HIMSS/NEMA規格HN 1-2008

医療機器セキュリティのための製造者開示説明書

発行元
National Electrical Manufacturers Association（米国電機工業会）
1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209
www.nema.org

通知及び免責条項

この出版物での情報は、開発当時は、文書の開発及び承認に従事していた人のコンセンサスによって技術的に正常であると考えられた。コンセンサスは、この文書の開発に参加するすべての人による満場一致を必ずしも意味しない。

米国電機工業会（NEMA）規格及びガイドライン出版物は、自発的なコンセンサス規格開発プロセスを通じて開発されている。本書もその一つである。このプロセスではボランティアを集め、この出版物の対象となるトピックに関心をもつ人の見解を求めている。NEMAはプロセスを処理し、コンセンサスの開発での公平を促進する規則を確立するが、文書の執筆はしない。また、NEMAは、規格とガイドライン出版物に含まれる情報の正確さ若しくは完全性、又は判断の健全性について、独立して試験、評価又は確認を行わない。

NEMAは、特別、間接、必然か補償かにかかわらず、直接的又は間接的にこの出版物、この文書の使用､適用又は依存に起因する身体傷害､財産又は他の損害に対し免責とする｡NEMAは、明示か黙示かを問わず、ここに出版された情報の正確さと完全性について免責とし保証はしない。またこの文書中の情報が読者の特定の目的又はニーズを満たすことは免責とし保証はしない。NEMAは、個々の製造者又は販売業者の製品又は役務の性能を、この規格又はガイドにより保証するものではない。

この文書を出版し利用可能にする際に、NEMAは、個人又は組織のために、又はそれらを代表して専門的その他の役務を与えるものではない｡またNEMAは個人又は組織が他の者に対し負う義務を行うものではない。この文書を使用する人は誰でも、自分自身の判断に頼ることが望ましい。又は、適切な場合、所定の状況での合理的な医療行為を決定する際に有能な専門家に対し助言を求めるほうがよい。この出版物の対象のトピックについての情報及び他の規格は、他の情報源から入手できることがある。この出版物の対象でない追加の見解又は情報を求めて、ユーザは他の情報源を調べる必要がある。

医療情報管理システム学会（HIMSS）もNEMAも、この文書の内容への適合を監視又は強制する権限も責任もない。HIMSSもNEMAも安全又は健康の目的のために、製品、設計又は設置の認証、試験、若しくは検査を行うものではない。この文書に記載の健康又は安全関連情報への適合の認証若しくは他の言明は、そのいずれに対してもHIMSS又はNEMAは免責とし、認証した者又は言明した者が全責任を負う。

目次

ページ

まえがき

この文書は、医療機器セキュリティのための製造者開示説明書（MDS^{2}書式）及びこの書式の記入方法の指示書から構成されている。医療提供者は、医療機器の送信又は保持する「保護対象電子健康情報（ePHI）」に関連する脆弱性及びリスクを査定する必要がある。MDS^{2}書式の意図は、この査定を支援する重要情報を医療提供者に提供することである。セキュリティのリスクアセスメントは組織全体に及ぶので、この文書が重視するのは、ePHIの保持又は送信する医療機器やシステムに関するリスクアセスメントプロセスの要素に限る。標準化した書式には次の利点がある。1) 製造者は、製造する医療機器のセキュリティ関連の特徴に関し、医療提供者から大量の情報要求を受けたとき、迅速に回答できる。そして、2) 医療提供者は、セキュリティ関連の大量の情報を製造者から提供されたとき、迅速に検討できる。

製造者が記入したMDS^{2}書式は次のようにすることが望ましい：

(1) 世界中の医療提供者組織にとって有用である。書式は、HIPAAプライバシー及びセキュリティ規則に適合しなければならない医療提供者にとって重要な情報を提供する。他方、その情報は、有効な情報セキュリティのリスクマネジメントプログラムをもちたいと熱望するすべての医療提供者にとって有用である。したがって米国以外でも、医療提供者は、MDS^{2}が地域的規制、例えばEU 95/46（欧州）、個人情報保護法（2003年の法律第57号、日本）、PIPEDA（カナダ）などに取り組む有効なツールであることを認識する。

(2) 個々の機器モデルの技術的なセキュリティ関連属性に取り組む機器固有の情報を含んでいる。

(3) 医療提供者組織（機器ユーザ／オペレータ）が必要とする共通かつ典型的な情報の技術的な機器固有の要素を集める簡単で融通のきく方法を提供する。この情報要素は医療機器情報セキュリティ（すなわち機密性、完全、利用可能性）のリスクアセスメントを始めるために必要である。

(4) この書式をコピーして使用することをHIMSSとNEMAは許可する。

注意事項―MDS^{2}書式は医療機器調達の唯一の根拠ではなく、かつ根拠としないほうが望ましい。調達仕様書を書くためには、セキュリティ及び医療の使命に関するより深い広い知識（個々の施設／医療提供者の状況を考慮して）が必要である。

医療提供者の学際的なリスクアセスメントのチームは、製造者がMDS^{2}書式で提供する情報、及びケアデリバリ環境について（例えばACCE/ECRIのバイオ医学技術情報セキュリティのためのガイドのようなツールを通じて）集めた情報を使用し、検討して、十分情報を得た上でローカルのセキュリティ管理計画の実行を決定できる。

この書式は、元来バイオ医学技術情報セキュリティ、すなわち、HIPAA適合ガイド（ACCE/ECRI、2004）の主要なツールであるACCE/ECRIのバイオ医学設備調査用紙の一部を改作したものであった。最初の書式は2004年に「MDS^2 v.1.0（2004-11-01）」として公表され、今回初めてHIMSS/NEMA合同規格として公表されるものである。HIMSSとNEMAは、各組織がACCE/ECRI書式に記入し、HIPAAセキュリティに適合する努力の一部として関連プロセスを完了することを支援するために、MDS^{2}書式中の情報を使用することを推奨する。この規格出版を準備する際に、ユーザ及び他の利害関係者の意見を求め評価した。

質問、コメント、改正提案、改正勧告は、下記宛先のNEMA製品サブディビジョンに提出して欲しい。

Vice President, Engineering
National Electrical Manufacturers Association
1300 North 17th Street, Suite 1752
Rosslyn, Virginia 22209

<このページは空白である>

セクション1
一般

1.1 適用範囲

MDS^{2}書式で提供される情報は、セキュリティのリスクアセスメントプロセスに責任をもつ専門家が、医療機器のセキュリティ問題を管理することを支援するために意図されている。MDS^{2}書式で提供される情報は、その他の目的を意図せず、またその他の目的には不適切かもしれない。

1.1.1 セキュリティ管理プロセスにおける医療提供者の役割

医療提供者組織は、有効なセキュリティ管理を提供することに最終的責任をもつ。
機器製造者は、医療提供者がセキュリティマネジメントプログラムを進めるとき、下記情報の提供により医療提供者を支援できる：

・製造者の機器又はシステムが保持／送信するデータのタイプ；

・製造者の機器又はシステムがデータを保持／送信する方法；

・製造者の機器又はシステムに内蔵されるセキュリティ関連の特徴。

医学情報セキュリティを有効に管理し、関連規制に適合するために、医療提供者は管理的、物理的、及び技術的な保護手段を使用しなければならない―それらの大部分は実際の機器にとって外部的である。

1.1.2 セキュリティ管理プロセスにおける医療機器製造者の役割

製造者が医療機器セキュリティに及ぼし得る最大の影響は、有効なセキュリティプログラムを保持し、関連する規制の要求事項及び／又は規格を満たす医療提供者の努力を容易にするために、機器に技術的保護手段（すなわちセキュリティ特徴）を組み入れることである。医療機器製造産業は、有効なセキュリティ機能性を機器及びシステムにもたせることは重要であるとの認識を深めているので、製造者は、医療提供者のニーズ及び要求事項に基づき新しい機器及びシステムを生産するとき、そのようなセキュリティ関連の要求事項を一般には含めている。

1.2 参考文献

次の参考文献は、推薦図書、裏付け資料、関連の出版物である。

1996医療保険の携行と責任に関する法律（HIPAA）、Pub L 104-191

健康保険改革：セキュリティ規格；最終規則、45 CFR pts. 160、162、164（2003年）

ECデータ保護指令、95/46/EC（EU 95/46）1995

個人情報保護法（2003年の法律、第57号、日本）

個人情報保護及び電子文書法（PIPEDA）、カナダ制定法、2000年

バイオ医学技術情報セキュリティ：HIPAA適合ガイド、2004年5月、米国臨床工学学会(ACCE)/ECRI

1.3 定義

管理的保護手段： 電子的に保護された健康情報を保護するためのセキュリティ手段の選択、開発、実施及び保持を管理し、並びにその情報の保護に関する対象組織の行動を管理する、管理的な行為、方針及び手続き [45 CFR Part 164]

アンチウイルスソフトウェア： ウイルススキャナを参照すること

監査証跡： セキュリティ監査を容易にするために集められ潜在的に使用されるデータ[45 CFR Part 142]

生物測定ID： 生物測定の同定システムは、個人の身体的な特徴又は反復可能な行動（例えば掌紋、網膜走査、虹彩走査、指紋パターン、顔の特徴、DNA塩基配列特性、声紋、手書きの署名）の測定から人間を識別する。[45 CFR Part 142]

電子媒体： (1) 電子記憶媒体。例えばコンピュータ内のメモリデバイス（ハードディスクドライブ）及び着脱／搬送可能なディジタルメモリ媒体、例えば磁気テープ又は磁気ディスク、光ディスク、又はディジタルメモリーカード。(2) 既に電子媒体内にある情報を交換するために用いられる送信媒体。例えばインターネット（ワイドオープン）、エクストラネット（関係者だけにアクセスできる情報を用いてビジネスをリンクするインターネット技術を使用する）、賃貸された回線、ダイアルアップ回線及び構内網、並びに着脱／搬送可能な電子記憶媒体の物理的な移動。一部の送信、例えばファクシミリによる紙及び電話による音声の伝送は、電子媒体による送信ではない。なぜならば交換される情報が送信前には電子媒体の形で存在しなかったからである。[45 CFR Part 160.103]

保護対象電子健康情報（ePHI）： 誰に関するものか特定できる健康情報（IIHI）であって、(1) 電子媒体を用いて送信されるか又は (2) 電子媒体の中に記憶されるもの[45 CFR Part 160.103]

誰に関するものか特定できる健康情報（IIHI）： 誰に関するものか特定できる健康情報とは健康情報の部分集合である。例えば個人から集められた人口学的情報を含む情報である。そして：(1) 医療提供者、保健計画、雇用者又は医療情報センターによって作成されるか受け取られる情報；及び (2) 次のことに関する情報である。個人の過去、現在、又は将来の身体的・精神的な状態；個人への医療の提供；又は個人の医療提供に対する過去、現在又は将来の支払；及び (i)個人を特定するもの；又は (ii) 個人を識別するため情報を使用し得ると考える妥当な根拠があるもの[45 CFR Part 160.103]。

暗証番号（PIN）： 個人に割当てて、同一性を立証するため使用される数字又は記号。[45 CFR Part 142]

物理的な保護手段： 対象となる組織の電子情報システム及び関連の建物及び設備を、自然・環境の危険及び無許可の侵入から保護する物理的な手段、方針及び手続き。[45 CFR Part 164]

遠隔サービス： 支援活動（例えば試験、診断ルーチン、ソフトウェアのアップグレード）で機器に直接接続されていないもの（例えばモデム、ネットワーク、インターネットを介する遠隔アクセス）。

着脱可能な媒体： 「電子媒体」の項を参照すること

リスク分析： 「保護対象電子健康情報」の完全性・利用可能性及び機密性に対する潜在的リスク及び「脆弱性」を、正確かつ徹底的に査定することをいう。[45 CFR Part 164]

リスクマネジメント： (1) リスクを査定し、容認可能な水準までリスクを減らす手段を講じ、

その水準のリスクを保持するための継続的プロセス。[NIST SP 800-26] (2) 合理的かつ適切なレベルまでリスク及び「脆弱性」を減らすために十分なセキュリティの手段。[45 CFR Part 164]

技術的な保護手段： 「保護対象電子健康情報」を保護し、その情報へのアクセスを制御する技術、方針及び手続き。[45 CFR Part 164]

トークン： ユーザが携行する物理的な認証機器（例えばスマートカード、SecureIDtm、など）。しばしば、単純なパスワード認証より優れていると一般に考えられているPINと組み合わされる二要素認証方式。

ウイルス： 一般に、次のいずれかのコンピュータコードである：

(1) 一種のプログラムされた脅威―別のプログラムに付いて再生するコード破片（独立プログラムではない）。それはデータを直接破損するか、又は認定ユーザによって利用できないシステム資源を引継ぐことによりシステム性能を低下させることがある。

(2) 一つ以上の他のプログラム中に自分自身のコピーを挿入させるプログラム内に埋込まれたコード；伝播することに加えて、ウイルスは通常、望まれない機能を行う。[45 CFR Part 164]

ウイルススキャナ： ウイルスコンピュータプログラム、又は他の種類の不正ソフトウェア（例えばワーム及びトロイの木馬）を検出し、その存在を警告し、それが保護コンピュータに影響することを防ぐコンピュータプログラム（「アンチウイルスソフトウエア」）。不正ソフトウェアは、しばしば、ユーザの想定外の望まれない副作用を起こす。

脆弱性： システム手続き、設計、実施､内部制御の欠点又は弱さで実行される（偶然に起こるか意図的に実行される）と、その結果セキュリティ違反又はシステムのセキュリティ方針の違反になるもの。[NIST SP 800-30]

1.4 頭字語

CD：コンパクトディスク

CF：コンパクトフラッシュ

DVD：デジタル汎用ディスク

IP：インターネットプロトコル

LAN：ローカルエリアネットワーク

ROM：読出し専用メモリ

SD：セキュアディジット

USB：ユニバーサル　シリアル　バス

VPN：仮想私設通信網

WAN：広域ネットワーク

WiFi：ワイ・ファイ

セクション 2
MDS²書式の入手、使用、記入の指示

2.1 MDS²書式の入手（医療提供者）
多くの機器及びシステムのために記入するMDS²書式は、機器製造者（例えば製造者ウェブサイト）から直接入手できる。

注－製造者が該当する機器／システムのために記入したMDS²書式をもっていない場合、ブランクのMDS²書式の最上部の適切な欄に製造者とモデル情報を記入し、この書式と指示書を製造者の法令順守担当部に提出し記入を依頼してください。

2.2 MDS²書式の使用（医療提供者）

2.2.1 セクション1－質問1-19
MDS²書式のセクション1は、機器の保持／送信するデータのタイプ、データの保持／送信の方法、機器に組み入れられた他のセキュリティ関連の特徴などの情報を適宜含む。書式の「他のセキュリティ考察」の欄に製造者は一般的なセキュリティ考察を追記することができる。

注意事項－リストされた機能を実行する機器の能力の表示（すなわち「はい」の答え）は、これは暗黙か明示かを問わず、製造者が機器の構成又はリストされた機能の実行を裏付け又は許可するものではない。

能力と許可とを区別することが重要である。MDS²書式に含まれる質問は機器能力を指している。許可はMDS²書式と無関係の契約上の問題であり、MDS²書式では扱わない。明示的な製造者による許可なくして機器を変更すると、重大な契約上の責任問題になることがある。

2.2.2 セクション2－解説
製造者が質問1-19に対する答えについて特定の詳細事項を説明するスペースを必要とする場合、MDS²書式の選択的セクション2には、解説を記入するスペースがある。

注－製造者は推奨慣行又は解説のためのスペースを更に追加する必要がある場合は、補足資料を添付してもよい。

2.3 MDS²書式の記入（製造者）

2.3.1 一般
製造者は、MDS²書式で要求される機器の保持／送信するデータのタイプ、データの保持／送信の方法、機器に組み入れられた他のセキュリティ関連の特徴に関する必要な記述的情報などすべての情報を、適切な要求組織に適宜提供しなければならない。

2.3.2 MDS²書式記入のガイダンス

書式冒頭の欄に記入する情報：

機器カテゴリ：これは文章を自由に記入する欄である。製造者は標準的な用語を用いて、主要なモダリティや設備の機能性を顧客が分かりやすく区別できるようにして欲しい。

機器モデル：これは文章を自由に記入する欄である。製造者は、市販される製品の名を記入して欲しい。

文書識別コード：文書識別コードは製品文書化を追跡するために内部で使用される製造者のユニークなタグである。

製造者の連絡情報：この情報は、書式の最終版の責任者に対する連絡方法を指定する。

質問1-19：

製造者はすべての質問に、「はい」「いいえ」「該当なし」のいずれかで答えなければならない。ただし他の答え方を質問が要求している場合を除く。

これらの答えを適切に解釈するため追加情報が必要な場合、セクション2「解説」の欄に記入しなければならない。

製造者は次のガイダンスに従って質問1-19に答えなければならない：

注ーこのサブセクション中の番号（下記）は、MDS^{2}書式のセクション1の質問番号と同じである。

1. ePHIの保持は、内部ディスク、着脱可能な媒体、短期のコンピュータメモリーなどへの記憶を含む。ePHIの送信は、機器の外部すなわちネットワーク、電話、直接接続のケーブル、着脱可能な媒体などを介する受信／送信を含む。

2. ePHIの定義は、国家規則及びローカルの経験によって異なる。一般に、ePHIは、特定患者に関するものとして識別できる保護された健康情報のすべての書式を含んでいる。例として、米国では、HIPAA規則は、ローカルの経験がない場合、ePHIの公称確認情報として次の18の要素を挙げている：

- *名前*
- *地理的なデータ（例えばアドレス）*
- *日付（例えば生年月日、入院、退院、死亡、治療）*
- *電話番号*
- *ファックス番号*
- *電子メールアドレス*
- *社会保障番号*
- *カルテ番号*
- *保健計画受益者番号*
- *アカウント番号*
- *証明書／ライセンス番号*
- *乗物確認情報*
- *機器確認情報*
- *ユーアールエル（URL）*
- *IPアドレス番号*
- *生物測定確認情報*
- *正面の（又は比較可能な）顔写真*
- *任意の一義的な識別番号、特性又は記号*

自由記入文に関する質問2dは、機器の保持する追加データ（恐らくePHI）であって医療提供者が文章で自由記入できるデータをカバーするように意図されている。

3. 製造者は、ePHIがどのように保持されるかについての詳細を提供する。

4. インポート及びエクスポートとは、情報が公開のオープンプロトコルを介して当該医療機器の外部の機器に移動することをいう（例えば、医療情報バス（IEEE 1073）、シリアルポート及びePHIへの一般的なアクセスを許可する公開プロトコル）。

ここで専用ケーブルとは、対象機器の外部にある機器又はシステムへの二点間ケーブルを介しての通信をいう。機器は、その構造内で専用ケーブルを内部的に使用してもよいが、そのケーブルは外部からアクセスできない限り言及される必要はない。

5. トレーニングと文書化に関する明確なセクションが、管理者又はユーザーのマニュアル中にあり、機器セキュリティの特徴及びそれらの使用を詳述する。

6. この質問は、基礎となる第三者システムソフトウェアプラットフォーム（オペレーティングシステム）名を特定するか、第三者プラットフォーム（すなわちこの製造者専用に作成された固有システム）がないことを示す。

7. 製造者の機器の典型的な設置方式を問う。

8. 着脱可能な媒体（例えば光ディスク、磁気ディスク、テープなど）上に情報をバックアップする統合された特徴かオプションがあるかどうかを問う。

9. 機器は、通常、製造者の正常なスタートアップ機器（例えば不可欠なハードディスクかROM）を用いて立ち上げるが、これ以外の出所からのソフトウェアを用い、ツールを使用せずに立ち上げることができるかどうか特定する。

10. ルートアクセス、管理上の特権、又は他の非侵入方法を通じて、ローカルユーザ及び／又はITスタッフは、製造者が提供していないし、認可していないソフトウェア（例えば電子メールクライアント、オフィスアプリケーション、ウイルススキャナ、ブラウザ、ゲームなど）を機器にインストールできるか。これが正常な機器構成によって可能であるが、契約又はサービス方針上できない場合、この質問には「はい」と答えて、関連するセクション2の注にその方針を明記すること。

11. 遠隔サービスとは、機器の保守活動をサービス要員がネットワーク又は他の遠隔接続を介して行うことをいう。

12. 所有者／オペレータは機器オペレーティングシステムに対しどのレベルまでアクセスできるか。ここで、機器所有者（一般に医療提供者）に対象医療機器へセキュリティ制御器類をインストールする技術的な能力があれば、製造者は技術的に可能なことを詳述する。所有者にこれらのすべてのステップを行う能力があれば、答えは「はい」である。ただし能力があっても契約又はサービス方針からこれを認可しないことがある。能力と認可とを区別することは重要である。この質問は能力に関係している。認可はMDS^2書式と無関係の契約上の問題であり、MDS^2書式では扱われない。

13. 機器がユーザー名とパスワード以外の識別方法を使用できる場合は、関連する注に簡潔にそれを記述すること（例えば、「XYZ安全トクンメカニズムを使用する」）

14. 答えが「はい」である場合、関連する注に簡潔に要約すること。

15. 質問の意味の説明：ビューイングとは、ePHIの表示、印刷又は他の使用（例えば画像表示、記録の印刷、など）と関係する操作をいう；生成、修正又は削除とは、これらの出来事がすべてログファイル中で追跡されることをいう;エクスポート又は伝達とは、対象機器の外部へePHIを移動することをいう。

16. 正常な認証が完了しないか適切に働いていない場合、緊急アクセス特徴によってオペレータは機器に緊急にアクセスできる。

17. 機器がディスクドライブのような恒久記憶機器をもっている場合、「はい」と答えるのがよい。停電でePHIの一部が失われる場合は、この振舞いの特性を注に簡潔に要約すること。

18. 質問の意味の説明：二点間の専用ケーブル経由とは、一般大衆にアクセスできないケーブルシステムである（すなわち、それが物理的に管理された場所、例えば検査室、通信室又は建物内部にある）；固定リストとは、接続と接続の性質を機器単位で制限する明確なメカニズムである。

19. 完全性を保証するとは、発信元のePHIメッセージと、外部機器の受信したePHIメッセージとの間の差異を検出及び／又は修正できる方法をいう。

セクション3
MDS^{2}書式

HN 1 MDS^2 *ワークシート*にアクセスしそれをダウンロードするためには、下記をウェブブラウザにタイプ入力してください：
http://www.nema.org/stds/complimentary-docs/upload/MDS2%20Worksheet.xls

又は下記のアイコンをダブルクリックしてください。

MDS^2 ワークシート

医療機器セキュリティのための製造者開示説明書 – MDS²

セクション 1

装置カテゴリー	製造者	文書識別コード	文書公表日時
装置モデル	ソフトウェア修正	ソフトウェア公表日時	

製造者又は代理人連絡情報	会社名 代理人名／役職	製造者連絡情報

保護対象電子健康情報の管理 (ePHI)	はい,いいえ 該当なし	注#
1. この装置は保護対象電子健康情報(ePHI)を送信又は保持できるか？		
2. 装置が保持する ePHI データ要素のタイプ:		
a. 患者基本情報(例えば名前、番地、住所、一義的な ID 番号)？		
b. 医療記録(例えば医療記録#、会計書#、検査又は治療日、装置識別番号)？		
c. 診断/治療(例えば写真/放射線写真、検査結果又は特徴を識別する生理学のデータ)？		
d. 装置利用者/操作者によって入力された公開フリーテキスト？		
3. ePHI の保守: 機器は次のことができるか。		
a. 揮発性メモリで ePHI を一時的に保持する(つまり、パワーオフ又はリセットによって消去されるまで)？		
b. 内部記録媒体に ePHI を確実に格納する？		
c. 他のシステムとの間で ePHI をインポート/エクスポートする？		
4. ePHI の送信、インポート/エクスポートのための機能:機器は次のことができるか。		
a. ePHI を表示する(例えば画面表示)？		
b. ePHI を含んでいる報告書又は画像を印刷する？		
c. ePHI を取り外し可能なメディアから取得する、又は ePHI を取り外し可能なメディアに記録する (例えば, ディスク, DVD, CD-ROM, テープ, CF/SD カード, メモリスティック)？		
d. ePHI の送信/受信又はインポート/エクスポートを専用ケーブルを介して行う(例えば, IEEE 1073, シリアルポート, USB, FireWire)？		
e. ePHI の送信/受信をネットワーク接続を介して行う (例えば LAN, WAN, VPN, intranet, Internet)？		
f. ePHI の送信/受信を無線接続を介して行う(例えば WiFi, Bluetooth, 赤外線)？		
g. その他？		

管理上の保護手段	はい,いいえ 該当なし	注#
5. 製造者は装置セキュリティの特徴につき操作者及び技術サポートにトレーニング、又は文書を提供しているか？		
6. 装置が使用する基本的なオペレーティングシステム(バージョン番号を含んで)は何か？		

物理的な保護手段	はい,いいえ 該当なし	注#
7. ePHI を物理的に保持する装置コンポーネント(取り外し可能なメディア以外の)は安全か(つまり、ツールなしでは移動できないようになっているか) ？		
8. 装置は完全なデータバックアップ能力を持っているか(例えばテープ、ディスクのような取り外し可能なメディア上へのバックアップを持っているか)？		
9. 装置は、非管理又は取り外し可能なメディア(つまり内部ドライブかメモリコンポーネント以外のソース)から立ち上げることができるか？		

技術的な保護手段	はい	いいえ	該当なし	注 #
10. 装置製造者によって認可されないソフトウェア又はハードウェアがツールを使用せずに装置にインストールされ得るか？				
11. 装置は遠隔サービスができるか(つまり保守活動をサービスマンがネットワーク又は遠隔接続を介して行うことが可能か)？				
a. 装置は特定の装置又はネットワーク位置への遠隔アクセスを制限できるか(例えば特定の IP アドレス)？				
b. 装置ログは遠隔サービス活動の監査証跡を提供できるか？				
c. セキュリティパッチ又は他のソフトウェアを遠隔インストールすることができるか？				
12. 所有者/オペレータが装置オペレーティングシステムに対しどのレベルまでサービスアクセスできるか: 装置所有者/オペレータは次のことができるか				
a. 装置製造者が妥当性確認したセキュリティパッチを適用する？				
b. アンチウイルスのソフトウェアをインストールするか更新する？				
c. 製造者のインストールしたアンチウイルスソフトウェア上でウイルス定義をアップデートする？				
d. 管理上の特権を得る (例えばオペレーティングシステム又はアプリケーションへのアクセスをローカルルート又は管理アカウントを介して行う)？				
13. 装置は利用者/操作者固有の ID 及びパスワードをサポートするか。 (別の同定法が使用されるかどうか説明する注記を使用すること)？				
14. 一定時間操作しない場合、装置は再認証を要求するか(例えば、自動ログオフする、セッションロック)？				

医療機器セキュリティのための製造者開示説明書 – MDS²

セクション 1

装置カテゴリー	製造者	文書識別コード	文書公表日時
装置モデル	ソフトウェア修正	ソフトウェア公表日時	

製造者又は代理人連絡情報	会社名 代理人名／役職	製造者連絡情報

15. 装置監査ログに記録された出来事(例えば利用者、日付/時間、実施された操作): 監査ログは次のことを記録できるか
    a. 利用者/操作者によるログイン及びログアウト？ ____ ____
    b. ePHI を見たこと？ ____
    c. ePHI の生成、修正又は削除？ ____ ____
    d. ePHI のインポート/エクスポート又は伝達/受取？ ____ ____
16. 装置はログされた緊急アクセス(「ブレイクグラス」)機能を組込んでいるか？ ____ ____
17. 装置は停電時に ePHI を保持できるか？ ____ ____
18. ePHI を他の装置と交換する場合の制御 ：
    a. 二点間の専用ケーブル経由の伝送に限るか？ ____ ____
    b. ネットワーク又は取り外し可能なメディア経由の送信に先立って暗号化するか？ ____ ____
    c. ネットワーク送信先の固定リストに制限されいるか？ ____ ____
19. 装置は、暗黙的・明示的なエラー検出/修正技術により ePHI データの完全性を保証しているか？ ____ ____

他のセキュリティ考察

医療機器セキュリティのための製造者開示説明書 – MDS²

セクション 1

装置カテゴリー	製造者	文書識別コード	文書公表日時
装置モデル	ソフトウェア修正	ソフトウェア公表日時	
製造者又は代理人連絡情報	会社名 代理人名／役職	製造者連絡情報	

セクション 2

解説 (質問 1 から 19 まで)**重要: この書式で要求される情報を適切に解釈するには、セクション 2.2.2 MDS2 の記入方法(NEMA規格 HN-1-2008)を参照すること。**