「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイド　Ver.4.1　に関するQ&A

（「医療情報システムの安全管理に関するガイドライン第5.2版」対応）

2023年8月

JIRA－JAHIS 合同開示説明書WG

目次

はじめに

本書は「製造業者/サービス事業者による医療情報セキュリティ開示書」（以下、製造業者による医療情報セキュリティ開示書をMDS、サービス事業者による医療情報セキュリティ開示書をSDSとする。）関連セミナー」で寄せられた質問を中心にまとめたものです。

※Qにおける「質問ｎ」の“ｎ”はMDS/SDS Ver.4.1における番号を指します。
※本書では厚生労働省の「医療情報システムの安全管理に関するガイドライン」を「安全管理ガイドライン」と記します。
※本書並びに本書に基づいたシステムの導入及び運用についてのあらゆる障害又は損害について、本書作成者は何ら責任を負わないものとします。

「全体」

Ｑ１．ある病院様から「御社より納入された医療情報パッケージシステムは、医療情報システムの安全管理に関するガイドラインに対応しているのか？」と回答を求められています。
本ガイドラインについては、どこまでがパッケージシステムに該当し、対応可否の回答をすれば良いのかが判別できない状況にいます。
「製造業者/サービス事業者による医療情報セキュリティ開示書」ガイドに「6.チェックリスト（製造業者編）（医療情報システムの安全管理に関するガイドライン第５.２版対応）」がありますが、本チェックリストにある項目が、医療情報システムの安全管理に関するガイドラインの中でパッケージシステムとして対応可否の回答をすべき事項が全て網羅されており、それ以外の項目はパッケージシステムとして関係が無く、対応可否の回答をせずとも良いとの考えで宜しいのでしょうか？

Ａ１．まず、大前提として「医療情報システムの安全管理に関するガイドライン」に対応すべき対象は、システムベンダー又はその医療情報システムではなく医療機関等であるということです。
医療機関等で誤解されている場合があるのですが、医療情報システムが安全管理ガイドラインに対応するのではなく、システムの持つ機能（技術的対策）と医療機関等がそれに相応した運用的対策を組み合わせて安全管理ガイドラインに対応するものです。必ずしも全項目に技術的対策が必須となる訳ではありません。

MDSでは安全管理ガイドラインのＣ項「最低限のガイドライン」の中の記載項目から、製造業者が提供する個々の医療情報システムの持つ機能(技術的対策)に関連するポイントを要約、抜粋したものとなっています。

そのため、MDS のチェックリストに御社のシステムについて回答したものを提出されれば、基本的には質問された病院様のニーズに応えた事になると思われます。

しかしながら、「MDS の全項目を回答すれば他は考慮しなくてよい」とは言えない場合があります。

第１に、MDS は「C 項に関して技術的対策項目」をピックアップし、D 項「推奨されるガイドライン」については対象外としているためです。

第２に、厚生労働省が MDS の使用を推奨していますが、完全網羅性が保証されている訳ではないためです。なぜなら、システムの使用条件が運用に制約を与える場合、その制約により安全管理ガイドラインの運用要件（C 項）が影響を受ける場合があり、医療機関から見れば、その部分も考慮ポイントとなりえるからです。

第３に、医療情報システムの提供だけではなく、それを利用したサービスを提供している場合は、SDS の作成、提供が必要になります。SDS では、医療情報システムの持つ機能(技術的対策)だけではなく、サービスを提供する事業者の運用的対策も記載します。

Q2．MDS/SDS チェックリストの使い方が今一つしっくりきません。医療機関から求められてチェックリストを提出していますが同じ製品又は同じサービスであっても、納品先によって詳細な機能の使い方が異なるため、チェックリストの内容が変わってしまいます。どのように使用すればよろしいのでしょうか？

A2． MDS/SDS チェックリストは納品仕様書ではなく、製品の機能リスト又はサービスで使用しているシステムの機能リストです。機能に関しては、「安全管理ガイドライン」の技術的対策の実装の有無を「はい」、「いいえ」、「対象外」で表しています。

そのため機能を有していて、納品先との調整の結果、設定で機能をオフにしていても MDS/SDS チェックリストとしては「はい」という回答になります。

例えば、案件段階で医療機関等が採用を検討する製品のセキュリティ対応状況を説明する際等に MDS/SDS を使用することができます。

Q3．質問の後ろの括弧の中の番号は何を示すのか？

A3．質問項目の括弧内に記載されている番号は、対応する安全管理ガイドラインの章番号を示しています。

Q4．MDS/SDS は医療機関から要求されて提出するものなのか、製造業者/サービス事業者側から積極的に提出するものなのか？

A4．MDS/SDS は製造業者/サービス事業者から自発的に開示することを想定したものです。統一フォーマットを使用することにより、製造業者/サービス事業者からの医療情報システムのセキュリティ対応状況の説明、医療機関側の情報収集が効率よく行えるようになることを期待しています。

Q5．ホームページでの MDS/SDS の公開等を考えるとマイナーバージョン毎の修正は避けたいが、バージョンは「ｘｘｘ以上」という表現でも良いか？

A5．MDS/SDS はお客様に対して提供する製品やサービスのチェックリストです。それぞれのお客様に対して提供するバージョンを記載した MDS/SDS を用意してください。ホームページで公開する場合のバージョンの記載方法は、医療機関が混乱しないよう各製造業者/サービス事業者で判断してください。

Q6．MDS に関して、製造する会社と販売する会社が異なる場合はどうすれば良いか？

A6．一般的には製造する会社が作成します。例外として OEM の場合、製造受託側ではなく、製造委託側の型式番号を持っている会社が発行する場合があります。

Q7．オプションの考え方（定義）が良くわからない。

A7．MDS/SDS におけるオプションの定義は、自社製品である必要はなく、動作確認が取れており、保守問合せ等の一次窓口になれる製品やサービスになります。単純に市販品等を調達して納品するだけではオプションとはみなせません。

Q8．ユーザの意向に応じて設定で機能がオン/オフできる場合、「はい」と回答して良いか？

A8．「はい」で結構です。デフォルト設定で機能がオフになっている場合は、備考にその旨を記載してください。

Q9．ユーザの要望により機能を追加する場合は「はい」と回答して良いか？

A9．「はい」とは回答できません。現時点で実装されていない機能については「いいえ」となります。

Q１０．MDS/SDS のチェックリストは安全管理ガイドラインの C 項を網羅しているのか？

A１０．MDS のチェックリストは、安全管理ガイドライン C 項の項目の中で製造業者が提供する個々の医療情報システムのセキュリティ機能に関して抜粋して記載しています。SDS のチェックリストは、安全管理ガイドライン C 項の項目の中でサービス事業者が提供する個々のサービスのセキュリティ機能とサービス事業者が実施すべきセキュリティ対策に関して抜粋して記載しています。これにより、医療機関側で C 項を網羅したセキュリティマネジメントを実施するための材料となります。

※網羅性については、A1. の解説もご参照ください。

Q１１．質問の内容に対して部分的に未対応な場合は「はい」と回答して、備考に未対応内容を記せば良いか？

A１１．一部でも未対応な場合は「いいえ」と回答し、備考に対応/未対応内容に関して記述してください。「はい」と回答する場合は全てについて対応できている場合になります。

Q１２．オプションで対応可能な場合は「はい」と回答して良いか？

A１２.「はい」で結構です。そのオプションの内容を備考に記載してください。

Q１３．「製造業者/サービス事業者による医療情報セキュリティ開示書」チェックリストについて、当社は医療機関向けに IT ツールを提供する側なのですが、MDS と SDS 作成者を教えてください。MDS が当社のように医療機関向けにサービスを提供する業者が書くもの、SDS はサービスの提供を受ける医療機関側が書くもの、と認識しているのですが、この認識は合っていますでしょうか？

A１３．いいえ。MDS は、医療情報を取り扱う医療機器や医療情報システムの製造業者が、医療機関等で使用する医療機器、医療情報システム等について作成するものです。
SDS は医療機関との契約に基づく医療情報システムによるサービスをデータセンター等で運用するサービス事業者が、そのサービスについて作成するものです。

また、医療機関内で運用するシステム等のリモートメンテナンスを行っている場合は、リモートメンテナンスもSDSの記載対象になります。

MDS/SDSの詳細については、下記のJAHISホームページで公開されているガイドをご参照ください。
https://www.jahis.jp/standard/detail/id=987

リモートメンテナンスのSDSのサンプルが下記JAHISホームページにて公開されていますので、こちらも併せてご参照ください。
https://www.jahis.jp/standard/detail/id=875

Q14．最近、製造業者/サービス事業者による医療情報セキュリティ開示書(MDS/SDS)を提出してほしいという医療機関からの問い合わせが増えております。

弊社取扱製品の内、弊社が開発・サポートを行っているオンプレミス型電子カルテについてはMDSを作成しておりましたが、他社が開発し、弊社では販売店として販売・サポートのみを行っている電子カルテ・レセコンについては、オンプレミス型・クラウド型にかかわらず、開示書を作成しておりませんでした。

医療機関向けユーザーズガイドの「「製造業者/サービス事業者による医療情報セキュリティ開示書」（MDS/SDS）の入手と利用」に記載されている図から、弊社ではMDSはメーカーが作成するもの、SDSはクラウドサービス事業者が、作成するものと認識していたのですが、一部社員から「サービス事業者」とは記載があるが、「クラウドを利用した医療情報システムを提供するサービス事業者」とは記載されていない為、販売店もサービス事業者に含まれ、SDS を作成して開示する必要があるのではないか、との意見がございました。

弊社で扱っている他社製品は、弊社にて用意したPCまたは医療機関が任意に用意したPCにて（オンプレミスの場合はインストールして）使用するのですが、製造業者/サービス事業者による医療情報セキュリティ開示書は、販売店が作成することも想定された様式でしょうか。
もし、想定された様式の場合、オンプレミス型・クラウドサービス型それぞれ、MDS/SDSどちらを開示となりますでしょうか。

A14．MDSはメーカーが作成するもの、SDSはクラウドを利用して医療情報システムによるサービスを提供するサービス事業者が作成するものです。
オンプレミスのシステムではMDSを作成、クラウドを利用して提供される医療情報システムによるサー

ビスではSDSを作成します。
ここで言う「サービス事業者」は販売店のことではありません。
※クラウドを用いてサービスを提供している「サービス事業者」＝「販売店」の場合は「販売店」がSDSを作成することになります。
なお、オンプレミスのシステムであっても、リモートメンテナンスを行っている場合は、リモートメンテナンスに関してはSDSを作成する必要があります。

MDS/SDSの詳細については、下記のJAHISホームページで公開されているガイドをご参照ください。
https://www.jahis.jp/standard/detail/id=987

リモートメンテナンスのSDSのサンプルが下記JAHISホームページにて公開されていますので、こちらも併せてご参照ください。
https://www.jahis.jp/standard/detail/id=875

Q１５．MDS/SDSで言うところの「製造業者」と「サービス事業者」の定義はどのようになりますでしょうか？
先月の厚労省の安全管理ガイドラインに関するチェックリストにて、MDS/SDSの作成について言及されたかと存じますが、MDSとSDSは両方とも作成し医療機関に提供するものなのかが判断できないでおります。
例えば
－ 医療情報システムを開発し、サービス展開している場合
－ 医療情報システムを輸入し、サービス展開している場合
などのケースも考えられると思いますが、それぞれMDS/SDSはどのように対応すれば良いものなのかが確認させていただきたいポイントとなります。
恐れ入りますが、ご確認、ご回答のほど、お願いいたします。

A１５．「製造業者」とは、医療機器や医療情報システムの開発、製造を行っている業者のことです。
「サービス事業者」とは、医療機関等との契約に基づく医療情報システムによるサービスをデータセンター等で運用する事業者、又は医療機関等で使用されている医療機器や医療情報システムのリモートメンテナンスを行っている事業者のことです。

MDSは、前述の「製造業者」が、医療機関等で使用する医療機器、医療情報システム等について作成するものです。
SDSは前述の「サービス事業者」が、そのサービスについて作成するものです。
また、医療機関内で運用するシステム等のリモートメンテナンスを行っている場合は、リモートメンテナン

スもSDSの記載対象になります。

MDS/SDSの詳細については、下記JAHISで公開されているガイドをご参照ください。
https://www.jahis.jp/standard/detail/id=987

リモートメンテナンスのSDSのサンプルが下記JAHISホームページにて公開されていますので、こちらも併せてご参照ください。
https://www.jahis.jp/standard/detail/id=875

Q16. 前の質問の「MDSとSDSは両方とも作成し医療機関に提供するものなのかが判断できないでおります。」の部分につきまして、例えば、「当社が医療情報システムを開発し、かつ、医療機関等との契約に基づいて医療情報システムによるサービスをデータセンター等で運用する場合」には、MDS/SDSを”ともに”作成するとの理解になりますでしょうか？

A16. 医療機関等、又はサービス提供事業者に医療情報システムを販売する場合にMDSが必要となります。
御社の場合は、自社のシステムを自社でサービス提供する形となりますが、医療機関等の契約に基づいて前述のサービスを提供しているためSDSの提供でよいです。なお、SDSにMDSの記載事項が含まれるため、MDSは不要となります。

Q17. MDSチェックリストおよびSDSチェックリストの記載方法についてご教示ください。
当社は医療情報システム（電子カルテ等）を稼働させるための複数のサーバ／ストレージ（ディスク装置）をハードメーカーから仕入れて、病院様に直接提供しております（電子カルテ等の医療情報システム自体は当社の範疇外）。このような提供状況において、病院様よりわかる範囲でよいので、MDSチェックリストおよびSDSチェックリストを記載してほしいとの依頼をいただきました。このような前提で以下質問です。

当社自体は製造物がございません。あるとすれば当社がメーカーから仕入れて販売しているサーバ／ストレージ（ディスク装置）複数になりますが、これらは製造物にあたるでしょうか？
製造物にあたる場合、これらの機器毎について、MDSチェックリストを記載すべきでしょうか？またハードウェア単体における機能を前提に記載すればよろしいでしょうか？
「サービス事業者」でのサービスとは、具体的にどのようなものを想定されていますでしょうか。一般にクラウドサービスの提供や病院様のIT運用のアウトソースサービス等と考えておりますが、当社の

ような立場の場合、サービス事業者にあたりますでしょうか？　以上、ご教示の程、よろしくお願いいたします。

A１７．MDS は、医療機器や医療情報システムの製造業者が、医療機関等で使用する医療機器、医療情報システム等について作成するものです。
SDS は医療機関等との契約に基づく医療情報システムによるサービスをデータセンター等で運用するサービス事業者が、そのサービスについて作成するものです。
また、医療機関内で運用するシステム等のリモートメンテナンスを行っている場合は、リモートメンテナンスも SDS の記載対象になります。

サーバやストレージ単体では MDS/SDS の対象とはなりません。
しかし、御社がサーバ/ストレージと電子カルテシステムを合わせてシステムとして納品されているのであれば、システム全体が MDS の記載対象となります。また、そのシステムに対してリモートメンテナンスをされている場合は、リモートメンテナンスシステムが SDS の記載対象になります。
御社がシステムを納入されているのではなく、単にハードウェアを納入されている場合は、そのハードウェアを使用してシステムを提供している業者に MDS を要求するよう医療機関等に、お伝えいただければよろしいかと思います。

MDS/SDS の詳細については、下記の JAHIS ホームページで公開されているガイドをご参照ください。
https://www.jahis.jp/standard/detail/id=987

リモートメンテナンスの SDS のサンプルが下記 JAHIS ホームページにて公開されていますので、こちらも併せてご参照ください。
https://www.jahis.jp/standard/detail/id=875

Q１８．医療機関様に診察や会計の番号案内のシステムを自社で開発し、販売している会社です。複数の医療機関様より MDS/SDS の提示を求められておりますが、ネット等で検索しても求めている回答に辿り着きませんのでご教示願います。
システムを開発し納入しているメーカーという立場になります。システムは全てクラウドではなくオンプレミスです。
下記 MDS/SDS に関する質問です。

1）個人情報を取り扱っていないシステムであっても医療機関様より提示依頼があった場合は、提示の必要が有るのか？

2） システムはオンプレミスだが、MDS、SDS 両方とも提示が必要か？それともどちらか片方で良いのか？

3） 医療機関に提示するものは「MDS/SDS Ver4.0 Format」エクセルシートの「MDS チェックリスト」「SDS チェックリスト」を印刷または PDF 化したもので良いのか？

他の製造メーカーにも弊社から提示依頼しているのですが、どこも提示をしてくれません。愛媛県は立入りが秋以降ということで各社の動きをみているように思います。
このままでは進まないため、率先して対応したく考えています。しかし、不明点等多いため何卒ご教示の程お願いいたします。

A１８.

1） システムの内容が不明なため、一概には言えませんが、患者の医療情報を扱う場合、保存が義務付けられた文章の電子保存に該当する場合、MDS は必要となります。
また、医療機関内で使用されているシステムであれば、提示された方が良いと思います。
結果的に MDS の回答が、ほぼ「対象外」、「非該当」となるかも知れませんが、医療機関側の立場で考えると、機微な情報を扱っていないということが確認できるため医療機関にとって有効な資料になると考えられます。
「対象外」、「非該当」の回答の備考に「個人情報を取り扱っていないため」等の説明を入れると、受け取った医療機関側にとって理解しやすいものになると思います。

2）オンプレミスのシステムの場合は MDS を提示してください。
ただし、システムをリモートメンテナンスしている場合は、リモートメンテナンスに関して、SDS の提示が必要となります。

3）印刷、または PDF での提示で結構です。

Q１９. 弊社はクリニック向けの予約システムのベンダーです。
顧客である医療機関様から医療情報セキュリティ開示書チェックリストの提出を求められていますが、弊社が「製造業者/サービス事業者 による医療情報セキュリティ開示書」で想定した事業者であるか判断できません。該当するか、ご教授願います。

A19.医療機関で使用されているシステムであれば該当すると、お考え下さい。
クリニック内オンプレミスで運用されている場合は MDS を、クラウドを用いたサービスとして提供されている場合は SDS を作成してください。

また、クリニック内での運用であっても、リモートメンテナンスをされている場合はリモートメンテナンスに関してSDSが必要となります。

Q２０．クラウドサービス型電子カルテの資料の作成をしていますが、この場合は SDS チェックリストを作成するという認識であっていますでしょうか？

A20.ご認識の通りです。

Q２１．貴社が制作されている「サービス事業者による医療情報セキュリティ開示書」を弊社でも参考にさせて頂いているのですが、「安全管理ガイドライン第 6.0 版」に対応したバージョンを公開されるご予定はありますでしょうか。
また、もし公開のご予定がある場合、いつ頃になるかご教示頂けますでしょうか。

A２１．「安全管理ガイドライン第6.0 版」への対応を検討しています。5.2 版で作成したMDS/SDS が6 版で有効あることは確認済みであり、そのままご使用になれます。その説明の５．２版と６版の対応表を付したものを2023 年８月に公開していますので、JAHIS ホームページでご確認ください。

Q２２．非常に基本的な内容で恐縮ですが、当ガイドに記載のある「「サービス事業者による医療情報セキュリティ開示書」チェックリスト」自体が「サービス事業者による医療情報セキュリティ開示書」であると捉えて間違いないでしょうか。チェックリストと開示書が別または親子関係の概念である場合にはご指摘をお願いいたします。
お客様から SDS の提出を求められ、その対応を社内検討進めようかという段階で念のため上述のチェックリストを提出することでその要求を満たしているのかを確認したかった次第です。

A２２．親子関係ではありません。Ｅｘｃｅｌで提供されているチェックリストは開示書を作成するためのツールになります。本ツールで印刷を行うと、Ｅｘｃｅｌの入力部分を除いた印刷領域をＰＤＦ化できますので、生成されたPDF をお客様へ提出してください。

Q２３．厚生労働省のサイバーセキュリティチェックリストに「医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出有無」の項目がありました。
このサイトにありました「チェックリスト（MDS SDS Ver.4.0）Rev.2.xlsx」を提出するには、会員になる必要があるのでしょうか。

また提出先は、病院様でよいのでしょうか。

A２３．MDS/SDS を提出するにあたり、JAHIS/JIRA 会員になる必要はございません。
提出先は、御社から見たお客様になります。お客様とは医療機関等、SIer、サービス事業者などがあります。
また、Rev.2 のチェックリストは旧版ですので、下記 URL から最新版を入手してください。
https://www.jahis.jp/standard/detail/id=987

Q２４．基本的なことで大変恐縮ですが、MDS/SDS の対象となるものに関するお尋ねです。次のシステムが対象となるかお教えください。

・CT・MRI 等に付属したシステム
・職員の線量管理システム

医療機器メーカー様に MDS/SDS の提出をお願いしたところ、これらは対象ではないという回答があったため、念のため確認をさせていただきたく存じます。

A２４．対象のシステムが医療情報を取り扱っている場合は、MDS/SDS の対象となります。
システムをオンプレミスで提供している場合は MDS、クラウドを用いたサービスを提供している場合は SDS をご依頼ください。

また、オンプレミスのシステムに対してリモートメンテナンスを提供している場合は、リモートメンテナンスシステムが SDS の記載対象になります。

お問い合わせのシステムが医療情報を扱っているかがポイントとなります。
医療情報を扱っていない場合は、対象外でよいと考えます。
その場合は当該システムが医療情報を扱っていないことを製造業者から明示していただければよいと考えます。

MDS/SDS の詳細については、下記の JAHIS ホームページで公開されているガイドをご参照ください。
https://www.jahis.jp/standard/detail/id=987

リモートメンテナンスの SDS のサンプルが下記 JAHIS ホームページにて公開されていますので、こちらも併せてご参照ください。
https://www.jahis.jp/standard/detail/id=875

Q２５．安全管理ガイドラインは、第６版が公開されています。しかし、MDS/SDS は、「医療情報システムの安全管理に関するガイドライン第５.２版対応」と記載されています。第６版対応ではなく、第5.2 版対応でいいのでしょうか？

Ａ２５．安全管理ガイドライン第6.0 版では、「本ガイドラインの内容の理解を促進し、医療情報システムの安全管理の実効性を高める観点から、本文について経営管理編、企画管理編及びシステム運用編に分け、各編で想定する読者に求められる遵守事項及びその考え方を示すとともに、QA 等で現状選択可能な具体的技術にも言及するかたちとすべく、構成の見直しを行った。そのほか、近時のサイバー攻撃及びクラウドサービス利用の普及等を踏まえ、医療機関等に求められる安全管理措置を中心に内容面の見直しを行った。」と示されています。このため、第５．２版対応で作成されたものであっても、医療機関等において安全管理ガイドライン第６版に対応するための情報提供としては有効であると認識しています。MDS/SDS は、今後もさまざまな状況等を踏まえ適切に改定をしていきます。
なお、チェックリストについては、５．２版と６版の対応表を付したものを 2023 年８月に公開していますので、JAHIS ホームページでご確認ください。

「安全管理ガイドライン６章　医療情報システムの基本的な安全管理」関係

Q２６．MDS「「質問１」、SDS「質問２」の「扱う情報のリスト」とは、どういうものか？

Ａ２６．患者情報の項目のリストです。例えば患者の氏名、ID、住所などです。扱う情報に関しては基本情報だけでなく、検査データや画像情報等も漏れなく記載してください。システムにもよりますが DICOM Conformance Statement 等でリストの代用も可能な場合があります。

Q２７．MDS「質問１」、SDS「質問２」の「はい」、「いいえ」の判断基準は、どう考えれば良いか？

Ａ２７．MDS／SDS のチェックリストは医療機関がリスクアセスメントを実施するための資料となるものです。リスト化され提示している場合は「はい」となります。リスト化されずに取扱説明書／サービス仕様書に記載されているだけでは「いいえ」となります。また、医療機関からの要求に応じて作成する場合も「いいえ」となりますが、備考欄にその旨記載しリストを提供可能であることを示してください。

Q２８．MDS「質問１」、SDS「質問2」に関して顧客が入力する任意の情報を扱うシステムで、情報の項目が製造業者側で把握できない場合はどう考えれば良いか？

Ａ２８．任意の情報が入力できる項目については、そのような項目が存在する旨を明記し、入力内容については医療機関等側で管理する必要がある旨、記載することを推奨します。

Q２９． MDS「質問１」、SDS「質問2」のリストのデータは複数の情報で構成されていても良いか？

Ａ２９．医療機関等による情報の見落としを防止するためには、データはまとまっていることが望ましいです。

Q３０．MDS「質問4．１」、SDS「質問１７．１」に関して、例えば「パスワード認証」と「生体認証」が「はい」となる場合、「二要素認証」が「はい」となるか。

Ａ３０．「パスワード認証」と「生体認証」を組み合わせて使用可能であれば「はい」と、いずれか片方のみが使用可能であれば「いいえ」になります。

Q３１．MDS「質問4．１．１」、SDS「質問１７．１．１」で書かれているパスワード管理とは何か？

Ａ３１．安全管理ガイドラインの 6.5C１４⑴から⑸で記載されている内容のことです。但し ⑵ の「本人確認に関する内容の台帳記載」に関しては一般的には運用でカバーする内容となりますので除外して回答いただいても結構です。

Q３２．MDS「質問4．１．１」、SDS「質問１７．１．１」の備考に「パスワードの登録・暗号化にのみ対応しています。パスワードの変更や類推性他の要素は運用でカバーしてください。」と記述された事例を見たことがあるが、なぜ、そのような記述になっているのか？

Ａ３２．技術面で求められているのは安全管理ガイドラインの6.5C１４⑴から⑸で記載されている通り５点あります。技術的にカバーしているのが全てでない場合は何がカバーできているのか、いないのかを備考にて記述してください。

Q３３．MDS「質問4．３」、SDS「質問１７．３」において、どのレベルが要求されているのか分からない。

Ａ３３.「JAHIS ヘルスケア分野における監査証跡のメッセージ標準規約　Ver.2.1」※を参考にしていただくと安全管理ガイドラインの要求事項と産業界としての標準フォーマットの両方を確認いただけます。

※ https://www.jahis.jp/standard/detail/id=803

Q３４．MDS「質問５」、SDS「質問１８」の解説の「標準時刻」は何を持って「標準」とすべきか分からない。

Ａ３４．日本での標準時刻は NICT が決定・維持を行っている日本標準時である JST（UTC+9）となります。日本標準時との時刻同期については NTP サーバの利用等にて適宜対応してください。

Q３５．MDS「質問６」、SDS「質問１９」に関して、モダリティの中には、不要なソフトウェアはインストールしない（できない）ため、インターネットに未接続であれば不正ソフトウェア対策は不要ではないか。こういった場合は「対象外」として良いか？

Ａ３５．必ずしも「対象外」として良いとは言えません。平成 27 年（2015 年）４月 28 日の厚生労働省からの通知（https://www.pmda.go.jp/files/000204891.pdf）でサイバーセキュリティ対応が要求されていることもあり、リスクアセスメントの結果、受容可能でないリスクがあれば不正ソフトウェア対策は必要となります。

また、院内 LAN や USB メモリ等を経由して感染する可能性があるためインターネットに未接続であっても必ずしも安全であるとは言えません。そのため、パターンファイル、ふるまい検知等を使用する「不正ソフトウェアのスキャン用ソフトウェア」をインストールすると過負荷となり画像のロスト等、運用に支障が発生する場合は、ホワイトリスト方式等の採用をお勧めします。

「アクセス制御リスト方式」等を含むウィルス対策ソフト等の不正ソフトウェア対策がされていれば「はい」となり、採用されている不正ソフトウェア対策について備考に記述してください。

また、ROM 上で動作する機器で書き込みが不可能であれば「対象外」として結構です。

Q３６．MDS「質問７」、SDS「質問２２」でオプションとして無線 LAN を準備している場合、「はい」、「いいえ」どちらになるか？

Ａ３６．オプションで準備している無線 LAN にセキュリティ機能がある場合は、「はい」で結構です。
※オプションの考え方についてはＡ７．をご参照ください。

Ｑ３７．オプションとして無線 LAN を用意しているのではなく、ユーザ指定で無線 LAN を納品する場合は、どのような回答になるか？

Ａ３７．「いいえ」としてください。
※オプションの考え方についてはＡ７．をご参照ください。

Ｑ３８．MDS「質問7」は、物によって違うのでは。サーバとかクライアントで回答が変わるかもしれないのだが。

Ａ３８．MDS のチェックリストは販売するシステム単位で記入するものなので、機器単位ではありません。システムを構成する機器の一部でも未対策の場合は「いいえ」としてください。なお、SDS のチェックリストは提供するサービス単位で記入するものです。

Ｑ３９．MDS「質問8」、SDS「質問５１．１」で通常の操作ではソフトウェアのインストールができなければ、「はい」で良いか？

Ａ３９．「はい」で結構です。

Ｑ４０．MDS「質問１２」で医事コンシステムにレセプトオンラインを含む場合は、どうなるか？

Ａ４０．外部との個人情報のやりとりがあるので「はい」としてください。

Ｑ４１．MDS「質問１２．１」において、クライアントまで含めたシステムのチェックという認識で良いか？

Ａ４１．MDS「質問１２．１」に限らず、クライアントが製品に含まれる場合は、クライアントも含みます。

Q４２．MDS「質問１２．１」において、クライアントに対してもなりすまし対策がなされているという理解で良いか？

Ａ４２．クライアントが製品に含まれる場合は、その理解で結構です。

Q４３．MDS「質問１２．３」でネットワークも含んで納品する場合、どう回答すれば良いか？

Ａ４３．「はい」と回答し、備考欄に具体的な内容を記載してください。

Q４４．MDS「質問１２」とMDS「質問１２．４」は同じことを問うているのか？

Ａ４４．MDS「質問１２」では「通信機能」または「リモートメンテナンス機能」などのネットワークで個人情報を含む医療情報を交換する機能があるかを問うており、MDS「質問１２．４」では「リモートメンテナンス機能」に限定して問うています。

Q４５．MDS「質問１２．４．１」、SDS「質問７５．１」において、何を持って不必要とするか？製造業者/サービス事業者と医療機関の間でギャップがありうるので両者間で協議しないと回答できないのでは？

Ａ４５．製造業者/サービス事業者側で作成するものなので、医療機関との協議は不要です。製造業者/サービス事業者の判断で記入してください。

Q４６．MDS「質問１３」、SDS「質問７８」においてモダリティは対象となるか？

Ａ４６．記名・押印が義務付けられた文書を生成する機能を有するモダリティの場合は対象となります。

Q４７．MDS「質問１４．１」、SDS「質問８０．１」において「区分」の意味する詳細な分類方法が分からない。「所見」と「処方」の違いも「区分」に入るのか？

Ａ４７．安全管理ガイドラインにおいては具体的な区分に関する規定はありません。例えばアクセス制御の際に、「所見」と「処方」に対する個別の権限管理が行われている場合には「区分」に入ります。
「所見」と「処方」が区分されていなくても、システムとして適切なアクセス制御が可能な区分管理がされていれば「はい」で結構です。

Ｑ４８．①SDS 質問20、21 で問われているメール送受信、ファイル交換の機能というのは、クラウド電子カルテサービスの中に機能として有しているケースのことを指していると認識しましたが合っていますでしょうか？
（システム利用端末で汎用的なメールソフトやファイル交換ソフトを使うケースではなく）

② ①の認識で合っている場合、弊社システムでは認証に利用するワンタイムパスワードをメール送信する機能を有していますが、一般的なｅメール送信と違って実行プログラムが含まれる（ユーザが添付等行う）余地はありません。この場合、回答は「対象外」で良いでしょうか？

③ これも①の認識で合っている場合、カルテ等にファイルを添付する機能は「ファイル交換機能」にあたりますでしょうか？

Ａ４８．
① ご認識の通りです。

② 「対象外」で結構ですが、なぜ「対象外」なのか備考に記されると受取側である医療機関で理解されやすいかと思います。

③ 該当します。

Ｑ４９．SDS 質問51～53 の持出機器についてですが、機器を持出利用する機能というものは特に設けておりませんが、クラウド型サービスのため、しかるべき認証を行うことでシステムを外部で利用することは可能です。
ですが、ここでの一連の設問では機器について問われているかと思われるため、回答は「非該当」「対象外」で良いでしょうか？

Ａ４９． SDS 質問51 に関しては機器についての質問ですが、SDS 質問52、53 に関しては「情報及び情報機器」に関する質問となるため、「対象外」、「非該当」にはなりません。

Q５０．SDS 質問 60.1「提供事業者に閉域性の範囲を確認しているか？」についてですが、ここで言う提供事業者とはNTT 東日本、西日本などの通信事業者という認識で合っていますでしょうか？（安全管理ガイドライン5.2 版 6.11.C1 において「～範囲を電気通信事業者に確認すること」とあるので）その場合、この設問項目では公衆網利用が前提ですが、通信事業者に確認する閉域性とはどのようなことでしょうか？安全管理ガイドライン5.2 版 6.11.C1 とそこに引用されている6.11.C11 においては、この場合の閉域性はTLS 等によって我々メーカー側で確保する必要があるもののように認識しますが、事業者にはどの部分を確認するべきなのでしょうか？

A50.ご認識の通りです。

回線事業者（NTT 東西、ドコモ、AU 等）が提供する公衆網について安全性をサービス提供者から回線事業者に確認することを求めるものです。

閉域性とは、インターネット等の他のネットワークとは接続されておらず、独立していることを指します。

なお、TLS は暗号化の技術であり、閉域性とは異なるものです。

（閉域網においてTLS 等の暗号化を行うことを否定するものではありません。）事業者への確認は、安全管理ガイドラインを参照して、サービスの閉域性の範囲を示してください、とお尋ねください。

「安全管理ガイドライン７章　電子保存の要求事項について」関係

Q５１．MDS「質問１６」、SDS「質問８１」において、確定機能とはデータベースにデータを登録することなのか、変更不可にすることなのか？

Ａ５１．どちらとも言えません。記録の確定については、安全管理ガイドライン別冊編 7.1（2）②を参照ください。

Q５２．MDS「質問１８」、SDS「質問８３」で、システムやサービスの更新（リプレース・契約変更）で製造業者、サービス事業者が変わる場合は「いいえ」で良いか？

Ａ５２．「いいえ」で結構です。マイグレーションの場合は、新システムとしてはデータが入力されるだけであり、以前のシステムの履歴は無関係となります。

Q５３．MDS「質問１８」、SDS「質問８３」では、製造業者、サービス事業者が変わる場合、旧システムの履歴は対象外だが安全管理ガイドライン的にはどうか？

Ａ５３．安全管理ガイドラインには明言されていませんが、移行時には標準形式のデータを使用することが推奨されています。

Q５４．MDS「質問２１．１」、SDS「質問９５．１」で、ネットワーク I/F や回線を複数有しており「ネットワークの冗長化」の機能があれば「はい」として良いか？

Ａ５４．冗長化された構成であれば「はい」で結構です。

Q５５．MDS「質問２１．２」において、外部保存サービスを利用した参照であっても「はい」で良いか？

Ａ５５．「はい」で結構です。

Q５６．MDS「質問２１．２」、SDS「質問９５．２」において、PDF 形式で保存されているが検索機能が用意されていない場合の回答はどうなるか？

Ａ５６．SS-MIX のようにフォルダ単位である程度、分別されている場合は「はい」と答えてください。全ファイルが押しなべて同一階層に保存されていて、ファイルを開かないと内容が確認できない場合は「いいえ」としてください。

Q５７．MDS 質問「２９ マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えているか？（7.3.C４(2)）」について、
「マスタデータベースの変更の際」で想定されているのは、以下のどちらのケースでしょうか？あるいはどちらもでしょうか？
・利用中のシステムが対象で、マスターデータベースを変更するケース
・利用中のシステムを別システムに切替時にマスターデータベースを変更するケース

A57.どちらのケースも対象になります。

特定条件にのみ対応している場合は、その旨を備考欄に記載してください。

「安全管理ガイドライン８章　診療録及び診療諸記録を外部に保存する際の基準」関係

Q５８．安全管理ガイドライン８章（外部保存）の質問がＭＤＳのチェックリストにないが、今後追加されるのか。

Ａ５８．検討の結果、製造業者が担保すべき事項がなかったため該当項目がありません。８ 章に関しては外部保存サービスを行っているサービス事業者側の内容となりますので、「サービス事業者による医療情報セキュリティ開示書」（SDS）に記載されています。

「安全管理ガイドライン９章 診療録等をスキャナ等で電子化して保存する場合について」関係

Q５９．原本として確定している紙のカルテを、スキャナを使って入力する場合、そのスキャナ入力の作業者が作業責任者となるのか。

Ａ５９．作業責任者と実際の作業者が異なる場合もあるので、必ずしもスキャナを使っている人が作業責任者になるとは限りません。医療機関の運用に依ります。

「その他」

Q６０．地域連携システムのサービスにおいても、参加する医療機関から MDS の提出が求められそうだがどう対応すれば良いか。

Ａ６０．地域連携ネットワークを構成する個々の製品に対して各々の MDS を用意してください。
MDS は個別製品用のものです。複数の製品を組み合わせて構築する地域連携システムのサービスにおいては要求仕様において三省ガイドライン（総務省、厚生労働省、経済産業省）に準拠することを求める場合が多くあり、運用も含めた対策を提案書等で提示する必要があります。「サービス事業者による医療情報セキュリティ開示書（SDS）」をご使用ください。

Q６１．モダリティ、機器に製造番号がある物が本チェックリストの対象とあるが、広域で利用される地域連携システムのサービスは対象となるか。

Ａ６１．地域連携システムのサービスのように大規模なものは運用面が係ってくることもあり、MDS の対象とすることは難しいです。地域連携システムのサービスに関しては、「サービス事業者による医療情報セキュリティ開示書（SDS）」をご使用ください。

Q６２．システムに外部保存の機能がある場合、MDS「質問１２」で回答すれば良いか。

Ａ６２．該当する製品（システム）に含まれる場合、通信に関する機能については、MDS「質問１２」で回答してください。外部保存サービスを提供する場合、「サービス事業者による医療情報セキュリティ開示書（SDS）」をご使用ください。

Q.６３．　MDS で言うところの製造業者とは「薬機法」における製造業の会社のことか？

Ａ.６３．　いいえ。　医療情報システム、医療情報機器を製造している業者を指しています。

改訂履歴

2016年9月	初版	Ver.2.0 対応
2017年10月	第2版	Ver.3.0(a)対応
2018年1月	第3版	Q&A の追加（医療機関からの問合せ対応）
2018年11月	第4版	Q&A の追加（製造業者からの問合せ対応）
2021 年5月	第5版	Ver.4.0 対応
2023年8月	第6版	Ver.4.1 対応