社団法人　日本臨床衛生検査技師会

個人情報保護ガイドライン

＝第１集＝

Ⅰ　個人情報保護方針

Ⅱ　プライバシー規約

Ⅲ　日臨技総合情報管理システム利用規約

Ⅳ　検査情報システムの安全管理に関する
　　ガイドライン

社団法人　日本臨床衛生検査技師会

目　次

社団法人日本臨床衛生検査技師会

個人情報保護方針

１．基本方針

会員の個人情報は重要かつ貴重な固有財産である。

ここに掲げる個人情報保護基本方針（以下「基本方針」という）の趣旨は、個人情報に係わるあらゆる脅威から、社団法人日本臨床衛生検査技師会(以下「当会」という)が保有する情報資産を保護することにある。

当会の業務に従事するすべての者は､個人情報を正確かつ安全に取り扱うことにより会員固有の情報を守り、その信頼に応えなければならない。

２．組織活動

基本方針を具体化するため、以下の活動を行うものとする。

（１）当会が行う業務に携わる役員をはじめとするすべての従事者は、個人情報に関する法令およびその他の規範を遵守すること。

（２）個人情報保護管理者を選任し、管理者には個人情報保護の実施や運用に係わる権限を与え、その責任を明確にしつつ業務に従事させること。

（３）会長レビューに基づき、当会の規程並びに運用方法を継続的に改善すること。

（４）都道府県技師会、関連団体、取引相手となる企業および個人に対し、規程の目的達成のための協力を要請すること。

（５）基本方針は、当会のホームページ（URL=http://www.jamt.or.jp)に掲載することにより常時閲覧可能とすること。

３．個人情報の取り扱い

（１）個人情報の収集･利用･提供

当会は、個人情報の収集にあたり、会員に対し収集目的を可能な限り明らかにし、収集した個人情報の使用範囲を限定し適切に取り扱うこととする。

（２）権利の尊重

当会は、個人情報に関する個人の権利を尊重し、固有の個人情報に対し、開示、訂正、削除を求められたときは、合理的な期間および妥当な範囲内でこれに応ずることとする。

（３）安全対策の実施

当会は､個人情報の漏洩あるいは不当な改竄などのトラブルを引き起こすことのないように規程を整備し、万全な安全対策を実施することとする。

平成17年４月１日

社団法人日本臨床衛生検査技師会
会　長　小　﨑　繁　昭

社団法人日本臨床衛生検査技師会
プライバシー規約

社団法人日本臨床衛生検査技師会（以下「当会」という。）では、会員固有の個人情報を慎重に取り扱い、プライバシーの尊重と個人情報の保護のため細心の注意を払うことを目的として、以下の取り組みを実施しております。

当会のホームページ をご利用された場合は、この「プライバシー規約」に同意されたものとみなされます。

Ⅰ．当会の取り組みについて

１．当会は、会員固有の個人情報を取り扱うにあたり管理責任者を置き、適切な管理を行っております。
２．当会から、会員の個人情報を取得する場合は、窓口等をあらかじめ明示するとともに、利用目的をできる限り特定したうえで必要な範囲の個人情報の取得を行います。
３．当会は、会員より取得した個人情報を適切に管理し、会員の同意を得た会社以外の第三者への提供並びに開示等は一切行いません。また、会員の同意による個人情報を提供する会社には、個人情報の漏えいや再提供等を行わないとする契約に基づく義務化などの適切な管理を実施します。
４．会員に係わる情報は、当会を中心とする都道府県技師会の運営にとり重要なものであり、各都道府県技師会間で共有し、いずれの共有者も、本プライバシー規約または少なくとも本プライバシー規約に規定されている条件と同様の保護条件に従うものとします。
５．当会は、電子メール、郵便等により会員に送信或いは送付または電話をする場合があります。ただし、申し出により、これらの取扱いを中止或いは再開させたりすることができます。
６．会員が、固有の個人情報の照会或いは修正等を希望するなど、ホームページあるいは当会窓口まで連絡があった場合は合理的な範囲で速やかな対応を行います。
７．当会は、保有する個人情報に関して適用される法令或いは規範を遵守するとともに上記各項における取り組みの適宜見直し並びにその改善を行います。

Ⅱ．当会の個人情報収集について

当会は、会員から収集した情報は、臨床・衛生検査技師として活動するために有用な情報の発信並びにその活用のため利用しており、その収集している情報は、以下のとおりです。

１．会員から提供される情報
　会員が入会時に提出した入会申込書および当会総合情報管理システム（以下「ＪAMTＩS」という。）＜Webサイト＞に入力された情報、またはその他の方法で提供された情報を受け、保管します。
　収集される情報は、ＪAMTＩSにて確認できます。会員は、一部の情報を提供しない選択をすることができます。しかし、その結果、当会或いは都道府県技師会の次挙機能が利用できなくなる場合があります。
提供された情報は、会誌発送、会費請求、会員サービスの向上、会員相互の連絡などの目的に利用されます。
２．電子メール
　電子メールを連絡手段として使用し、情報の共有化をより有効かつ有意義なものにするため、会員より送付された電子メールアドレスを保存しています。
３．その他の情報
　会員に関する情報を各都道府県技師会から入手し、当サイトの個人情報に追加する場合があります。

Ⅲ．情報の開示

当会は、情報を開示することにより、法令の遵守、利用規約並びにその他の合意の援用、適用或いは当会、会員などの権利、財産、安全の保護のために適切であると判断した場合に限りその個人情報を開示します。

これには､詐欺被害および信用リスク対策のために行われる企業やその他の組織との情報交換も含まれます。ただし、本プライバシー規約に記載された義務違反となるような商業目的のために、会員からの個人識別情報を販売、レンタル、共有、その他開示を行うことはありません。

上記の場合以外に、会員に関する情報が第三者に渡る可能性がある場合には、その旨をお知らせします。その際、会員は個人情報の共有を拒否することができます。

Ⅳ．個人情報の安全性

当会では、会員の情報が送信される際のセキュリティのために、SSL（Secure Socket Layer ソフトウェア）を用い、入力された情報を暗号化します。

また、不正なアクセスから自身のパスワードやコンピュータを保護することは、会員にとって重要です。他人と共用しているコンピュータを使い終ったときには、必ずサインアウトしたことを確かめてください。

Ⅴ．利用規約とポリシーおよびその改訂

会員がＪＡＭＴＩＳを利用する場合、その利用およびプライバシーに関するあらゆる紛争については、本文書と利用規約が適用され、日本国法の適用を含みます。

また、プライバシーに関して懸念を生じた場合は、その連絡により解決に努めます。

当会の事業は絶えず変化し、プライバシー規約および利用規約もまた変更されます。

最新の内容変更に関しては、ＪＡＭＴＩＳにおいて確認されるようお願いします。別途規定されていない限り、最新のプライバシー規約は当会が会員に関して有するすべての情報に対して適用されます。

平成17年４月１日

社団法人日本臨床衛生検査技師会
会　長　小　﨑　繁　昭

社団法人日本臨床衛生検査技師会
ＪAMTＩS 利用規約

社団法人日本臨床衛生検査技師会（以下「当会」という。）および各都道府県技師会は、以下の規約に基づき日本臨床衛生検査技師会総合情報管理システム（ＪAMTＩS）の運用を行い、会員および各都道府県技師会に対し、会員管理及び学術研究に関する情報・サービスの提供を行います。

ＪAMTＩSは、当会における会員管理及び学術研究に関する活動を支援し、その発展に寄与することを利用目的としています。ただし、当会の管理・運営及び会員の交流のための利用については、これを認めるものとします。

会員および各都道府県技師会がＪAMTＩSを利用される場合は、この規約に同意されたものとみなされますので注意してください。

Ⅰ．利用資格とは

ＪAMTＩSを利用することができる者の範囲は、以下のとおりです。

1．当会正会員、Ｂ・Ｃ賛助会員
2．前掲のほか、当会が認めたもの

注）当会並びに都道府県技師会事務所職員に関しては、別に定めることとします。

Ⅱ．利用者の義務

1．利用者は、ＪAMTＩSを利用するために必要な通信機器、ソフトウェア、その他これらに付随して必要となる全ての機器を、自己の費用と責任において準備し、ＪAMTＩSが利用可能な状態に置くものとします。また、自己の費用と責任で、利用者が任意に選択しインターネットに接続するものとします。
2．利用者は、当会又は関係官庁等が提供する情報を参考にし、自己の利用環境に応じ、コンピュータ・ウィルスの感染、不正アクセス及び情報漏洩の防止等セキュリティを保持するものとします。
3．ＪAMTＩSにアクセスされる利用者は、投稿、提案、アイデア、コメント、質問、その他の情報の送信を行うことができます。ただし、それらの内容が、法令に反するもの、猥褻なもの、脅迫的なもの、名誉を毀損するもの、プライバシーを侵害するもの、知的財産権を侵害するもの、第三者を誹謗中傷するもの、不快感を与えるもの、あるいは、ソフトウェアウイルス、政治的主張、商業目的の勧誘、チェーンレター、メールの大量送信を含むものは、この限りではありません。虚偽の電子メールアドレスの使用、他人または組織になりすますこと、などの行為は禁止します。

Ⅲ．利用許可およびサイトへのアクセス

1．ＪAMTＩSにアクセスし個人的に利用される場合、利用者個人の情報、あるいは当会からの書面による明示的な承諾を得た場合を除き、ＪAMTＩSのいかなる部分もダウンロード（キャッシュを除く）または変更しないという制限の下で利用を認めています。ただし、各都道府県技師会に対して、ダウンロードを許可している項目は除きます。
2．利用許可には、ＪAMTＩSまたはそのコンテンツの転売および商業目的での収集と利用、ＪAMTＩSまたはそのコンテンツの二次的利用、他社のために行う個人情報のダウンロードとコピー、データマイニング、などのデータ収集・抽出ツールの使用は、一切含まれておりません。
3．ＪAMTＩSまたはそのいかなる部分も、当会からの書面による明示的な承諾を得ていない限り、商業目的の、複製、複写、コピー、販売、再販、アクセス、その他の利用はできません。
4．当会、各都道府県技師会、または両者のサービスを、不正な、誤解を招くような、名誉を毀損するような、あるいは不快感を与えるような方法で表現しない限り、ＪAMTＩSにハイパーリンクを作成することを

認められています。

5．当会と各都道府県技師会は、それぞれの裁量の下で、サービスの拒否、パスワードの停止を行う権利を留保します。

6．利用者が原稿または素材の送信を行った場合、利用者は、当会と各都道府県技師会に対して、そのような原稿などを使用し、複製、公開できる、完全なサブライセンスを含む権利を許諾したものとみなします。また、そのような原稿などに関連して利用者が送信された名前を使用する権利を許諾したものとみなします。

7．当会は、いかなる行為またはコンテンツも監視し編集する権利を保有しますが、義務はありません。当会は、利用者または第三者から投稿されたいかなるコンテンツに対しても、責任を負わず、義務が生じることもありません。

Ⅳ．利用上の制約

会員は、入会及び継続申込の経路・手段、会費納入時期によっては、ＪAMTＩＳが提供する特定のサービスを一時的に利用できない等の制約を受ける場合があることを承諾します。

Ⅴ．個人認証情報の管理

1．ＪAMTＩＳを利用する場合、パスワードの機密性を維持し、コンピュータへのアクセスを制限する責任は、利用者にあります。利用者は、自己のパスワード等の個人認証情報を失念した場合は直ちに当会に申し出るものとし、当会の指示に従うものとします。

2．利用者は、自己の個人認証情報および個人認証を条件とするＪAMTＩＳを利用する権利を他者に使用させず、他者と共有あるいは他者に許諾しないものとします。また、自分のパスワードを使って行われるすべてのことに対する責任を認めることに同意するものとします。

3．利用者は、自己の個人認証情報不正利用の防止に努めるとともに、その管理について一切の責任をもつものとします。当会は、会員の個人認証情報が第三者に利用又は変更されたことによって当該利用者が被る損害については、当該利用者の故意過失の有無にかかわらず一切責任を負いません。

Ⅵ．プライバシーについて

プライバシーに対する考え方の内容(日本臨床衛生検査技師会プライバシー規約)は、利用者がＪAMTＩＳを利用される場合にも適用されます。よくお読みになり、ご理解いただきますようお願いします。

Ⅶ．電子メール

利用者がＪAMTＩＳにアクセスをし、日本臨床衛生検査技師会事務所(当会事務所)に電子メールを送信するときは、当会事務所から会員への連絡は、電子メールまたは本サイトにお知らせを掲載する方法によることとします。利用者は、当会からから電子的な方法で連絡を受けることに同意するものとします。利用者は、全ての合意、お知らせ、情報開示その他の連絡を当会事務所が電子的に行うことをもって、かかる連絡を書面で行うことを求める法律上の要請を充たしていることに同意することとします。

Ⅷ．著作権

ＪAMTＩＳに含まれるすべてのコンテンツ（文字、グラフィック、ロゴ、ボタンアイコン、画像、オーディオクリップ、デジタル形式でダウンロードされたもの、データに編集を加えたもの、ソフトウェアなど）は、当会、またはコンテンツ提供者の財産であり、日本の著作権法、および著作権に関する国際法によって保護されています。

1．ＪAMTＩＳに含まれるすべてのコンテンツの編集物は、当会の独占的な財産であり、日本の著作権法および著作権に関する国際法によって保護されています。

２．ＪAMTＩＳで使用されているすべてのソフトウェアは、当会. またはソフトウェア提供者の財産であり、日本の著作権法および著作権に関する国際法によって保護されています。
３．ＪAMTＩＳに提供されている情報および画像等の無断転載をお断りいたします。

Ⅸ. 著作権侵害に関する申し立て

当会と各都道府県技師会は、他者の知的財産を尊重します。会員の著作物が、著作権の侵害を構成するような方法で複写されたと判断された場合は、当会の著作権侵害についての申し立てとその手続きに従って申し立ててください。

Ⅹ．免責事項

当会のサービスは、ＪAMTＩＳというWebサイトとしてその時、有る姿でしか提供しておりません。利用者は、ご自分の責任でＪAMTＩＳをご利用になることに明示的に同意されたものとみなされます。
１．当会は、適用される法律によって認められる限り、特定の目的に対する適合性の黙示的な保証を含みこれに限定されない保証を一切いたしません。
２．当会は、ＪAMTＩＳ、サーバー、当会事務所から送信された電子メールが、ウイルス、またはその他の有害な要素に感染していないことを保証いたしません。
３．当会は、直接的、間接的、付随的、懲罰的、必然的な損害を含み、ＪAMTＩＳの使用から生じるいかなる種類の損害に対しても責任を負うものではありません。ただし、お住まいの国や地域の法律によっては、黙示的な保証、ある種の損害の例外または制限を認めていません。そのような法律が適用される場合は、上記の免責事項、例外、制限の全部または一部が適用されず、利用者は追加的な権利を有することがあります。

ⅩⅠ．準拠法

ＪAMTＩＳをご利用いただいた場合、日本国内法が、法の抵触の原則にかかわらず、この利用規約、および利用者と当会または各都道府県技師会との間に起きる可能性のあるあらゆる種類の紛争について、これを規制することに同意されたものとします。

ⅩⅡ．紛争

ＪAMTＩＳへのアクセスを通じた紛争に関してはすべて、東京地方裁判所を管轄裁判所として指定します。ただし、利用者が何らかの方法で当会 の知的財産権を侵害した、または侵害すると提訴した結果、当会が東京地方裁判所以外の裁判所に命令的、またはその他の適切な救済を求め、会員がそのような裁判所での独占的な裁判権と裁判地に同意された場合を除きます。この同意に基づく紛争は、紛争時に有効な日本国内法の下で行われます。

ⅩⅢ．サイトの運営方針

ＪAMTＩＳの運営方針については、当サイトに掲載されている文書をよくお読みください。これらの方針は、利用者のＪAMTＩＳのご利用も規制します。
当会は、ＪAMTＩＳ、方針、利用規約をいつでも変更できる権利を保有します。この規約の一部が不正または無効である、何らかの理由で施行できない場合は、その規約は可分であるとみなされ、それ以外の規約の有効性および拘束力に影響を及ぼすことはありません。

＜附　記＞

Ⅰ．ＪAMTＩＳのアクセス権限について

１．アクセス権限の種類

会員および都道府県事務員がＪAMTＩＳで行う作業をアクセス権限という形で制限します。アクセス権限は次の６種類があります。

会員の場合は与えられたアクセス権限と会員権限を持ちます。

【日臨技事務権限】

アクセス権限としては一番強く、ＪAMTＩＳ上の機能全てが実行できます。管理できる範囲は、47 都道府県の情報全てです。

（1）日臨技事務権限の登録方法

日臨技事務所の事務専用端末から職員登録をします。

職員番号（日臨技職員専用会員番号）とパスワードが発行されます。

（2）ＪAMTＩＳでのアクセス方法

職員番号とパスワードを入力してログインします。

【都道府県事務権限】

都道府県の事務処理を行うためのアクセス権限で、管理できる範囲は、担当都道府県の情報のみです。都道府県事務権限は、下記に示す都道府県学術のアクセス権限も含まれます。

このアクセス権限をもつ会員の場合は、都道府県の役職を有する者である事が必須です。

都道府県事務職員にアクセス権限を持たせる場合は、日臨技に申請し、登録の後、職員番号（都道府県職員専用会員番号）とパスワードを通知します。

（1）都道府県役員登録とアクセス権限を与える方法

役職マスターに役職を登録し会員の役員就任処理を行います。

役員リストからアクセス権限の登録をします。この権限は会員個人の情報として保存されます。

（2）ＪAMTＩＳでのアクセス方法

会員の場合　　：会員番号とパスワードを入力してログインします。

職員の場合　　：職員番号とパスワードを入力してログインします。

【都道府県学術権限】

都道府県の学術関連処理を行うためのアクセス権限で、管理できる範囲は、担当都道府県の情報のみです。

（1）都道府県役員登録とアクセス権限を与える方法

このアクセス権限をもつ会員の場合は、都道府県役職を有する者である事が必須です（都道府県役員登録とアクセス権限を与える方法を参照）。

（2）ＪAMTＩＳでのアクセス方法

会員の場合：会員番号とパスワードを入力してログインします。

職員の場合：職員番号とパスワードを入力してログインします。

【学会・全国研修会権限】

学会（日臨技・地区・県）と全国研修会関連の業務を行うためのアクセス権限です。管理できる範囲は、取得した学会（研修会）コードのみです。

このアクセス権限を持つ会員は、都道府県学術権限以上が必要です（都道府県学術権限の項参照）。

（1）学会・全国研修会権限を得る方法

日臨技に新規学会・研修会登録を依頼します。

日臨技では専用端末で新規登録を行い、学会・全国研修会コードおよびパスワードを申請者に通知します。

学会・全国研修会コードの変更は出来ません。またパスワードの変更は、日臨技で行うことが出来ます。

（2）ＪAMTＩＳでのアクセス方法

会員の場合

会員番号とパスワードを入力してログインし、学会（研修会）コードと学会（研修会）パスワードを入力します。

職員の場合

職員番号とパスワードを入力してログインし、学会（研修会）コードと学会（研修会）パスワードを入力します。

【施設連絡責任者権限】

自施設の情報変更等を行うことが出来ます。このアクセス権限は施設情報で施設連絡責任者に設定しておく必要があります。それ以外は会員権限と同一です。

ＪAMTＩＳでのアクセス方法は、会員番号とパスワードを入力しログインします。

【会員】

会員個人の情報変更および参照等を行うことが出来ます。

ＪAMTＩＳでのアクセス方法は、会員番号とパスワードを入力しログインします。

Ⅱ．ＪAMTＩＳのアクセスパスワードについて

【会員の場合】

パスワードは、会員全員に発行し送付します。

新規の会員には入会手続き終了後、会員証と一緒に封書で送付します。

パスワードはＪAMTＩＳ上で会員個人が変更できます。

会員資格を消失した場合はＪAMTＩＳページに入ることができません。

パスワードの問い合わせは､所定の用紙をより日臨技事務所に申請し､日臨技は封書で会員に送付します。

【職員の場合】

日臨技で登録後、職員番号とパスワードを封書で送付します。

パスワードと職員情報はＪAMTＩＳ上で職員個人が変更できます。

職員資格を消失した場合は、直ちに日臨技に連絡し、削除処理を行ってください。

パスワードの問い合わせは､所定の用紙により日臨技事務所に申請し､日臨技は封書で職員に送付します。

検査情報システムの安全管理に関するガイドライン

はじめに

高度情報通信社会の進展に伴い、インターネットを利用した情報公開は一般企業をはじめ、行政機関、医療機関にまで広がりをみせてきた。しかし、情報通信の進展にはリスクが存在し、機密情報、個人情報の漏えい、不正取引などの犯罪を生むこととなった。

そこで、個人情報を保護するための仕組みづくりが必要とされ「個人情報の保護に関する法律（個人情報保護法)」、「行政機関の保有する個人情報の保護に関する法律（行政機関個人情報保護法)」及び「独立行政法人等の保有する個人情報の保護に関する法律（独立行政法人等個人情報保護法)」が施行されるに至り、責任と権限、個人情報の収集・利用・管理方法、教育、監査の徹底などの明確化が求められるとともに、違反した場合の罰則規定等の整備も要求される。また平成 16 年 12 月には「医療・介護関連機関における個人情報保護に関するガイドライン」が公表された。

平成 16 年 11 月に成立した「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（以下 e-文書法）によって原則として法令等で作成または保存が義務付けられている書類は電子的に取り扱うことが可能となり、平成 17 年 3 月には情報システムの運用管理における法的責務および努力義務に関して「医療情報システムの安全管理に関するガイドライン」が公表されるに至った。

このような情勢の中、社団法人日本臨床衛生検査技師会として、検査室等で検討されなければならない検査室情報システムの安全管理事項として、情報技術の進歩・e-JAPAN 戦略 2004 を初めとする情報 IT 化の要請の高まりをふまえ「検査情報システムの安全管理に関するガイドライン」を作成することとした。

また、本ガイドラインは「検査室における個人情報保護ガイドライン」を補完ものであるが、個人情報保護は決して情報システムにかかわる対策だけで達成されるものではない。

検査室における個人情報保護ガイドラインを十分理解し、情報システムにかかわらない部分でも個人情報保護に関する対策が達成されていることを確認することが必要である。

さらに本ガイドラインは定期的に内容を見直す予定である。本ガイドラインを利用する場合は最新の版であることに十分留意されたい。

平成 17 年 9 月 23 日

社団法人　日本臨床衛生検査技師会

Ⅰ．ガイドライン策定の目的

本ガイドラインは、「個人情報の保護に関する法律」（平成 15 年法律第 57 号。以下「法」という。）に基づき、検査室における個人情報の適正な取扱いの基本的活動を確保するとともに、「医療情報システムの安全管理に関するガイドライン(厚生労働省)」に準拠した検査システムの安全管理確立に関する活動を支援するために定めるものである。

Ⅱ．ガイドラインの適用範囲

「医療情報システムの安全管理に関するガイドライン(厚生労働省)」が保存システムだけではなく、診療にかかわる情報を扱うすべての情報システムと、それらのシステムの導入、運用、利用、保守および廃棄にかかわる人または組織を対象としているのに対し、本ガイドラインは検査室情報処理システムに範囲を限定している。そのため、該当するシステムについては「医療情報システムの安全管理に関するガイドライン(厚生労働省)」が要求する事項に比べ、より詳細に多くの要求を掲載し、具体例を示している。

しかし、検査室の規模、要員数には差があり、本ガイドラインをすべて網羅することが必ずしも適切でない場合もありうる。

そこで、本ガイドラインを参考に検査室検査情報管理を行う場合は、自施設の現状を懸案し、適切な要求事項の選択をすることにより実効的なものとしていただきたい。

Ⅲ．参照

【法令】

- 個人情報の保護に関する法律(平成 15 年法律第 57 号)
- 憲法 20 条　「信条の自由」
- 刑法 35 条　「正等行為」、37 条「緊急避難」、134 条「秘密漏示」
- 労働安全衛生法 104 条　「健康診断に関する秘密の保持」
- 臨床検査技師、衛生検査技師等に関する法律 19 条「秘密を守る義務」

【規格】

- JIS Q 15001 :個人情報保護に関するコンプライアンス・プログラム(医療機関の認定指針)
- ISO 15189：臨床検査室-品質と能力に関する特定要求事項-
- JIS X 5080: :2002 情報技術－情報セキュリティマネジメントの実践のための規範
- TRQ0008:2003 リスクマネジメント－用語集－規格において使用するための指針

【ガイドライン】

- 医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン(厚生労働省)
- 医療情報システムの安全管理に関するガイドライン(厚生労働省)
- 診療録の外部保存に関するガイドライン（財団法人医療情報システム開発センター)
- 診療録の電子媒体による保存に関する解説書（財団法人医療情報システム開発センター)
- コンピュータウイルス対策基準(通商産業省)
- コンピュータ不正アクセス対策基準(通商産業省)
- 情報システム安全対策基準(通商産業省)
- 民間部門における電子商取引に係る個人情報の保護に関するガイドライン Ver2.0　（電子商取引推進協議会　平成 15 年 9 月）

Ⅳ．情報セキュリティ

Ⅳ－１．情報セキュリティとは

情報セキュリティとは、機密性・完全性・可用性を保護し維持することをいう。
機密性・完全性・可用性とは次のような意味を持つ。

機密性　：　アクセスを認可された者だけが、情報にアクセスできることを確実にすること。
完全性　：　情報および処理方法が正確であること及び完全であることを保護すること。
可用性　：　認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

さらに、厚生労働省から診療録等の電子媒体による保存についてはその対象文書等を明らかにするとともに、①真正性の確保、②見読性の確保、③保存性の確保の 3 つの基準(電子保存の 3 基準)を満たす場合には、電子媒体による保存を認めるとともに、その実施に際し、留意すべき事項を示した内容の通知が発出されている。

以下、厚生労働省発上記通知からの抜粋である。

① 真正性の確保

真正性とは、正当な人が記録し確認された情報に関し第三者から見て作成の責任の所在が明確であり、かつ、故意または過失による、虚偽入力、書き換え、消去、及び混同が防止されていることである。

なお、混同とは、患者を取り違えた記録がなされたり、記録された情報間での関連性を誤ったりすることをいう。

制度上の要求事項に対する対応は運用面と技術面の両方で行う必要がある。運用面、技術面のどちらかに偏重すると高コストの割に要求事項が充分満たされない事が想定され、両者のバランスが取れた総合的な対策が重要と考えられる。各医療機関等は、自機関の規模や各部門システム、既存システムの特性を良く見極めた上で、最も効果的に要求を満たす運用面と技術面の対応を検討されたい。

② 見読性の確保

電子媒体に保存された内容を、権限保有者からの要求に基づき必要に応じて肉眼で見読可能な状態にできること。必要に応じてとは、「診療」、「患者への説明」、「監査」、「訴訟」等に際して、それぞれの目的に支障のない応答時間やスループットと、操作方法でということである。特に監査の場合においては、監査対象の情報の内容を直ちに書面に表示できることが求められている。

電子媒体に保存された情報は、そのままでは見読できず、また複数媒体に分かれて記録された情報の相互関係もそのままでは判りにくい。また、その電子媒体から情報を取り出すには何らかのアプリケーションが必要であり、表示のための編集前提となるマスタ、利用者テーブル等が別に存在したりする可能性がある。これらの見読化手段が日常的に正常に動作することが求められる。

また、必要な情報を必要なタイミングで正当な情報利用者に提供できなかったり、記録時と異なる内容で表示されたりすることは、重大な支障となるので、それを防ぐためのシステム全般の保護対策が必要であるが、見読性の観点では、何らかのシステム障害が発生した場合においても診療に重大な支障が無い最低限の見読性を確保するための対策が必要である。

さらに、「診療」、「患者への説明」時に求められる見読性は、主治医等の医療従事者に対して保障されるべきものであり、緊急時等においても、医療従事者が診療録等を閲覧するために、必ず医療従事者以外の許可を求める必要がある等の制約はあってはならない。

③ 保存性の確保

保存性とは、記録された情報が法令等で定められた期間に渡って真正性を保ち、見読可能にできる状態で保存されることをいう。

診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、下記のものが考えられる。

- ウイルスや不適切なソフトウェア等による情報の破壊及び混同等
- 不適切な保管・取扱いによる情報の滅失、破壊
- 記録媒体、設備の劣化による読み取り不能または不完全な読み取り
- 媒体・機器・ソフトウェアの整合性不備による復元不能

これらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。

Ⅳ－２．組織体制

検査室が保有する情報システム及び個人情報に関する安全管理(以下安全管理)について、従業者の責任と権限を明確に定め､安全管理に関する規程や手順書を整備運用し､その実施状況を確認しなければならない。これは検査室内で情報システムを利用するかどうかにかかわらず遵守すべき事項である。組織的安全管理対策には以下の事項が含まれる。

（1）安全管理対策を講じるための組織体制の整備

① 情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。

② 検査室には，コンピュータの機能不全について直ちに報告を受ける責任者を任命しておくこと。

③ 内部又は外部の助言者から専門家による情報セキュリティの助言を求め、検査室全体を調整すること。

＊　ただし小規模施設などにおいて役割が自明の場合は、明確な規程を定めなくとも良い。

（2）安全管理対策を定める規程等の整備と規程等に従った運用

① 管理責任や説明責任を果たすために運用管理規程はきわめて重要であり、必ず定めなければならない。運用管理規程には必ず以下の項目を含めること。

- 理念
- 検査室内の体制、外部保存に関わる院外の人および施設
- 契約書・マニュアル等の文書の管理
- 機器を用いる場合は機器の管理
- 患者等への説明と同意を得る方法
- 監査
- 苦情の受け付け窓口

② 個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限するなどの入退管理を定めること。

③ 情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。
運用管理規程等において下記の内容を定めること。
(a) 個人情報の記録媒体の管理（保管・授受等）の方法について定めた規程
(b) リスクに対する予防、発生時の対応の方法

④ 個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。

（3）医療情報取扱い台帳の整備

① 検査室が保有する情報システムそれぞれに関連づけて登録情報の目録を作成し、維持すること。

② 情報の分類及び関連する保護管理策では、情報を共有又は制限する業務上の必要、及びこのような必要から起こる業務上の影響を考慮に入れておくこと。

（4）他部署との連携

検査室情報処理システムは、病院等のシステムの一部であることが多く、他部署との連携を取る必要がある。

部署間の情報及びソフトウェアの交換(電子的又は人手によるもの)については、場合によっては正式な契約として、合意を取り交わすことが必要である。

（5）医療情報の安全管理対策の評価、見直し及び改善

定期的内部監査を実施し、管理者によるレビューを行い、是正処置、予防処置を講じると共に、検査室情報安全管理策の有効性を継続的に改善することが重要である。

（6）事故又は違反への対処

セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処を確実に行うために、事件・事故管理の責任及び手順を確立すること。

Ⅳ－３．人的セキュリティ

人的セキュリティの安全性を高めるため、従業者による誤り、盗難、不正行為、誤用を軽減するための事前措置が重要である。

（1）従業者に対する人的安全管理

検査室管理者は、個人情報に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。

① 医療従事者以外の事務職員の採用にあたっては、雇用及び契約時に守秘・非開示契約を締結することなどにより安全管理を行うこと。

② セキュリティの役割及び責任は、組織の情報セキュリティ基本方針で定められたとおりに、職務定義の中に文書化し、セキュリティを職責に含めること。

③ 定期的に従業者に対し教育訓練を行うこと。

情報セキュリティの脅威及び懸念に対する従業者の認識を確実なものとし、通常の仕事の中で従業者が組織のセキュリティ基本方針を維持していくために、組織の基本方針及び手順について適切な教育を行うこと、並びに定期的に更新教育を行うこと。

④ 従業者の退職後の個人情報保護規程を定めること。

⑤ サーバ室などの管理上重要な場所では、可能であればモニタリング等により従業者に対する行動の管理を行うことが望ましい。

⑥ すべての従業者は、新しいシステムの使用法，又は古いシステムの改変について教育を受けることが望ましい。

（2）事務取扱委託業者の監督及び守秘義務契約

外部受託業者を採用する場合は、施設内における適切な個人情報保護が行われるように、以下のような措置を行うこと。

① 委託先との守秘契約を締結すること。

② 保守作業など電子保存システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。

③ 清掃など、直接電子保存システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。

④ 委託先事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託先と同等の個人情報保護に関する対策および契約がなされていることを条件とすること。

⑤ プログラムの異常等で、保存データを救済する必要があるときなど、やむをえない事情で外部の保守要員が検査結果等の個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。

Ⅳ－４．物理的・環境的セキュリティ

物理的安全対策とは、情報システムにおいて個人情報が格納される、コンピュータ、情報媒体等を物理的な方法によって保護することである。具体的には以下の事項を考慮する必要がある。

（1）個人情報の物理的保存を行っている区画への入退管理を実施すること。

① 検査室全体が個人情報保護区画であると考えられ、適切な入退管理策によってセキュリティを保護すること。

② 入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録し、入退者

の記録を定期的にチェックを行うことで、妥当性を確認すること。

（2）盗難、窃視等の防止
① 個人情報が存在するPCなど重要な機器に盗難防止用チェーンを設置すること。組織に属する装置、情報又はソフトウェアの持ち出しに際しては、管理者による認可を必要とし、組織の敷地外で情報処理のために装置を使用するいかなる場合も、管理者による認可を要求すること。
② 離席時にも端末等での正当な権限者以外の者による窃視防止の対策を実施すること。
③ 可能であれば、防犯カメラ、自動侵入監視装置等を設置すること。

（3）機器・装置・情報媒体等の物理的な保護
① コンピュータの取外し可能な付属媒体(例えば、テープ、ディスク、カセット)及び印刷された文書を管理し、媒体が不要となった場合は、安全、かつ、確実に処分すること。
② 組織間の情報及びソフトウェアの交換(電子的又は人手によるもの)については、ある場合には正式な契約として、合意を取り交わすこと。

環境的要件としては、最低限以下の事項を考慮すること。

（1）コンピュータ設備及び装置は、清潔で保全が十分であり、製造者の仕様に合う場所及び環境に設置されること。
（2）コンピュータコンポネート及びその保管場所は、適切な防火用具を容易に利用できること。
（3）線類又はコンピュータケーブルが通路上にある場合は、保護されること。
（4）電源の多重化、無停電電源装置（UPS)、非常用発電機等の電力の供給が途切れないための対策がなされていること。

Ⅳ－５．アクセス制御

技術的な対策のみで全ての脅威に対抗できる保証はなく、一般的には運用管理による対策との併用は必須である。しかし、その有効範囲を認識し適切な適用を行えば、これらは強力な手段となりうる。
不正なアクセスを防止するため、利用者へのアクセス権限の登録から登録抹消までの手順が文書化され、整っていなければならない。
また、特権管理、パスワードの扱い、権限の変更管理についても記載されていること。

（1）利用者の識別および認証
ID、パスワード等により、診療録データへのアクセスにおける識別と認証を行うこと。
以下のような行為により、本人の識別、認証に用いられる情報が第三者に漏れないように防止策を取らなければならない。
① ID/パスワードが書かれた紙などが貼られていて、第三者が簡単に知ることができてしまう。
② パスワードが設定されておらず、誰でもシステムにログインできてしまう。
③ 代行作業等のためにパスワードを他人に教えており、システムで保存される作業履歴から作業者が特定できない。
④ 容易に推測できる、あるいは、文字数の少ないパスワードが設定されており、容易にパスワードが推測できてしまう。
⑤ パスワードを定期的に変更せずに使用しているために、パスワードが推測される可能性が高くなっている。
⑥ 認証用の個人識別情報を格納するトークン（IC カード、USB キー等）を他人に貸与する、または持ち主に無断で借用することにより、利用者が特定できない。
⑦ 退職した職員のIDが有効になったままで、ログインができてしまう。
⑧ 医療情報部等で、印刷放置されている帳票などから、パスワードが盗まれる。

⑨　コンピュータウイルスにより、システムの ID とパスワードが盗まれ、悪用される。

具体的パスワード管理対策としては、

①　個人のパスワードを取得する際、パスワード等に関する秘密保持宣言書への署名を求める。
②　パスワードを紙に記録して保管しない。ただし、記録がセキュリティを確保して保管される場合は、その限りではない。
③　システム又はパスワードに対する危険な兆候が見られる場合は、パスワードを変更する。
④　パスワードに当人の関連情報(名前、生年月日、電話番号、職番など)を使用しない。
⑤　パスワードは定期的に、又はアクセス回数に応じて変更する。この際、古いパスワードの再利用や循環利用しないこと。
⑥　自動ログオン処理にパスワードを含めない。
⑦　個人用パスワードを共有しない。

などが考えられる。

さらに、アクセス制御の方法として「端末のログオン手順」が JIS X 5080:2002 に詳細な記述があるので以下に掲載する。

【端末のログオン手順(JIS X 5080:2002)】

a)システム又は業務用ソフトウェアの識別子を、ログオン手続きが無事完了するまで表示しない。
b)コンピュータへのアクセスは認可されている利用者に限定されるという警告を表示する。
c) ログオン手順に、認可されていない利用者の助けとなる表示をしない。
d)ログオン情報の妥当性検証は、すべての入力データが完了した時点でだけ行なう。誤り条件が発生しても、システムからは、データのどの部分が正しいか又は間違っているかを指摘しない。
e)許容されるログオンの試みの失敗回数を制限し（推奨は三回）、次の事柄を考慮する。
　1)　失敗した試みを記録すること。
　2)　次のログオンの試みが可能となるまでの間に意図的な時間をおくこと、又は特別な認可なしに行われる次回の試みを拒否すること。
　3)　データリンク接続を切ること。
f) ログオン手順のために許容される最長及び最短時間を制限する。この制限から外れる場合、システムはログオンを終了する。
g)ログオンが無事できた時点で、次の情報を表示する。
　1)　前回ログオンが無事できた日時
　2)　前回ログオン以降、失敗したログオンの試みがある場合は、その詳細。

（2）アクセス権限の管理

情報システムの利用に際しては、組織における利用者や利用者グループ（業務単位など）ごと、情報ごとに利用権限を規定する必要がある。ここで重要なことは、付与する利用権限を必要最小限にすることである。知る必要のない情報は知らせず、必要のない権限は付与しないことでリスクが低減される。情報システムに、参照、更新、実行、追加などのようにきめ細かな権限の設定を行う機能があれば、さらにリスクは低減される。

アクセス権限の見直しは、人事異動等による利用者の担当業務の変更やなどに合わせて適宜行う必要があり、組織の規程で定められていなければならない。

具体的アクセス権限の管理対策としては、

①　アクセス権を定期的に、また、何らかの変更があった時点で見直す。
②　特権的アクセス権は、一般的アクセス権に比べ頻繁に見直す。
③　特権の割当てを定期的に検査して、認可されていない特権が取得されていないかを確認する。

などが考えられる。

（3）アクセスの記録（アクセスログ）

個人情報を含む資源については、全てのアクセスの記録（アクセスログ）を収集し、定期的にその内容をチェックして不正利用がないことを確認しなければならない。

アクセスログは、それ自体に個人情報が含まれている可能性があること、さらにはセキュリティ事故が発生した際の調査に非常に有効な情報であるため、その保護は必須である。したがって、アクセスログへのアクセス制限を行い、削除／改ざん／追加等を防止する対策を講じなければならない。

また、アクセスログの証拠性確保のためには、記録する時刻は重要である。精度の高いものを使用し、検査室内の全てのシステムで同期をとらねばならない。

アクセスログには次の事項を含める。

① 利用者ＩＤ
② ログオン、ログオフの日時
③ 使用端末のＩＤ
④ システムへのアクセスに成功及び失敗した記録
⑤ データ、他の資源へのアクセスに成功した及び失敗した記録

（4）不正ソフトウェア対策

外部との通信を遮断し、ＦＤ、ＣＤドライブ、ＵＳＢ等を使用不能にした完全に独立した情報システムでないかぎり、常にウイルス、ワーム、トロイの木馬などと呼ばれる様々な形態を持つ不正ソフトウェアの脅威にさらされている。

利用者には、無認可又は悪意のあるソフトウェアの危険を知らせることが重要である。

対応策としては、以下のことが考えられる。

① 無許可のソフトウェアのインストール及び使用を禁止する。
② 外部ネットワークからのファイルやソフトウェアのダウンロードを禁止する。
③ ウイルス検出ソフト及び修復ソフトの導入及び定期的更新。
④ オペレーティング・システム等でセキュリティ・ホールの報告されているものについては、対応版（セキュリティ・パッチと呼ばれるもの）への逐次更新を実施する。
⑤ 利用していないサービスや通信ポートの非活性化、マクロ実行の抑制などを行う。

コンピュータウイルス対策基準：平成 12 年 12 月 28 日（通商産業省告示 第 952 号）（最終改定）では、コンピュータウイルス（以下「ウイルス」とする。）を以下と定義している。

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

① 自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

② 潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

③ 発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能、さらに、コンピュータウイルス対策基準では、システムユーザが実施すべき対策基準として以下を挙げている。

a. ソフトウェア管理

① ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。
② オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。

b. 運用管理

① 外部より入手したファイル及び共用するファイル媒体は、ウイルス検査後に利用すること。
② ウイルス感染の被害が最小となるよう、システムの利用は、いったん初期状態にしてから行うこと。
③ ウイルス感染を早期に発見するため、システムの動作の変化に注意すること。

④ ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。
⑤ 不正アクセスによるウイルス被害を防止するため、パスワードは容易に推測されないように設定し、その秘密を保つこと。
⑥ 不正アクセスによるウイルス被害を防止するため、パスワードは随時変更すること。
⑦ 不正アクセスによるウイルス被害を防止するため、システムのユーザＩＤを共用しないこと。
⑧ 不正アクセスによるウイルス被害を防止するため、アクセス履歴を確認すること。
⑨ 不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。
⑩ システムを悪用されないため、入力待ちの状態で放置しないこと。
⑪ ウイルス感染を防止するため、出所不明のソフトウェアは利用しないこと。
⑫ ウイルスの被害に備えるため、ファイルのバックアップを定期的に行い、一定期間保管すること。

c. 事後対応
① ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。
② ウイルス被害の拡大を防止するため、システムの復旧は、システム管理者の指示に従うこと。
③ ウイルス被害の拡大を防止するため、感染したプログラムを含むフロッピーディスク等は破棄すること。

d. 監査
① ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

【最低限の遵守事項】
- コンピュータプログラムは、偶発的な又は権限を与えられていない者による変更又は破壊から適切に保護されていること。
- コンピュータシステムの使用権限付与について厳正な方針が定められていること。方針には患者データにアクセスする権限のある者、及び患者の検査結果の入力、結果の変更、請求書の変更、又はコンピュータプログラムの改訂について権限を与えられたコンピュータ使用者について定めることが望ましい。
- 他のコンピュータシステム中のデータ（例えば，薬局又は診療録）が検査室システムを通してアクセスできる場合には、権限を与えられていない者が検査室システムを通してこれらのデータをアクセスすることを防ぐのに適切なコンピュータセキュリティ対策があること。検査室システムは他のシステムのデータを危機にさらすべきではない。

Ⅳ－６．保守

（1）システムの維持管理

極めて重要な業務情報及びソフトウェアのバックアップは定期的に取得し、緊急使用時のための信頼性確保のために、可能であれば検査することが望ましい。災害又は媒体故障が発生した場合、重要な業務情報及びソフトウェアができるようなバックアップ設備を整える必要があり、手順を明確にし、定期的に検査及び試験を実施することが望ましい。

運用担当者は、自分の作業の記録を継続し、運用担当者の記録は、定期的に独立した検査を受けること。

（2）ネットワーク管理

ネットワークにおけるセキュリティを実現し、かつ、維持するために一連の管理策として以下の項目を実施すること。
① ネットワークの運用責任とコンピュータの操作作業とは分離することが望ましい。
② ネットワークサービスの可用性及び接続したコンピュータの可用性を維持すること。
③ 管理策は、検査室全体について統一した管理策を用いること。

【保守管理の具体例】

・　メンテナンスのための「ダウンタイム」は、患者診療サービスの中断を最低限にするよう計画されること。
・　データの完全性、中断のない検査室のサービス、及び再起動後にシステムが機能していることを確実にするために、システム全体又は一部のシャットダウン及び再起動の操作について文書化した手順があること。
・　患者データの完全性を確実にするために、病院情報システムのような他のシステムのダウンタイム時の処理手順があることが望ましい。他のシステムの回復及びデータファイルの交換やアップデートを検証する手順があること。
・　計画になかったすべてのコンピュータダウンタイム、システムの機能低下の期間（応答時間）、その他のコンピュータの問題発生に関して、機能不全の理由及び是正処置を含めて文書化すること。
・　患者結果が迅速に有用な形で報告されないようなコンピュータシステムの故障が生じた場合のサービスの取扱いについて明文化した緊急対策プランを開発すること。
・　定期的保全を文書化した記録を維持し、それによりコンピュータシステムに施したあらゆる作業をオペレータが追跡できるようにすること。
・　コンピュータが正しく作動していることを確実にするために、コンピュータ警報システム（一般的にハードウェア及びソフトウェアの作動を監視するメインのコンピュータコンソール）を監視し、定期的にテストすること。
・　すべてのコンピュータハードウェアについて、すべての予防保全について記載された手順及び全体の記録が容易に利用できること。
・　バックアップ及び（又は）データファイルの復旧を実施するごとに不注意による変更が起こらなかったことを確実にするためにシステムをチェックすること。
・　システムのバックアップの間に検出された間違いは、実施した是正処置とともに文書化し、検査室内の責任者に報告されること。
・　システムのハードウェア及びソフトウェアに対するあらゆる変更が満足で適切であることを確実なものとするために、変更を検証し、確認し、かつ完全に文書化すること。
・　プログラムの目的、その機能の仕方、他のプログラムとの相互作用について明確に記述されることが望ましい。適用できる場合は、コンピュータのオペレータによる故障対策、システムの改変、プログラミングを支援するのに適切な程度に詳細であること。
・　最初に設置したときと変更又は修正を行ったときは、プログラムの適正な性能についてチェックすること。

Ⅳ－７．データの保護と内部保存管理

(1) 電子保存の 3 基準の遵守
① 真正性の確保
② 見読性の確保
③ 保存性の確保
の 3 つの基準(電子保存の 3 基準)を満たす必要がある。

(2) データの保護
① 報告書及び画面上の患者データは、決められた間隔でオリジナル入力と比較し、データ伝送、保存、手順の間違いを検出すること。
② 最終的な承認及びコンピュータにより報告される前に、手動で又は自動的にコンピュータシステムに入力されたデータを見直し、その正確さを検証すること。
③ 患者データ、管理ファイル、コンピュータプログラムの入力又は修正を行ったすべての個人を検査室が特定できること。

(3) 内部保存管理
① 保存された患者の検査結果データ及び文書記録情報は、患者診療のニーズに合う時間枠内に容易に、

迅速に検索できること。

② コンピュータは、検査が実施されたときの生物学的基準範囲、及び結果に付記されていたすべてのフラグ、脚注、解釈に関するコメント並びに測定の不確かさを含め、保管されている検査結果を完全に復元できること。

③ テープ、ディスクなどのようなデータ保存媒体は、正しくラベルを付して保存し、破損や無許可の使用から保護されること。

④ ハードウェア又はソフトウェアの異常が生じた場合に患者データが消失することを防ぐために効果的なバックアップが実施されていること。

Ⅳ－８．外部保存管理

(1) 委託先の選定と契約

検査室が情報処理を委託する、検査外注などのために個人情報を預託する場合は、委託運用管理規程を定め実施し、委託先選定に当っては十分な個人情報の保護水準を満たしているものを選定しなければならない。

さらに、外部委託によるサービスを利用する前に、そのリスクを識別し、適切な管理策を請負業者の同意を得て契約に組み入れることが重要であり、次に示す内容を規定することで、その保護水準を担保しなければならない。

a) 法的な要求事項をどのように満たすか。
b) 個人情報に関する秘密保持。
c) 再委託に関する事項について。
d) 災害時のサービス継続方法
e) 事故時の責任分担。
f) 契約終了時の個人情報の返却及び消去。
g) 監査する権利

(2) 電子保存の 3 基準の遵守

① 真正性の確保
② 見読性の確保
③ 保存性の確保

の 3 つの基準(電子保存の 3 基準)を満たす必要がある。

(3) 電気通信回線を通じた保存

電気通信回線を通じた医療機関等以外の場所での外部保存については、システム堅牢性の高い安全な情報の保存場所の確保によるセキュリティ対策の向上や災害時の危機管理の推進、保存コストの削減等が期待できる。

一方、患者等の情報が瞬時に大量に漏洩する危険性がある反面、漏洩した場所や責任者の特定が困難であり、検査室等の責任が相対的に大きくなる。

従って、外注検査業者を含め、個人情報や検査結果が外部で保存される場合は、法令上の保存義務を有する保存主体の検査室等が、保存受託者に対して安全管理上の体制を確保した上で、電子保存された検査結果等を必要時に直ちに利用できるように管理し、患者に対する保健医療サービス等の提供に当該情報を利活用するための責任を果たせることを前提とするべきである。

(4) 可搬型媒体による保存

可搬型媒体に電子的に保存した情報を外部に保存する場合、委託元の検査室等と受託先の機関はオンラインで結ばれていないために、なりすましや盗聴、改ざん等による情報の大量漏洩や大幅な書換え等、電気通信回線上の脅威に基づく危険性は少なく、注意深く運用すれば真正性の確保は容易になる可能性がある。

可搬型媒体による保存の安全性は、紙や超音波診断写真等による保存の安全性と比べておおむね優れてい

るといえる。媒体を目視しても内容が見えるわけではないので、搬送時の機密性は比較的確保しやすい。さらに、セキュリティMO 等のパスワードによるアクセス制限が可能な媒体を用いればさらに機密性は増す。

従って、一般的には次節の紙媒体による外部保存の基準に準拠していれば大きな問題はないと考えられる。しかしながら、可搬型媒体の耐久性の経年変化については、今後とも慎重に対応していく必要があり、また、媒体あたりに保存される情報量が極めて多いことから、媒体が遺失した場合に、紛失、漏洩する情報量も多くなるため、より慎重な取扱いが必要と考えられる。

なお、検査結果等のバックアップ、法令で定められている保存義務を伴わない文書を外部に保存する場合についても、個人情報保護の観点からは保存義務のある文書と同等に扱うべきである。

⑸　紙媒体での保存

紙媒体とは、紙だけを指すのではなく、超音波診断写真等の電子媒体ではない物理媒体も含む。検査技術の進歩等によって、医療機関等で保存しなければならない診療録等が増加しており、その保存場所の確保が困難な場合も多い。

一定の条件の下では、従来の紙媒体のままの検査結果等を当該医療機関等以外の場所に保存することが可能になっているが、検査結果等は機密性の高い個人情報を含んでおり、また必要な時に遅滞なく利用できる必要がある。保存場所が当該医療機関等以外になることは、個人情報が存在する場所が拡大することになり、外部保存に係る運用管理体制を明確にしておく必要がある。

また保存場所が離れるほど、検査結果等を搬送して利用可能な状態にするのに時間がかかるのは当然であり、診療に差し障りのないように配慮しなければならない。

さらに、紙や超音波診断写真等の搬送は注意深く行う必要がある。可搬型媒体は内容を見るために何らかの装置を必要とするが、紙や超音波診断写真等は単に露出するだけで、個人情報が容易に漏出するからである。

Ⅳ－９．操作マニュアル・手順書等

権限を与えられたすべての使用者が完全なコンピュータ操作マニュアルを容易に利用できる必要があり、管理者は検査室のコンピュータ操作マニュアルを定められた期間ごとに見直し、承認することが必要である。

また、災害が発生した場合にデータ、コンピュータ装置を保護するために実施すべき処置について記述した手順を作成するべきである。

データテーブルの複製がシステムに数多く保存されている場合（例えば、検査室情報システムと病院情報システムの両方に存在する生物学的基準範囲に関する表）には、使用されているすべての複製を定期的に比較し、適切な複製であるか確認する必要があり、比較に関する手順を作成しておくこと必要がある。

さらに、検査室情報システムを安全な状態で運用するためには、運用の変更に関する管理が重要である。操作手順やソフトウェアの変更は、業務全体に対して影響を及ぼし、不測の事態を引き起こしかねない。そのため、あらかじめ変更のための手順やその責任者を定めておくべきである。

Ⅳ－１０．改善

⑴　継続的改善

検査室は、情報セキュリティ基本方針、情報セキュリティ目標、監査結果、監視した事象の分析、是正処置、予防処置及び管理者によるレビューを通じて、検査室情報安全管理策の有効性を継続的に改善することが重要である。

⑵　是正処置

検査室は、再発防止のため、検査室情報安全管理策の導入及び運用に関連する不適合の原因を除去するための処置を講ずる必要がある。

是正処置に関する文書化された手順では、次の事項に関する要求事項を規定すべきである。

・　検査室情報安全管理策の導入及び運用における不適合の識別。

- 不適合の原因の特定。
- 不適合の再発防止を確実にするための処置の必要性の評価。
- 必要な是正処置の決定及び実施。
- 実施した処置の結果の記録と保存。
- 実施した是正処置のレビュー。

(3) 予防処置

検査室は、不適合の発生を未然に防ぐための処置を決めること。予防処置は、起こり得る問題の影響に見合ったものである必要がある。不適合を予防するための処置は、多くの場合、是正処置よりも費用対効果が高く有用である。

予防処置に関する文書化された手順では、次の事項に関する要求事項を規定すること。

- 起こり得る不適合及び原因の識別。
- 必要な予防処置の決定及び実施。
- 実施した処置の結果の記録と保存。
- 実施した予防処置のレビュー。
- 変化したリスクの識別及び大きく変化したリスクに対して確実に注意が払われるようにすること。

予防処置の優先順位については、リスクアセスメントの結果に基づいて決定すること。

Ⅴ．本ガイドラインの見直し等

個人情報保護法は、施行後 3 年を目途として、法の試行状況について検討を加え、その結果に基づいて必要な処置を講ずる。また、両院付帯決議においては医療に関する個別法の作成が挙げられている。この様な状況において個人情報の取扱い方法をより明確化し、適切な取扱いを推進するためには、本ガイドラインに対する対応例等の情報を集積し、こうした情報に基づき見直しを行っていく必要がある。

また、本ガイドラインは技術的な記載の陳腐化を避けるために定期的に内容を見直す予定であり、日本医師会、対がん協会をはじめとする各医療関連団体、関連学会との整合性を図るため常時見直しを図ることとともに、必要に応じ全般に関して検討を加えた上で、改正を行うものとする。

【 参考資料 】

【　安全な医療を提供するための 10 の要点　】

安全な医療を提供するための10 の要点

（1）根づかせよう安全文化 みんなの努力と活かすシステム
（2）安全高める患者の参加 対話が深める互いの理解
（3）共有しよう 私の経験 活用しよう あなたの教訓
（4）規則と手順 決めて 守って 見直して
（5）部門の壁を乗り越えて 意見かわせる 職場をつくろう
（6）先の危険を考えて 要点おさえて しっかり確認
（7）自分自身の健康管理 医療人の第一歩
（8）事故予防 技術と工夫も取り入れて
（9）患者と薬を再確認 用法・用量 気をつけて
(10) 整えよう療養環境 つくりあげよう作業環境

（厚生労働省）

以下に、厚生労働省医政局　医療安全対策検討会議ヒューマンエラー部会が、平成 13 年９月 11 日に策定した、『安全な医療を提供するための 10 の要点』を、「解説」と「具体的な取組に向けて」も含めて、付録として提示する。

本要点策定の趣旨は、安全な医療サービスを提供することは、医療の最も基本的な要件であり、このために、医療安全に関する意識の啓発と、これを推進する組織体制の構築が求められている。そこで、基本的な考え方を標語形式でとりまとめ、それぞれの医療機関が、その特性に応じてより具体的な標語を作成する工夫を望むものである。と謳われている。

また、策定方針は以下の 3 点である。

Ⅰ　全ての職員対象
Ⅱ　安全確保の基本理念をわかりやすく覚えやすい簡潔に表現
Ⅲ　その医療機関の特性に応じた独自の標語を作成できるよう、「解説」と「具体的な取組に向けて」を記載

策定方法としては各種調査を行い、重要な分野と項目を検討することにある。重要な分野としては①理念、②患者との関係、③組織的取組、④職員間の関係、⑤職員個人、⑥人と環境モノとの関係、の 6 分野を取り上げ、これらに特に重要な 10 の項目を標語としてまとめたものである。

1　根づかせよう安全文化　みんなの努力と活かすシステム

解　説

○　医療において患者を最優先させることは、古くから医療人の基本的な行動規範とされてきました。
○　今日、患者の安全は何よりもまず優先されるべきであることを再認識し、医療に安全文化を根づかせていくことが必要です。
○　医療における安全文化とは、医療に従事する全ての職員が、患者の安全を最優先に考え、その実現を目指す態度や考え方およびそれを可能にする組織のあり方と言えるでしょう。
○　なお、安全文化という言葉は、他の分野では「安全性に関する問題を最優先にし、その重要性に応じた配慮を行う組織や個人の特性や姿勢の総体」（国際原子力機関 1991 年）という意味で用いられています。
○　人は間違えうることを前提として、システムを構築し機能させていくことが必要です。

【具体的な取組に向けて】
○　全ての職員は、安全を最優先に考えて業務に取り組みましょう。
○　安全に関する知識や技術を常に学び向上することを心がけましょう。
○　管理者のリーダーシップの発揮、委員会やリスクマネジャーの設置、教育訓練の充実といった事故予防のための体制づくりに取り組みましょう。
○　業務の流れを点検し、個人の間違いが重大な事故に結びつかないようにする「フェイルセーフ」のしくみの構築に努めましょう。

2　安全高める患者の参加　対話が深める互いの理解

解　説
○　医療は患者のために行うものです。その主役である患者が医療に参加することが重要です。
○　このことは安全に医療を提供していくためにも大切です。
○　患者と職員との対話によって､医療内容に対する患者の理解が進むとともに､相互の理解がより深まります。

【具体的な取組に向けて】
○　医療内容について十分に説明しましょう。
○　日々の診療の場で、その内容や予定について説明しましょう。
○　一方的な説明ではなく、患者との対話を心がけましょう。
○　患者が質問や考えを伝えやすい雰囲気をつくりあげましょう。

3　共有しよう　私の経験　活用しよう　あなたの教訓

解　説
○　ミスが起こる要因はある程度共通していることから、その要因を明らかにし改善していくことが必要です。
○　職員の経験を収集し、原因分析に基づいて改善策を導き出し、それを共有することが不可欠です。
○　効果的な安全対策を講じるためには、個人の責任を追及するのではなく、システムの問題ととらえ改善していく「問題解決型」の取組が必要です。
○　他産業の安全対策に関する知見を、医療における安全対策に活用することも有効です。

【具体的な取組に向けて】
○　すべての職員は、積極的に報告システムに参加しましょう。
○　報告された事例の原因を分析しましょう。
○　得られた改善策は職員全員で学び、実践しましょう。

4　規則と手順　決めて　守って　見直して

解　説
○　規則や手順は、現実的かつ合理的なものを、職員自らが考え話し合いながら文書として作り上げることが必要です。さらにそれらは、必ず守らなければなりません。
○　問題点や不都合な点が見つかった時には躊躇なく改善することが必要です。その際、あらかじめ関係する部門同士がよく調整することが必要です。
○　規則や手順、各種用紙の書式などを統一することも、ミスを減らす上では大切です。

【具体的な取組に向けて】
○　規則や手順を文書として整備し、遵守しましょう。
○　必要なときには積極的に改善提案し、見直しましょう。
○　見直しの際には関係者とよく話し合いましょう

５　部門の壁を乗り越えて　意見かわせる　職場をつくろう

解　説

○　医療においては多様な職種や部門が存在し、チームで医療を行っています。
○　安全な医療の提供のためには、部門・職種の違いや職制上の関係を問わず、相互に意見を交わしあうことが重要です。
○　特にチーム内では、お互いが指摘し、協力しあえる関係にあることが不可欠と言えます。
○　思い込みや過信は誰にでも起こりうるもので、自分では気がつきにくいものです。他人の目により互いに注意しあうことは、思い込みや過信の訂正にも有効です。
○　なお、ひとりの患者に複数の施設がかかわる場合には、外部の組織とのコミュニケーションも重要です。

【具体的な取組に向けて】

○　気づいたらお互いに率直に意見を伝え、周りの意見には謙虚に耳を傾けましょう。
○　上司や先輩から率先してオープンな職場づくりを心がけましょう。
○　関係する他施設等とのコミュニケーションにも努めましょう。

６　先の危険を考えて　要点押さえて　しっかり確認

解　説

○　確認は、医療の安全を確保するために最も重要な行為です。
○　ただし、漫然と確認するのではなく、業務分析を行い、確認すべき点を明らかにした上で、要点を押さえて行うことが重要です。
○　正しい知識を学び、的確な患者の観察や医療内容の理解により起こりうる危険を見通すことで、事故を未然に防ぐことができます。
○「いつもと違う」と感じた場合には、危険が潜んでいることがあるため注意が必要です。

【具体的な取組に向けて】

○　決められた確認をしっかり行いましょう。
○　早期に危険を見つけるために、正しい知識を身につけましょう。
○「何か変」と感じる感性を大切にしましょう。

７　自分自身の健康管理　医療人の第一歩

解　説

○　安全な医療を提供するためには、自らの健康や生活を管理することが必要であり、このことは医療人としての基本です。
○　自己管理を行うためには、自分の体調を常に把握しておくことが必要です。

【具体的な取組に向けて】

○　次の業務に備えて、健康管理や生活管理を心がけましょう。
○　リーダーはメンバーの体調や健康状態にも配慮しましょう。

８　事故予防　技術と工夫も取り入れて

解　説

○　安全確保のための取組を人間の力だけで行うには限界があります。このため、積極的に技術を活用することで、人的ミスの発生を減らすことができます。

○　特に、近年発達を遂げている情報技術の活用は医療安全を推進するための手段の一つです。
○　一つのミスが全体の安全を損なわないよう十分配慮され、操作性にも優れた機器や器具などを使うことが大切です（フェイルセーフ技術の活用やユーザビリティへの配慮）。
○　機器や器具などに関する医療現場の意見や創意工夫も安全確保のために重要です。

【具体的な取組に向けて】
○　機器や器具などの購入や採用にあたっては、安全面や操作性に優れたものを選定しましょう。
○　機器や器具などに改善すべき点があれば、関係者に対して積極的な改善提案を行いましょう。

9　患者と薬を再確認　用法・用量　気をつけて

解　説
○　医薬品に関するミスは、医療事故の中で最も多いと言われています。
○　誤薬を防ぐために、医薬品に関する「５つのＲ」に注意することが必要です。５つのＲ（Right＝正しい）とは、「正しい患者」、「正しい薬剤名」、「正しい量」、「正しい投与経路」、「正しい時間」を指します。

【具体的な取組に向けて】
○　処方箋や伝票などは読みやすい字で書き、疑問や不明な点があれば必ず確認しましょう。
○　患者誤認防止のため、与薬時の患者確認は特に注意して行いましょう。
○　類似した名称や形態の薬には特に注意しましょう。

10　整えよう療養環境　つくりあげよう作業環境

解　説
○　療養環境の整備は、患者の快適性の観点からだけでなく、転倒・転落等の事故予防の観点からも重要です。
○　作業環境の整備も、手順のミスを防ぐなど、事故防止につながります。
○　なお、作業する場所だけでなく、記録や医療機器等も作業環境の一環として整備する必要があります。
○　医療機器等はその特性をよく理解し、安全に使用することが必要です。

【具体的な取組に向けて】
○　施設内の整理・整頓・清潔・清掃に取り組みましょう。
○　他の人にもわかりやすい正確な記録を心がけましょう。
○　医療機器等は操作方法をよく理解し、始業・終業点検や保守点検を行った上で使用しましょう。

【 OECD８原則と個人情報保護取扱の義務規程の対応について 】

OECD(経済協力開発機構)が、1980 年に公表したプライバシーガイドラインの８原則と個人情報の保護に関する法律における条文の対比を以下に記載する。

(OECD８原則)
目的明確化の原則
◇　収集目的を明確にし、データ利用は目的に合致すべきである
利用制限の原則
◇　データ主体の同意がある場合、法律の規定がある場合以外は目的以外に利用してはならない
(個人情報保護取扱い事業者の義務規程)
○　利用目的をできる限り特定しなければならない（第 15 条）
○　利用目的の達成に必要な範囲を超えて取り扱ってはならない（第 16 条）
○　本人の同意を得ずに第三者に提供してはならない（第 23 条）

(OECD８原則)
収集制限の原則
◇　適法・公正な手段により、かつ本人に通知または同意を得て収集されるべきである
(個人情報保護取扱い事業者の義務規程)
○　偽りその他不正の手段により取得してはならない（第 17 条）

(OECD８原則)
データ内容の原則
◇　利用目的に沿ったもので、かつ、正確、完全、最新であるべきである
(個人情報保護取扱い事業者の義務規程)
○　正確かつ最新の内容を保つよう努めなければならない（第 19 条）

(OECD８原則)
安全保護の原則
◇　合理的安全保護措置により、紛失・破損・使用・修正・開示等から保護するべきである
(個人情報保護取扱い事業者の義務規程)
○　安全管理のために必要な措置を講じなければならない（第 20 条）
○　従業者・委託先に対し必要な監督を行わなければならない（第 21、22 条）

(OECD８原則)
公開の原則
◇　データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示すべきである
個人参加の原則
◇　自己に関するデータの所在及び内容を確認させ、又は異議申立を保障するべきである
(個人情報保護取扱い事業者の義務規程)
○　取得したときは利用目的を通知又は公表しなければならない（第 18 条）
○　利用目的等を本人の知り得る状態に置かなければならない（第 24 条）
○　本人の求めに応じて保有個人データを開示しなければならない（第 25 条）
○　本人の求めに応じて訂正等を行わなければならない（第 26 条）
○　本人の求めに応じて利用停止等を行わなければならない（第 27 条）

(OECD８原則)
責任の原則

◇　管理者は諸原則実施の責任を有する

（ 個人情報保護取扱い事業者の義務規程 ）

○　苦情の適切かつ迅速な処理に努めなければならない（第 31 条）

【 リスボン宣言（患者の権利に関する世界医師会リスボン宣言）抜粋 】

1981 年　ポルトガル・リスボンにおける世界医師会第 34 回総会で採択
1995 年　インドネシア・バリにおける同第 47 回総会にて改訂

【 情報に関する権利 】

A　患者は自分の診療録（カルテ）に記載された自分自身に関する情報を開示され、自己の健康状態（自己の病状についての医学所見を含む）について十分な情報を得る権利を有する。しかし、カルテに記載されている第三者に関する個人的情報はその第三者の承諾なしには患者に開示すべきではない。

B　情報開示により患者の生命あるいは健康に重大な害を与えると信ずるに足る理由がある場合には、例外的に患者への情報開示を差し控えることができる。

C　情報開示は患者の属する文化的背景に従い、患者に理解可能な形でなされるべきである。

D　患者がはっきり望む場合、第三者の生命の危機に関与しない限り、自己の情報を知らされずにおく権利を患者は有する。

E　患者は自分に代わって自己の情報の開示を受ける人物を選択する権利を有する。

【 秘密保持に関する権利 】

A　患者の健康状態、症状、診断、予後および治療に関する本人を特定し得るあらゆる情報、ならびにその他すべての個人的情報の秘密は、患者の死後も守られねばならない。ただし、患者の子孫が自らの健康上の危険に関わる情報を知る権利は、例外的に認められる。

B　秘密情報の開示は患者本人が明確な承諾を与えるか、法律に明確に規定されている場合にのみ許される。他の医療従事者への情報開示は、患者が明確な承諾を与えていない限り、業務遂行上知る必要がある範囲内でのみ許される。

C　患者を特定することが可能なデータは保護されねばならない。データの保護はその保存形態に応じて適切になされねばならない。個人の特定が可能なデータが導き出されうる生体試料や標本も同様に保護されねばならない。

【 個人情報保護関連サイト 】

【内閣府】
個人情報保護に関するページ
http://www5.cao.go.jp/seikatsu/kojin/index.html

【法　令】
個人情報の保護に関する法律
http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html
個人情報の保護に関する法律施行令
http://www5.cao.go.jp/seikatsu/kojin/seirei/pdfs/kojinseirei507.pdf
個人情報の保護に関する基本方針（閣議決定）
http://www5.cao.go.jp/seikatsu/kojin/kihonhoushin-kakugikettei.pdf

【医療関連のガイドライン】
医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（厚生労働省）
http://www.mhlw.go.jp/houdou/2004/12/dl/h1227-6a.pdf
ヒトゲノム・遺伝子解析研究に関する倫理指針
http://www.mhlw.go.jp/general/seido/kousei/i-kenkyu/genome/0504sisin.html
遺伝子治療臨床研究に関する指針
http://www.mhlw.go.jp/general/seido/koisei/i-kenkyu/idenshi/0504sisin.html
疫学研究に関する倫理指針
http://www.mhlw.go.jp/general/seido/koisei/i-kenkyu/ekigaku/0504sisin.html
臨床研究に関する倫理指針
http://www.mhlw.go.jp/general/seido/koisei/i-kenkyu/rinri/0504sisin.html
症例報告を含む医学論文及び学会研究会発表における患者プライバシー保護に関する指針（外科関連学会協議会）
http://www.jssoc.or.jp/docs/aboutus/us_privacy_guide.html
遺伝学的検査関するガイドライン（遺伝医学関連学会 10 団体）
http://www.jsgc.or.jp/guideline.doc
ヒト遺伝子検査受託に関する倫理指針（日本衛生検査所協会）
http://www.jrcla.or.jp/info/info/dna.pdf
厚生労働省　診療情報の提供等に関する指針
http://www.mhlw.go.jp/shingi/2004/06/s0623-15m.html
日本医師会　診療情報の提供に関する指針
http://www.med.or.jp/nichikara/joho2.html
健康保険組合等における個人情報の適切な取扱いのためのガイドライン
http://www5.cao.go.jp/seikatsu/kojin/houritsu/index.html
雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/koyou.pdf
雇用管理に関する個人情報のうち健康情報を取り扱うに当たっての留意事項
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/tsuutatsu.pdf
保健医療分野のプライバシーマーク制度
http://privacy.medis.jp

【他分野のガイドライン】

経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン
http://www.meti.go.jp/press/20041217010/041217iden.pdf
福祉関係事業者における個人情報の適正な取扱いのためのガイドライン
http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/fukushi.pdf
個人情報の保護に関する法律について経済産業分野を対象とするガイドライン
http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf
診療録の外部保存に関するガイドライン(財団法人医療情報システム開発センター)
http://www.medis.or.jp/2_kaihatu/denshi/index.html
診療録の電子媒体による保存に関する解説書(財団法人医療情報システム開発センター)
http://www.medis.or.jp/2_kaihatu/denshi/index.html
コンピュータウイルス対策基準(通商産業省)
http://www.ipa.go.jp/security/antivirus/kijun952.html
コンピュータ不正アクセス対策基準(通商産業省)
http://www.ipa.go.jp/security/ciadr/guide-crack.html
情報システム安全対策基準(通商産業省)
http://www.meti.go.jp/policy/netsecurity/downloadfiles/esecu03j.pdf
民間部門における電子商取引に係る個人情報の保護に関するガイドライン Ver2.0
(電子商取引推進協議会　平成 15 年 9 月)
http://www.ecom.jp/home/privacy_gl/GuideLineV2.pdf

【その他】
個人情報保護に関するコンプライアンス・プログラムの要求事項　JIS　Q　15001：1999　日本工業規格
http://www.jisc.go.jp/
検査室に対する認定の基準　JAB　RL130-2004　（財）日本適合性認定協会
http://www.jab.or.jp/
付属書 B（参考）　検査室情報システム（LIS）の保護についての勧告
付属書 C（参考）　検査医学における倫理　　（財）日本医療機能評価機構
http://jcqhc.or.jp/