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．JIPDEC-MEDISの解釈

事業の代表者は病院および診療所の管理責任者（院長）にあたります。管理責任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ません。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から選任すべきです。個人情報保護管理者は兼任でかまいませんが、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ります。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ります。そして個人情報保護管理者とその権限および責任をすべての従業員に周知しなければなりません。

また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ません。資源とは例えば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ます。

医療機関におけるプライバシー保護は微妙な問題が数多く存在します。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しょう。プライバシーだけでなく医療には診療上の必要性と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す。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・規範がありますので、倫理委員会を構成する場合は参照してください。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すが、例えば地区医師会などで設けるなどの工夫が推奨されます。

C．考慮すべき問題点

個人情報保護のための責任とはなにか？

個人情報保護のための権限とはなにか？

個人情報保護に必要な資源とはなにか？

微妙な問題に対処するために倫理委員会を設置するべきか。

D．最低限のガイドライン

医療機関の管理責任者は従業員のうち、法令で守秘義務が定められている職種の従業員から個人情報保護管理者を選任する。

医療機関の管理責任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。

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規の遵守を求めることができる。

個人情報保護管理者は従業員が理念を理解し、内規を遵守するために、理念および内規の周知を図り、採用時および年に1度以上は適切な教育を行わなければならない。

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、医療機関の管理責任者に遅滞なく報告しなければならない。

E．推奨されるガイドライン

D．に加えて従業員の内規の遵守違反およ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。

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。

F．要求を満たすにあたって困難な点

G．コメント

H．議論点

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．JIPDEC-MEDIS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および回復であるが、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使用しない情報収集がないことを確認する必要があります。

a）　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したり、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

a´）臨床治験

b）　診療報酬の請求事務

c）　労働者災害補償保険や自賠責の手続きなど

d）　医師や看護婦、その他の医療従事者の教育や臨床研修

e）　臨床研究のためのデータ収集

f）　がん登録のような公益性の高い疫学調査の実施

g）　厚生労働省等の医療行政にかかわる統計･調査、サーベイランス事業
h）　医療機関の経営、運営のための基礎データ
i）　医療機関の上部組織への報告
j）　患者さんの職場、学校等に対する情報提供
k）　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
l）　医療監視や医療指導監査への対応
m）　警察からの問合せ
n）　裁判所からの問合せ
o）　一般の保険会社等からの問合せ

C．考慮すべき問題点

上記の目的には医療機関にとって自明であり、包括的な同意でよいものと、医療機関にとっても自明ではなく、法律的な根拠が明白か、個々に同意をとるべきものが混在しています。これの区別（項目の区別、扱いの区別）をどうするか。

D．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。

E．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。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。

F．要求を満たすにあたって困難な点

G．コメント

H．議論点

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．JIPDEC-MEDIS 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ます。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します。

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、近隣の住民およ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。
d）　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ますが、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りません。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ます。d）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、問題を含んでいます。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すので、取得することはやむを得ませんが、その扱いには十分な配慮が求められます。

C．考慮すべき問題点

D．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。

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。

E．推奨されるガイドライン

D．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得る場合で当該患者の了承を得ることができない場合に、診療遂行上の必要性を複数の従業員が検証を行う。

F．要求を満たすにあたって困難な点

G．コメント

H．議論点

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．JIPDEC-MEDIS の解釈

4．4．2．3の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す。人種、民族、身体・精神障害およ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ます。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ります。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す。ただしこれらは特にプライバシー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ります。

プライバシーに敏感で医療の遂行上必要な情報は少なからず存在します。これらの情報収集には慎重でなければなりませんが、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えます。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す。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ます。

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ります。これも宗教に関する情報収集にあたります。医療面からの必要性は乏しく、安易に収集すればプライバシーの侵害にあたります。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す。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ために情報を収集する場合があります。診療上の必要性はあると考えられますが、止むを得ないかどうかは判断が困難です。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す。

C．考慮すべき問題点

D．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いけない。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ができる。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。

E．推奨されるガイドライン

D．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。

F．要求を満たすにあたって困難な点

G．コメント

H．議論点

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．JIPDEC-MEDIS の解釈

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ります。JISQ15001 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ません。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ますが、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かない項目に関しては利用時に個別に同意を得るべきです。また客観情報の訂正・削除には注意が必要です。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ません。

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ります。ただし乳幼児およ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ありません。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ません。

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ますが、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りません。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ます。

C．考慮すべき問題点

D．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、了解したことを確認する。初診申し込み用紙などに了解した趣旨を確認できる記載を求める。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了解を得る。

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非了解を優先する。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了解を優先してよい。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。患者が乳幼児およ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了解は必要としない。

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およ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およ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仲で利用時に個別に同意を得、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およ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、およ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。）

E．推奨されるガイドライン

F．要求を満たすにあたって困難な点

G．コメント

H．議論点

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．JIPDEC-MEDIS 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、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ります。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ります。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ります。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りません。

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します。この場合は要求事項の例外のａに相当すると考えられます。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りません。

C．考慮すべき問題点

診療遂行上の必要性があれば、すべて同意なく取得してよいか？

意識障害がある場合（客観的に意識障害があることを示さなければならないが）はやむをえないとして、本人が虚偽を述べる可能性が強い場合にも周囲から情報を得る必要がある場合がある。しかし本人が当該項目に関して虚偽を述べているかどうかは、慎重に判断しなければならない。

D．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。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。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、およ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。

E．推奨されるガイドライン

D．に加えて診療の遂行上の必要性、およ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。

F．要求を満たすにあたって困難な点

G．コメント

H．議論点

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．JIPDEC-MEDIS 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、個別のものがあります。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ります。ｂ）は緊急避難に相当するものです。

C．考慮すべき問題点

D．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。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。

情報の利用が法令による場合は同意を必要としない。

患者および公衆の生命、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。

E．推奨されるガイドライン

F．要求を満たすにあたって困難な点

G．コメント

H．議論点

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．JIPDEC-MEDIS 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であって、原則的には患者の同意を必要とする。ただし診療情報では公益目的およ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があり、この場合は同意を必要としないと考えられます。

また患者が意識障害、精神障害、乳幼児等で、同意を得られない場合があります。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す。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ります。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提供してはいけません。

C．考慮すべき問題点

D．最低限のガイドライン

あらかじめ同意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、財産および公衆の生命、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。

E．推奨されるガイドライン

F．要求を満たすにあたって困難な点

G．コメント

H．議論店

医療情報地域連携ネットワークシステム用認証局

証明書ポリシおよび認証業務運用規程（案）

Version　0．2

2002年　1月22日

（財）医療情報システム開発センター

1．　はじめに

1．1．　概要

1．1．1．　本ポリシの適用範囲

本ポリシは、医療従事者用公開鍵証明書および患者用公開鍵証明書を発行する「医療情報地域連携ネットワークシステム用認証局」の証明書ポリシおよび認証業務運用規程作成の標準として参照される。個々の医療情報地域連携ネットワークシステム用認証局」は、これを基準にして差分を明確にして個々の環境に適合した証明書ポリシおよび証明業務運用規程を作成するものとする。

1．1．2．　証明書のライフサイクル

1．1．2．　本ポリシが依拠する文書

ISO/DTS17090-3 保健医療情報 – 「公開鍵基盤 パート3: 認証局のポリシ管理」

1．1．4．　本ポリシが参照する文書

ISO 17799-1:2000　情報技術 － 情報セキュリティ管理の運用規程

電子署名及び認証業務に関する法律（平成12年5月31日　法律第102号）

電子署名及び認証業務に関する法律施行規則（平成13年3月27日　総務省・法務省・経済産業省令第2号）

電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成13年4月27日　総務省・法務省・経済産業省告示第2号）

1．1．　本ポリシの名称とオブジェクト識別子

本規程の名称を「ＸＸＸＸＸＸＸ」とする。本規程および関連サービスに割り当てられた
オブジェクト識別子（ＯＩＤ）を以下に示す。

1．2．３９２．２ＸＸＸＸＸ　　（財）医療情報システム開発センター

1．2．３９２．２ＸＸＸＸＸ．Ｙ．ＺＺＺＺ　本規程

1．3．　本証明書が流通するコミュニティと証明書の利用目的

1．3．1．　認証局 (Certification Authority

1．3．2．　登録局 (Registration Authority)

1．3．3．　エンドエンティティ (End Entity)

1．3．4．　利用範囲

紹介状等の診療諸記録等への医療従事者としての署名用鍵。

患者の同意書等への署名用鍵

医療従事者あるいは患者のアクセスコントロール用鍵

データ暗号用鍵。

1．4．　問い合わせ先
1．4．1．　主管部署
1．4．2．　照会窓口
1．4．3．　ポリシ責任者

2．　一般条項
2．1　義務
2．1．1．　認証局の義務

CAは，登録プロセス，証明書に含まれる情報の検証，証明書製造業者，発行，失効，停止，及び更新の管理を含めて，証明書の発行と管理のすべての局面に責任がある。CAは，CAのサービスと運用のすべての局面がこの証明書ポリシの要件，表現，及び保証とCAの認証実践規定に従って行われることを保証する責任がある。

ヘルスケアPKI内のCAは，提供するサービスについて利用可能なポリシと手続きをもつものとする（SHALL)。それらは，次のことを扱うものとする（SHALL)。

1. 適用可能な場合は，本ガイドラインＸＸＸＸで定義される証明利用者の役割も含めて，証明書発行に先立つ証明書利用予定者の登録手続き。
2. 証明書発行に先立つ，証明書利用予定者のアイデンティティの認証手続き。
3. 証明書が与えられる人々に関して保持される個人情報のプライバシーを保持する手続き。
4. 証明書利用者及びディレクトリへの証明書の配布手続き。
5. 秘密鍵危殆化の可能性に関する情報を受け取る手続き。
6. 証明書失効リストの配布手続き（発行頻度，発行方法，及び発行場所）。
7. 鍵のサイズ，鍵生成プロセス，証明書の有効期間，鍵の再生成など，その他の鍵管理問題。
8. 他の認証局との相互認証手続き。
9. セキュリティの管理と監査。

この機能を果たすためには，基盤内の各CAは，証明書利用者及び検証者にいくつかの基本的なサービスを提供する必要がある。これらのCAサービスを以下に列挙する。

2．1．1．1．　証明書の発行、停止、および失効の通知

発行CAは，証明書利用者の識別名を持つ証明書が発行されるときには，各証明書利用者に通知するものとする（SHALL)。

発行CAは，証明書利用者の識別名を持つ証明書が失効または停止されるときには，証明書利用者に通知するものとする（SHALL)（装置またはアプリケーション証明書の場合，通知は，責任を持つ個人または組織に対して行われるものとする)。

発行 CA は，本規程 4.4 に従って，検証者が証明書失効リスト（CRL）を入手できるようにするものとする（SHALL)。

２．１．１．２．　ＣＡの表現の正確性

発行 CA が証明書を発行するときには，証明書利用者に証明書を発行したことと，証明書に記載されている情報が CA の証明書ポリシ（CP）に従って検証されたことを確認する。証明書利用者がアクセスできるリポジトリでの証明書の発行が，このような検証の通知を構成するものとする（SHALL)。

CA は，この証明書ポリシに基づく証明書利用者の権利と義務を各証明書利用者に通知するものとする（SHALL)。このような通知は，証明書利用者同意書の形でもよい（MAY)。このような通知は，この CP に基づいて発行された証明書の許される用途，証明書利用者の鍵の保護に関する責任，及びサービス提供の変更またはこのポリシーの変更の伝達も含めて，証明書利用者と CA 及び LRA の間の通信手続きの記述を含むものとする（SHALL)。CA は，鍵の危殆化のおそれ，証明書または鍵の更新，サービスの取り消し，及び紛争解決を処理するための手続きを証明書利用者に通知するものとする（SHALL)。

２．１．１．３．　証明書の申請から発行までの期間

CA は，証明書所有者が鍵活性化の生成後に鍵活性化プロセスを完了しなければならない最大期間を記述することが推奨される（RECOMMENDED)。

２．１．１．４．　証明書の失効と更新

発行 CA は，証明書の期限切れ，失効，及び更新の手続きが，この CP の該当する条項に従わなければならない（SHALL）ことを確実にするものとする（SHALL)。CRL 配布ポイントのアドレスは，証明書で定義されることが推奨される（RECOMMENDED）（本ガイドラインＸＸＸＸ参照)。

２．１．１．５．秘密鍵の保護

CA は，それが保有または格納する秘密鍵及び活性化データが本規程 6.2，6.3，及び 6.4 に従って保護されることを確実にするものとする（SHALL)。

CA は，それがバックアップまたは保存した証明書利用者の秘密復号鍵が本規程 6.2 に従って保護されることを確実にするものとする（SHALL)。CA は，法によって必要とされない限り，証明書利用者の事前同意なしで他の関係者に秘密復号鍵を開示しないものとする（SHALL)。前記にかかわらず，非資格ヘルスケア従業員または支援組織従業員は，自分の雇用者の事業を遂行するために証明書を受け取るので，CA は，データ回復の目的のために，非資格ヘルスケア従業員または支援組織従業員の雇用者に秘密復号鍵を開示してもよい（MAY)。

２．１．１．６．ＣＡの秘密鍵使用制限

CA は，その証明書署名秘密鍵が，証明書及び証明書失効リストに署名するためだけに使用されることを確実にするものとする（SHALL)。CA は，CA アプリケーションへのアクセスと操作のためにその人員

に発行した秘密鍵が，このような目的のためだけに使用されることを確実にするものとする（SHALL)。

2．1．2．　登録局の義務

CA は，それが責任を持つ識別及び認証機能を登録局（RA）に委託してよい（MAY)。ヘルスケア組織 RA が果たす主要な機能は，初期登録の際の証明書利用者のアイデンティティとヘルスケア役割の検証である。RA は，CA が自ら使用するのと同じ規則集と認証方法に従うものとする（SHALL)。RA のものは，特定の CA から独立して，個別に認定されてよい（MAY)。

証明書及びそれに含まれる公開鍵の真正性と完全性が確信されるためには，証明書利用者は，信頼できる出所に証明書を作成してもらわなければならない。RA は CA に代わって認証機能を果たすので，CA の証明書利用者認証ポリシに従い，正しい証明書利用者情報を CA に渡すことが信頼されなければならない。同様に、RA は，証明書失効申請を正確かつタイムリーに CA に渡すことが信頼されなければならない。

登録局は，CA に代わって果たす行為について個別に責任を負うことが推奨される（RECOMMENDED)。

RA は，次のことを行うものとする（SHALL)。

1. RA がオンラインでその責務を果たしている場合は，その署名秘密鍵が証明書申請に署名するためだけに使用されることを確実にする。
2. 証明書利用者のアイデンティティを認証したことを CA に対して証明する。
3. 証明書アプリケーション情報及び登録記録を安全に伝送し，格納する。

（適用可能な場合は）本規程 3.4.2 に従って失効申請を開始する。

2．1．2．1．　証明書失効申請

RA は，証明書失効申請の取り扱いに役立ちうる。一部の医療 PKI 実装では，RA は，証明書失効申請手順を開始または認証するために使用されてよい（MAY)。適用可能な場合，RA は，認証した要求を適切な CA に転送するものとする（SHALL)。RA 自身が失効申請を開始してもよい（MAY)（たとえば，医療専門家が不行跡によって停職処分にされ，RA が医療専門家登録局または許可局の場合)。いずれかの場合，報告を認証するのは RA の責任である。 CA が使用したであろう同じ基準を適用することによって，報告が真正であると RA が認めた場合，RA は，証明書識別情報とその証明書を失効する記載理由を含んだ署名つきメッセージを CA に送信するものとする（SHALL)。

2．1．2．2．　監査

RA は信頼できるという確信を提供するため，及び内部監査を実施する人員に情報を提供するために，各 RA の行動は監査可能であるものとする（SHALL)。イベントの監査記録及び監査証跡は，適切なポリシに従って生成されなければならない。

2．1．2．3．　保管

将来，証明書の生成方法と生成理由を知ることが重要になるかもしれない。ヘルスケア PKI またはその CA 内の RA は，証明書の作成要求または失効要求などのイベントを保管するものとする（SHALL)。

2．1．3．　利用者の義務

ヘルスケア PKI の証明書利用者は，次のことを行うものとする（SHALL)。

1. 証明書アプリケーションの表現の正確さを確認し，証明書を受け入れることによって，証明書に含まれている情報のすべてが真実であることを承認する。
2. 秘密鍵及び（適用可能な場合は）鍵トークンを保護し，それらの紛失，開示，変更，または無許可使用を防止する妥当な措置をすべて取る。
3. 自分の秘密鍵の紛失，開示，または無許可使用を防止するためにあらゆる努力を払う。
4. 自分の秘密鍵の実際の紛失，開示，またはその他の危殆化，またはそれらが疑われるときには，ただちに CA 及び/または RA に通知する。
5. 証明書情報，ヘルスケア組織における役割または地位の変更を RA 及び/または CA に通知する。
6. 証明書ポリシ（CP），または証明書利用者の責任を平易なことばで明瞭に述べた PKI 開示文書を読む。
7. CP に従って鍵ペアを使用する。
8. 証明書利用者同意書に署名することによって，これらの義務に正式に同意する。

また，ヘルスケア PKI の証明書利用者は，証明書が使用される医療情報機能に適したセキュリティトレーニングを受けたことを証明することが推奨される。

2．1．3．　検証者の義務

ヘルスケア PKI の検証者は，次の場合に限り，ヘルスケア証明書に対する権利を保有する。

1. 証明書が使用される目的が，このポリシの下で適切であった場合。
2. 検証が、検証の時点で検証者に知られているすべての状況を考慮に入れて，妥当であり，誠意によるものである場合。
3. 証明書が失効または停止されていないことを確認することによって，検証者が証明書の現在の有効性を確認した場合。
4. 適用可能な場合は，検証者がデジタル署名の現在の有効性を確認した場合。
5. 責任と補償の適用限界を承認した場合。

2．1．4．　リポジトリの義務

証明書及び CRL は，本規程 4.4.9 の要件に従って，検証者にとって入手可能であるものとする（SHALL)。

2．2．　責任

2．2．1．　認証局の責任

ヘルスケアPKIのCAの責任は，CA部門の怠慢行為に限定されてよい（MAY）。特に，

1. CAは，秘密鍵の証明書利用者による紛失に関しては責任がないとみなしてよい（MAY）。
2. CAは，ヘルスケアPKIの指針に完全に従って生成されなかった場合，証明書利用者が生成した鍵に関して責任がないとみなしてよい（MAY）。
3. CAは，鍵がCAにおいて危殆化したこと，または鍵生成プロセス中に文書化されたポリシ及び手続きが遵守されなかったことが，秘密鍵の危殆化の疑いを強めたか，秘密鍵の実際の発覚をもたらしたことが証明されない限り，CAが生成した秘密鍵の危殆化に関して責任がないとみなしてよい（MAY）。
4. CAは，ヘルスケアPKIの文書化されたポリシ及び手続きが遵守されなかったことが偽造をもたらしたか，それらを示すことによって偽造を許した場合を除き，偽造された署名に関して責任がないとみなしてよい（MAY）。
5. CAは，その責任を，CAがこのポリシの条項に従わなかったことが原因で検証者がこうむった直接損害に限定してよい（MAY）。

ヘルスケアPKIのCAの責任は，次のことに関して制限されないものとする（SHALL NOT)。

6. CAは，鍵配布プロセス中の秘密鍵の危殆化に責任があるものとする（SHALL）。
7. CAは，身元確認と認証に関する文書化されたポリシ及び手続きが遵守されたことが証明されない限り，個人のアイデンティティとそれに関連付けられたデジタル署名及びその他の認定情報との誤った結合に責任があるものとする（SHALL）。この責任は，CAが結合に誤りがあることを知っていたか疑っていた状況，または知っているべきか疑うべき状況にも及ぶものとする（SHALL）。
8. CAは，その失効ポリシに従って証明書を失効しなかったことに対して責任があるものとする(SHALL)。
9. CAは，その失効ポリシで規定されていない理由のために証明書を失効したことに対して責任があるものとする（SHALL）。

2．2．2．　登録局の責任

ヘルスケアPKIのRAの責任は，RA部門の怠慢行為に限定されてよい（MAY)。
ヘルスケアPKIのRAの責任は，次のことに関しては限定されないものとする（SHALL NOT)。

1. RAは，身元確認と認証に関する文書化されたポリシ及び手続きが遵守されたことが証明されない限り，個人のアイデンティティとそれに関連付けられたデジタル署名及びその他の認定情報との誤った結合に責任がある。この責任は，RAが，結合が行われるサブジェクト情報が誤りであることを知っていたか疑っていた状況，または知っているべきか疑うべき状況にも及ぶものとする（SHALL）。
2. RAは，その失効ポリシに従って証明書を失効しなかったことに対して責任がある。
3. RAは，その失効ポリシで規定されていない理由のために証明書を失効したことに対して責任がある。

2．3．　財務上の責任

本規程は，さらなる規定をしない。

2．4．　解釈および執行

2．4．1．　準拠法

ヘルスケア PKI は，ISO 17799-1:2000 と同等以上の規格，または認可された認定あるいはライセンス基準に従って，ローカル及び国際的な法律上の要件に従うものとする（SHALL)。

2．4．2．　分割、存続、合併及び通知

ヘルスケア CP は，CP の 1 つのセクションが正しくないか無効であると判断した場合，ポリシが更新されるまで，他のセクションは事実上存続するものとする（SHALL）ことを明記するものとする（SHALL)。CA または RA が別の組織と合併する場合，新しい組織は元の同意書の方針に責任を持ちつづける。

2．4．3．　紛争解決の手続き

本規程では，さらなる規定をしない。

2．5．　手数料

本規程では，さらなる規定をしない。

2．6．　情報の公表とリポジトリ

2．6．1．　CA に関する情報の公開

ヘルスケア PKI 内のすべての CA は，次のものを証明書利用者と検証者にとって入手可能にするものとする（SHALL)。

1. CA によって，または CA に代わって管理され，証明書ポリシを含んでいる使用可能な Web サイトの URL
2. このポリシの下に発行された各証明書。
3. このポリシの下で発行された各証明書の現在の状態。
4. CA が運営の基準としている認定またはライセンス基準（CA が運営されている管轄区域でそれらの認定またはライセンス基準が適用可能な場合）。

2．6．2．　公表の頻度

CA は，このような情報が変更されたときにはいつでも，その情報を公開するものとする（SHALL)。証明書失効についての情報は，本規程セクション４．４に従うものとする（SHALL)。

2．6．3．　公表される情報に対するアクセス制御

証明書ポリシ，運用規程，証明書，及びそれらの証明書の現在の状態などの公開情報は，読み取り専用とする（SHALL)。

２．６．４．　リポジトリ

RA または CA リポジトリに証明書利用者に関して保持される情報は，次のようであるものとする（SHALL)。

1. 最新に保たれる（変更の 1 日以内，状況によってはさらに早く検証される）。
2. ISO 17799-1:2000 と同等以上の規格，または認可された認定あるいはライセンス基準に従って管理される。

２．７．　準拠性監査

準拠性監査は，多くの PKI 相互運用性モデルの不可欠なコンポーネントである。

２．７．１．　監査頻度

ヘルスケア PKI ポリシに従って証明書を発行する CA は，それがこのポリシーの要件に完全に従っているという検証者の満足を確立するものとする（SHALL)。CA 準拠性監査は，1 年より長くない間隔で，資格を持った独立した第三者によって行われるものとする（SHALL)。

２．７．２．　監査人の身元・資格

監査者は，（ISO9000 認定など）適切な関連職業団体への加入に必要な程度の情報システム監査者としての資格を持つものとする（SHALL)。監査者は，豊富な PKI 経験を持つものとする（SHALL)。正式な認定団体が存在する場合，監査者は，その団体の要件を満たしているものとする（SHALL)。

２．７．３．　監査人と被監査部門の関係

監査者は，CA とは別個の組織に属することによって，被監査者から完全に独立しているものとする（SHALL)。監査者は，非監査者に対しての財政的利害を持たないものとする（SHALL)。

２．７．４．　監査テーマ

証明書利用者登録，証明書登録，危殆化した鍵の報告，及び証明書失効などのイベントが監査されるものとする（SHALL)。監査は，一般に，証明書ポリシ及び関連する認証業務運用規程の準拠性をカバーする。

２．７．５．　監査指摘事項への対応

監査で違反が発見された場合，CA は，是正措置を取るものとする（SHALL)。CA が監査に対して適切な措置を取らなかった場合，CA の統制責任部門は，次のようにしてよい（MAY)。