。

○　就業規則での守秘義務を定めている。
○　退職後も守秘義務を課している。
○　個人情報保護に関する研修教育を行っている。
○　情報システムのセキュリティ仕様を明示でき、その内容が十分である。

（2）委託先との契約書

その上で、いわゆる守秘義務契約を取り交わすことになる。例えば、検査会社等が内部的に検査の較正を行うための数値の利用等まで規制することはできないが、氏名を特定できるような情報を他者に開示したりしないようにしなければならない。また、再委託の制限や禁止等も盛り込む必要がある。

（3）外国人雇用者への契約書等の配慮

また、清掃や廃棄物処理等の業務には、外国人が雇用されるようになってきており、(日本語で書かれている)規則自体が理解できない可能性もある。

（4）入札時の仕様書

公的な医療機関では入札を行うことになるが、実際には他の会社への振り替えが難しい場合もあり、仕様書に明記すれば、費用面での問題が発生することも考えられ、配慮が必要である。

C．最低限のガイドライン

受託者の守秘義務や教育研修義務を明記した仕様書を提示し、再委託時には再々委託を禁じ、同様の契約を結ぶこと。

D．推奨するガイドライン

基本的にプライバシーマーク取得者に対して委託を行うようにする。

４．４．５　個人情報に関する情報主体の権利

４．４．５．１　個人情報に関する権利

A．JIS Q 15001 の要求事項

情報主体から自己の情報について開示を求められた場合は、合理的な期間内にこれに応じなければならない。また、開示の結果、誤った情報があり、訂正又は削除を求められた場合は、合理的な期間内にこれに応じるとともに、訂正又は削除を行った場合は、可能な範囲内で当該個人情報の受領者に対して通知を行わなければならない。