- ECMA 168 Volume and File Structure of Read-Only and Write-Once Compact Disk Media for Information Interchange
- JIS X 0609:1998 情報交換用非逐次記録高密度光ディスクのボリューム構造及びファイル構造
- JIS TR X 0006:1998 DVD - 再生専用ディスクのボリューム構造及びディスク構造
- JIS TR X 0038:2001 DVD - 書換形ディスクのボリューム構造及びファイル構造

2.1.4 インターネット・データ形式

- Extensible Markup Language (XML) 1.0 (Third Edition), World Wide Web Consortium.
  - JIS X 4159:2002 拡張可能なマーク付け言語 (XML)
- XHTML 1.0 The Extensible HyperText Markup Language (Second Edition), World Wide Web Consortium.
  - HTML 4.01 Specification, World Wide Web Consortium.
  - JIS X 4156:2000 ハイパーテキストマーク付け言語 (HTML)
- Uniform Resource Identifier (URI): Generic Syntax, RFC3986, The Internet Society.

2.1.5 医療情報規格

- HL7 Clinical Document Architecture, Release 2.0, Health Level Seven.
- IHE Radiology Technical Framework (Revision 6.0 May 20, 2005), The Integrating the Healthcare Enterprise (IHE) initiative.
- Digital Imaging and Communications in Medicine (DICOM) - Part 10: Media Storage and File Format for Media Interchange, PS 3.10-2004, National Electrical Manufactureres Association.
- CDA文書暗号化規格 V1.00, 日本HL7協会, 2006.

2.2 用語

本規格書において使用される用語について定義する。

2.2.1 電子診療文書 (Clinical Document)

- 患者についての診療にかかわる情報が記載された HL7 CDA に準拠した XML インスタンス。
- 単一の可搬電子診療文書媒体には、その主目的に対応する唯一のインスタンスが存在する。

2.2.2 外部参照データ (External Reference Data)

- 電子診療文書より正式に外部参照される診療データ
- 以下のような内容をもった診療データが想定される (informative)
  - 患者に対する客観的観測結果など
    - 臨床検査結果
    - 臨床診断画像
  - 患者に対する診断文書など
    - 放射線画像診断レポート
    - 内視鏡診断レポート
    - 病理診断レポート
  - 患者に対する治療実施記録など
    - 処方箋
    - 処置、手術、看護処置などの行為についての記録
  - 患者に対する治療の計画文書など
    - 治療計画書

        - 看護計画書
        - 放射線治療線量分布画像
    - 患者に対する指導情報
        - 服薬指導
        - 栄養指導
        - 理学療法など各種療法
    - 患者に関する会計、保険、行政情報
        - 診療費明細書
- データ形式は各種標準規格に準拠することが推奨される。
  以下の形式が想定される（informative）
    - 内容の意味的構造を記述する形式
        - DICOM
        - HL7
        - MFER
        - MML
    - 内容の視覚表現を記述する形式
        - JPEG
        - MPEG
        - PNG
        - HTML
        - PDF
- 単一の可搬電子診療文書媒体には、複数の外部参照データが存在してよい。

2.2.3 可搬電子媒体（Portable Media）

- 以下の条件を満たす一般的な計算機により情報の読み込み、書き込みが可能な記録媒体。
    - 複数のデータに名前などの属性を与えて格納できる。
    - 外部からのエネルギー供給無しに記録されたデータを長時間維持することができる。
    - 人間が無理なく所持・運搬ができる大きさ・質量をもつ。

2.2.4 電子診療ファイル集合（Clinical File Set）

- 単一の可搬電子媒体に記録される、電子診療文書及び外部参照データの総称
- ファイル集合を本規格に特化した概念である。

2.2.5 ファイル（File）

- 「JIS X 0606 §4.7 ファイル」による

2.2.6 ディレクトリ（Directory）

- 「JIS X 0606 §6.8.1 ディレクトリ」による

2.2.7 ファイル集合（File Set）

- 「JIS X 0609 §1.4.8 ファイル集合」による

2.2.8 PDI（Portable Data for Imaging）

IHE の Integration Profile の一つ。IHE Radiology Technical Framework 参照。

3. 可搬電子媒体

3.1 物理記録方式

物理記録方式について本規格では規定しない。本節の内容は推奨である。

3.1.1 推奨媒体

可搬電子診療文書媒体として使用が推奨される可搬電子媒体は JIS 規格に準拠したものうち以下に列挙したものである。

データ保護の観点より、書き換え不能な媒体の利用を推奨する。

3.1.1.1 FDC

- JIS X 6221:1987 90mm フレキシブルディスクカートリッジ（７９５８磁束反転／ｒａｄ）
- JIS X 6223:1987 90mm フレキシブルディスクカートリッジ（１３２６２／１５９１６磁束反転／ｒａｄ）
  （１３２６２磁束反転／ｒａｄを除く）

3.1.1.2 CD-R

- TS X 0025:2005 追記形コンパクトディスク（ＣＤ－Ｒ）システム

3.1.1.3 CD-RW

- TS X 0066:2004 書換形コンパクトディスク（ＣＤ－ＲＷ）システム

3.1.1.4 DVD-R

- JIS X 6245:1999 80mm (1.23 GB/面) 及び120mm (3.95 GB/面) DVD-レコーダブルディスク (DVD-R)

3.1.1.5 DVD-RAM

- JIS X 6243:1998 120mm DVD-書換形ディスク (DVD-RAM)
- JIS X 6246:2005 120mm (4.7GB/面) 及び80mm (1.46GB)DVD-書換形ディスク (DVD-RAM)

3.1.2 記録方式

データ保護の観点より、記録方式の選択にて以下の方式の適用を勧告する。

- ディスク一括記録モード (Disk at once recording mode) を使用する。
- 増加記録モードを使用する場合は、ファイナライズ (finalize) を実施する。

3.2 論理記録方式

3.2.1 データ格納方式

複数のデータを単一の記録領域に格納するために利用されている技術としてファイルシステムとアーカイブ、メッセージ等がある。本規格では、ファイルシステム技術を用いる。

3.2.2 ボリューム構造及びファイル構造

ファイルシステムは以下の規格の何れかに準拠しなければならない。

3.2.2.1 FDC

- JIS X 0605 情報交換用ディスクカートリッジのボリューム及びファイル構成
  - ISO/IEC 9293 Volume and file structure of disk cartridges for information interchange

3.2.2.2 CD-R, CD-RW

- JIS X 0606:1998 情報交換用CD-ROMのボリューム構造及びファイル構造
  - ISO 9660:1988 Information processing - Volume and file structure of CD-ROM for information interchange
  - ECMA-119 Volume and File Structure of CDROM for Information Interchange
- JIS X 0608:1997 再生専用形及び追記形の情報交換用コンパクトディスク媒体のボリューム及びファイル構造
  - ISO/IEC 13490 Volume and File Structure of read-only and write-once compact disk media for information interchange
  - ECMA 168 Volume and File Structure of Read-Only and Write-Once Compact Disk Media for Information Interchange

3.2.2.3 DVD-R, DVD-RAM

- JIS X 0606:1998 情報交換用CD-ROMのボリューム構造及びファイル構造
  - ISO 9660:1988 Information processing - Volume and file structure of CD-ROM for information interchange
  - ECMA-119 Volume and File Structure of CDROM for Information Interchange
- TR X 0038:2001 DVD - 書換形ディスクのボリューム構造及びファイル構造

4. ファイル体系

本章では、ファイルの配置、属性、形式などについての規定を定める。

これは、ファイルシステム規格によって定められた規定を越えるものではなく、ファイルシステム規格の範囲内で、可搬電子診療文書媒体を用途とした場合に追加される制限を規定するものである。

4.1 ファイル形式

可搬電子診療文書媒体に格納されるファイルの形式については制約しない。

4.2 ファイル属性

4.2.1 ファイル識別子

本規格では以下の制約を適用する

d文字については「JIS X 0606 §7.4.1 d文字およびa文字」を参照。

- ファイル名及びファイル拡張名は d文字により構成する。
- ファイル名の長さの上限は 8 文字とする。
- ファイル拡張名の長さの上限は 3 文字とする。
- ファイル拡張名の長さが 0 の場合は、区切り文字 1 は存在してはならない。
- 区切り文字2は存在してはならない。
- ファイル版数番号は存在してはならない。

4.2.2 ディレクトリ識別子

本規格では以下の制約を適用する

- ディレクトリ識別子は d文字により構成する。
- ディレクトリ識別子の長さの上限は 8 文字とする。

4.2.3 電子診療文書のファイル属性

本規格では以下の制約を適用する

- 電子診療文書のファイル名は HL7CDA でなければならない。
- 電子診療文書のファイル拡張名は、暗号化されていない場合は、XML でなければならない。暗号化される場合は、暗号化規則に従ったファイル拡張名が付与されなければならない。

4.2.4 外部参照データのファイル属性

本規格ではファイル識別子について規定しない。ファイル形式を定める規格にファイル識別子についての規約が定められている場合はそれに則ること。その他の規格などでファイル形式に対応したファイル識別子についての規約が定められている場合はそれに則ることが望ましい。

4.3 ファイル配置

4.3.1 ディレクトリ階層の深さ

階層のレベル数は１～８とする。(JIS X 0606:1998 §6.8.2.1 ディレクトリ階層の深さ 参照

4.3.2 ルートディレクトリ

4.3.2.1 必須ディレクトリ

4.3.2.1.1 HL7CDA

電子診療文書及び関連ファイルは HL7CDA ディレクトリに配置しなければならない。

HL7CDA ディレクトリには、電子診療文書及び関連ファイル以外のファイルを配置してはならない。

4.3.2.2 必須ファイル

ルートディレクトリには、以下のファイル識別子を持つファイルを配置しなければならない。

4.3.2.2.1 INDEX.HTM

ファイルの形式、内容については 5.2 を参照

4.3.2.3 必要ディレクトリ

指定された条件に合致する場合、ルートディレクトリに以下のディレクトリ識別子を持つディレクトリを配置しなければならない。

4.3.2.3.1 IHE_PDI

条件：可搬電子診療文書媒体が PDI に準拠した Web Contents を記録している場合。

内容は PDI に準拠すること。

4.3.2.4 必要ファイル

指定された条件に合致する場合、ルートディレクトリに以下のファイル識別子を持つファイルを配置しなければならない。

4.3.2.4.1 CRYPTLOG.XML

条件：可搬電子診療媒体に格納されるファイルが CDA 文書暗号化規格に準拠した方式で暗号化される場合。

内容はCDA 文書暗号化規格に準拠すること。

4.3.2.4.2 DICOMDIR

条件：可搬電子診療文書媒体が PDI に準拠した DICOM Contents を記録している場合。

内容はPDIに準拠すること。

5.3.2.5 推奨ファイル

以下のファイルをルートディレクトリに配置することを推奨する。

4.3.2.5.1 README.TXT

ファイルの形式、内容については 5.3 を参照

4.3.2.6 配置可能ディレクトリ

任意のディレクトリをルートディレクトリに配置しても良い。

ただし、ディレクトリ識別子として PDI_ で始まるディレクトリは PDI により予約されているので、PDI に合致した内容以外のものを格納するために配置してはならない。

4.3.2.7 配置可能ファイル

INDEX.HTM, README.TXT, CRYPTLOG.XML, DICOMDIR 以外のファイルをルートディレクトリに配置してはならない。

4.3.2.8 外部参照データの配置

外部参照データをルートディレクトリに配置してはならない。必ず、ディレクトリを設け、その中に配置する。

外部参照データが配置されているディレクトリに、外部参照データ以外のファイルを配置してはならない。

本規格では外部参照データを配置するディレクトリのディレクトリ識別子について規定しない。ファイル形式を定める規格にディレクトリ配置について規約が定められている場合はそれに則ること。その他の規格などでファイル形式に対応したディレクトリ配置についての規約が定められている場合はそれに則ることが望ましい。

5. ファイル内容

5.1 電子診療文書

本節では、電子診療文書（HL7 CDA 準拠のXMLインスタンス）について、本媒体に格納する場合の制約について規定する。

5.1.1 外部参照データへのリンク

電子診療文書から外部参照データを参照する際の URI は相対URI を用いなければならない。

5.2 INDEX.HTM

5.2.1 位置づけ

INDEX.HTM は可搬電子診療文書媒体の内容を計算機が読み取り可能になった際に、最初に参照されると想定される。

可搬電子診療文書媒体に記録された全てのファイルについて直接あるいは間接のリンクが確保されねばならない。

5.2.2 ファイル形式

- XHTML 1.0 The Extensible HyperText Markup Language (Second Edition)
- 以下の DTD により検証できなければならない
  - PUBLIC ID "-//W3C/DTD XHTML 1.0 Strict//EN"
  - SYSTEM ID "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"
- XML 宣言は必須とする
- frameset, iframe, img, link 要素を用いてはならない

5.2.3 内容

5.2.3.1 必須情報

5.2.3.1.1 作成機関情報

- 機関名称
- 可搬電子診療文書媒体について問い合わせ可能な連絡先

  電話番号、住所は必須

  部署名、担当者識別情報も記載することを推奨する。

- 作成機関による個人情報保護、セキュリティ対応についての表明を付記しても良い。

5.2.3.1.2 データ収集日時

電子診療ファイル集合が用意が完了した日時

日時には年、月、日を必須とする。

5.2.3.1.3 電子診療文書へのハイパーリンク

電子診療文書へのハイパーリンクがなければならない。

5.2.3.2 必要情報

指定された条件に合致する場合は記載しなければならない。

5.2.3.2.1 README.TXT へのハイパーリンク

条件：可搬電子診療文書媒体に README.TXT が存在する場合

5.2.3.2.2 PDI 情報

条件：可搬電子診療文書媒体に PDI 準拠の内容が記録されている場合

PDI が規定する内容を記載しなければならない。

5.2.3.2.3 処理ソフトウェア起動リンク

条件：可搬電子診療文書媒体に格納されている電子診療ファイル集合に対して表示などの処理を行えるソフトウェアが格納されている場合

リンクには以下の説明を付しなければならない。

- ソフトウェアの機能の概要
- リンクによって起動されるプログラムが、処理ソフトウェア自身なのか、処理ソフトウェアを利用者の計算機に設定するインストーラなのか。
- 対応しているオペレーティングシステム
- 起動後、最初に表示される画面の説明

5.2.4 個人情報保護及びセキュリティ

INDEX.HTM には個人情報が記載されてはならない。

INDEX.HTM を暗号化してはならない

5.3 README.TXT

5.3.1 位置づけ

README.TXT は可搬電子診療文書媒体に記録される患者臨床情報とは独立のものとする。従って、同一の README TXT は同一機関が作成する可搬電子診療文書媒体では全て同じものを使用できると考えられる。

5.3.2 ファイル形式

- 文字コード符号化体系は UTF-8 を用いなければならない
- 改行は CR+LF でなければならない。

5.3.3 内容

5.3.3.1 必須情報

5.3.3.1.1 準拠規格情報

可搬電子診療文書媒体及び電子診療ファイル集合が準拠している規格を識別する情報

- 制定団体
- 規格名称
- 規格バージョン
- 制定年度

特に下記の規格については必須とする。

- 可搬電子診療文書媒体（本規格）
- 電子診療文書

5.3.3.1.2 作成機関連絡先

可搬電子診療文書媒体を作成した機関の連絡先

5.3.3.1.3 作成システム情報

可搬電子診療文書媒体を作成したシステムを識別する情報

- ベンダー名
- 製品名

5.3.3.2 必要情報

指定された条件に合致する場合は記載しなければならない。

5.3.3.2.1 処理ソフトウェア情報

条件：可搬電子診療文書媒体に格納されている電子診療ファイル集合に対して表示などの処理を行えるソフトウェアが格納されている場合

- ベンダー名
- 製品名
- バージョン
- ソフトウェア動作の必要条件
- ソフトウェアの使用法
- 利用条件などの断り書き

5.3.4 個人情報保護及びセキュリティ

README.TXT には個人情報が記載されてはならない。

README.TXT を暗号化してはならない。

【資料２】

CDA 文書暗号化規格（案）　Ver0.99

日本 HL7 協会

CDA 文書暗号化規格（案）

ver. 0.99

日本 HL7 協会

目次

まえがき

昨今、患者あるいは家族から診療の把握、あるいはセカンドオピニオンを得たいという要求が高まってきている。また、医療・介護機関の機能分化と施設間連携を通じた医療・介護の効率向上が求められている。これらの要求を満たすために、適切に電子化された診療に関する情報を提供あるいは交換することが求められ、それらの文書の規格として HL7 CDA が存在する。CDA に準拠した文書は紙などの物理媒体と比べて大量の情報を含めることが可能で、一定の程度の安全性確保をすることがのぞましい。本規格は CDA 文書に安全性確保の目的で暗号化する場合の暗号化の手段を記述するものである。なお、この規格は暗号化を強制するものではなく、暗号化を行うかどうかは他の規格やドメインでの規約などで強制されない限り、CDA 文書を作成し、使用する当事者が自由に決めることができる。また暗号化の強度を用いる暗号の最高強度以下の任意のレベルに自由に設定できるように、鍵長を 16 octet より短く設定した場合のパディングルールを含めている。

ただし、鍵長を 16 octet より短く設定した場合はパディングルールを公開しているために、この規格が採用している暗号化方式の本来の強度が期待できないことに十分留意して使用する必要がある。

なお、本規格の目標は、以下のとおりである。

(1) 患者ケア情報の提供に重点をおく
(2) システムを低コストで実現できるようにする
(3) 記述された情報は、再利用の可能性があるものとする
(4) さまざまなドキュメント生成アプリケーションで互換性をもつようにする
(5) その文書の転送方式や格納のメカニズムとは独立である
(6) すみやかに設計書を提供する
(7) オープンな標準を使う

1. 適用

本規格は、特定の目的を持つ CDA 文書を可搬電子媒体に記録し使用する場合にデータを暗号化する際の仕様に適用する。暗号化を行うかどうかは本規格では規定しない。

2. 引用規格

本規格は、以下の規格を引用する。日付の付いた引用規格については、その日付以降に発行された修正票または改訂版は参照しない。しかしながら、本仕様書を使用する場合は、各規格の最新版を調べて適用するよう努めなければならない。

ISO/IEC 18033-3 :2005 Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers

XML Encryption Syntax and Processing (W3C 2002)

患者診療情報提供書規格 V1.00 (日本 HL7 協会 2006)

CDA 文書電子署名規格 V1.00 (日本 HL7 協会 2006)

3. 用語と定義

本規格では、以下の用語と定義が適用される。

3.1 可搬電子媒体

持ち運び可能な記録媒体のこと。CD-R、DVD、MO などを指す

3.2 共通鍵暗号

共通鍵暗号方式(Common key cryptosystem)とは、暗号化と復号に同一の鍵を用いる暗号方式である。秘密鍵暗号方式 (secret key cryptosystem) や対称鍵暗号 (Symmetric key encryption scheme) とも呼ばれる。

3.3 ブロック暗号

ブロック暗号 (Block cipher) とは、共通鍵暗号の一種で、ブロックと呼ばれる固定長のデータを単位として暗号化復号を行う暗号である。これに対して、ビット単位やバイト単位で暗号化を行う暗号はストリーム暗号と呼ばれる。

3.4 AES

AES は、アメリカの国家新標準暗号規格 (Advanced Encryption Standard) で規格

化された共通鍵暗号方式である。 1977 年に発行された暗号規格 DES が技術進歩により時代遅れとなったため、新たな暗号方式の公募を行い、2001 年 3 月に FIPS PUB 197 として公表された。

3.5 SEED

SEED は 1998 年から韓国情報 Korea Information Security Agency と専門家のグループによって開発された 128 ビットの共通鍵ブロック暗号である。

3.6 Camelia

NTT と三菱電機で開発された共通鍵ブロック暗号である。鍵長は 128 ビット、192 ビット、256 ビットを選択できる。

3.7 ファイル名称

ファイルを可搬電子媒体上で一意に指し示すことができるラベル

3.8 拡張子

ファイルの属性等を示すために使われるファイル名称の部分文字列、JIS X 0606 のファイル拡張名など

4. 暗号化

可搬電子媒体には個人情報、および診療情報が含まれる。媒体は紛失、盗難の恐れがあるため、データの暗号化を行うことが望ましい。可搬電子媒体に含まれる診療情報ファイルを暗号化する場合は個別に暗号化を行う事とする。暗号化する診療情報には CT のシリーズ画像等も含まれる事があり、暗号化する電子ファイルの数が膨大となる可能性があるため IC カードでの暗号化の処理を必須としない。暗号化を行った電子ファイルの情報はデータを暗号化する際にログとして記述し、暗号化したファイルを復号する際に使用する。このファイル名を CRYPTLOG.XML とする。CRYPTLOG.XML は本規格による暗号化を行ってはならない。

また、可搬電子媒体に CDA 文書およびそこから参照されている情報以外のデータファイルやビュアソフトなどのプログラムファイルが含まれる場合には本規格による暗号化を行ってはならない。

4.1 要求事項

- 電子診療情報提供書には個人情報および診療情報が含まれるため、電子診療情報提供書に対するセキュリティを確保する必要がある。必要なセキュリティとして個人情報保護に関する法律や関連するガイドラインに適合する必要がある。

・ 紹介元と紹介先の機器のＯＳが異なっていてもデータが性格に伝達されなければならない。そのため、暗号化についてはファイルシステムに依存しない方法をとる。

【資料 3】

CDA 文書電子署名規格（案）　Ver0.99

日本 HL7 協会

CDA 文書電子署名規格（案）

ver. 0.99

日本 HL7 協会

目次