#	ご質問	回答
医療情報システムの有無		
1	インターネットに接続できない環境で、電子カルテ等を導入している場合も「医療情報システムを導入している」に該当するのかご教示ください。	インターネット接続の有無ではなく、患者情報の取扱いの有無でご判断ください。
2	医療情報システムには検体検査システムや薬剤発注システム、遠隔画像診断システムなども含まれますでしょうか。	ご質問頂いたシステムは患者情報が含まれると想定されるため、医療情報システムの対象になります。
3	医療情報システムの範囲についてお伺いします。当院は医事課内に介護事務職員が在籍しており、介護請求ソフトを導入しています。当方は介護情報は医療情報とは異なると考え、事業者確認用のチェックリストの依頼をしておりませんが、必要でしょうか？	ご意見をありがとうございます。
4	外部(ネットワーク)接続がない、医療情報を扱う端末も対象になりますか？例えば、患者の住所、生年月日などをExcelでまとめた情報を管理しているパソコン、検査機器、放射線機器に蓄積されている、検査結果のデータなどは医療情報システムの対象でしょうか？ また、レセコンなどで外部接続が送信時だけ一時的に行うものもネットワーク機器といいますか？ セキュリティパッチの適用や接続元制限の実施は医療情報システムのなかでもネットワーク接続がない機器に関しては該当なしという回答でもよいでしょうか？	患者情報の有無で判断しますので対象です。またレセコンについてはネットワーク機器というよりも端末とする方が適切かと思います。また、まず本当に閉域網であるのかどうか確認が必要です。また外部との接続が無くてもUSB等のデータやファイルのやり取りは生じていると思われ、セキュリティパッチやウイルス対策ソフトの定義ファイル等の更新が必要です。
5	職員専用の無線LAN（医療情報システムとの直接的な連携はしていない）のアクセス制限の実施も対象となりますでしょうか。	患者情報が含まれなければリストとしては対象外ですが、病院のITガバナンスを考えれば対象と考えるほうが望ましいでしょう。
令和5年度中 ＞1 体制構築＞（１） 医療情報システム安全管理責任者を設置している。		
1	【1 体制構築】医療情報システム安全管理責任者は，実質的に電子カルテや院内ネットワークを停止する権限を有する医療情報部長が務めることになろうと思うが，一般的な病院とは異なり，大学病院における医療情報システム安全管理責任者は，必ずしも大学や病院における経営層を兼ねていないことが多い．かといって，経営層が医療情報システム安全管理責任者を務めるのだとすると，医療情報システムの素人があてがわれることになりかねない．この際，医療情報部長を病院の経営層（院長・副院長，それらの補佐）に含むことが望ましいと明記されてはどうかと思うが，どのようにお考えでしょうか．	ご意見をありがとうございます。
2	１．安全管理責任者は、経営層・課長（科長）以上級（人事・予算・責任権限のある者）が担うべきでしょうか？担当者と別人が担うべきでしょうか？また、どのような知識・判断が求められますか？ 当院では、人材・予算・能力等色々な面で不足があり、「分からないからやっておいて」「お金が無いので人手でやって」「いいからやって」「人員募集かけても来ないのでよろしく」「個々の事柄について都度稟議で院長の許可を求めて」等々もあり、一人の現場担当者に責任者・管理者・立案設計者・検収者・運用実行者の役割を求められます。	１．電子カルテシステムを止める判断ができる人やインシデント発生時の対応主体となる方などが望ましいです。もし記載のような内容であればインシデントが発生した際の対応を前もって確認しておく必要があるでしょう。またセキュリティインシデントが発生したときに経営者が責任をとる必要があることを前もって伝えておきましょう。半田病院も大阪急性期も管理者や総長、病院長などが記者会見の対応をされています。
3	紙レセプトでレセコンもない医療機関でも、医療情報システム安全管理責任者を置く必要がありますでしょうか？	まったく端末やシステムがない環境であれば必要ありません。
令和5年度中 ＞2 医療情報システムの管理・運用＞（１） サーバ、端末PC、ネットワーク機器の台帳管理を行っている。		
1	管理台帳において独立したシステムと接続されている全く外部につながっていないPCやプリンターなどは台帳での管理が必要となりますか	はい、情報資産は組織の管理台帳の対象です。
2	台帳管理にて、記載するソフトウェアの例として「OS、Office、Adobe」が挙げられておりましたが、インストールされている必要なソフトウェアは全て台帳に記載するという認識でよろしいでしょうか。	はい、わかる範囲でソフトウェアの台帳管理を行ってください。ツールなどを用いて運用すると負荷も軽減するでしょう。
3	台帳管理やアカウント管理に連動して、パスワード管理もついて回ることかと思いますが、パスワード管理に関すること（保存方法・参照権限）が気になります。	パスワードは平文で保存されていると簡単に漏洩するなどリスクを伴うため暗号化することが必要です。またパスワードは基本的にすべて個別にするものであり、共有するものではありません。 （参照権限の意図が充分に汲み取れず、上記回答といたしました。）
4	端末PCについては令和５年度は参考項目としていますとありますが、端末PCとは具体的にどのようなものを指しますか。イメージが湧く例を教えてください。	電子カルテ端末や検査機器などです。
令和5年度中 ＞2 医療情報システムの管理・運用＞（３） 事業者から製造業者/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）を提出してもらう。		
1	情報システム調達の仕様書に必要要件として、MDSの提出を入れることは可能でしょうか？	含めることが望ましいです。
2	医療機器ベンダーに依頼したところMDS2（製造業者による医療機器セキュリティ開示書）しか提出できないと言われたが、それで問題ないでしょうか。	恐れ入ります状況がわかり難く、頂いた内容だけで問題の可否を判断することができません。
3	MDS/SDSは、放射線や臨床検査の医療機器ベンダーはどのように扱えばよいのですか。	同様に提出を求めてください。
4	人事給与システムは職員の情報は扱うが、患者情報は扱わない。したがってベンダー側はチェックリストや開示書の提出は不要と言っております。しかし当院の環境では人事給与システムも電子カルテと同じネットワーク、電子カルテ端末と相乗りで人事給与システムも利用しております。この場合でも人事給与システムのベンダーのチェックリスト及び開示書の提出は不要なのでしょうか？	患者情報の有無で判断すべきであり、人事給与システムそのものに無ければ不要と思われますが、組織のITガバナンスの視点からはベンダーと連携を行い、インシデント発生への備えやセキュリティ強化を実施すべきと思われます。
5	本院では事業者に対して、総務省・経済産業省が定めている「医療情報を取り扱う情報システム・サービスの提供事業者における安全管理ガイドライン」における「サービス仕様適合開示書」の提出を求めているが、「サービス仕様適合開示書」を受領していても別途「医療情報セキュリティ開示書（MDS/SDS）」を提出してもらう必要があるのか。	機器やサービスそのものの詳細はMDS/SDSでしか確認ができないと思われるため、提出いただく必要があります。
令和5年度中 ＞2 医療情報システムの管理・運用＞（４） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。		
1	当院、電子カルテシステムの運用に際し、利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定し、電子カルテシステムは利用できるようにしています。 ソフト面では権限設定ができており「はい」となると考えています。しかし、そのサーバあるいはクライアント自身（ハードウェア）には、共通のアカウントを利用して入ることができる状況です。 つまり、患者情報を見るためには利用者毎の権限設定で動いているのですが、サーバや端末のハードは利用できてしまいます。 この仕組みで動かしている医療機関がほとんどだと思うのですが、この状況では適合していないということで「いいえ」になってしまいますでしょうか？	今年度の対応としては「いいえ」です。アップデートなどについては参照環境を検証環境にするなどの工夫が必要です。
2	PCを利用する為の、ログインユーザーなのか、医療システムを利用する為のログインユーザーなのか、何が対象か教えていただきたい。	患者情報を取り扱う端末のログインユーザー、医療システムを利用するログインユーザー双方です。
3	アクセス制限やログイン時のパスワード管理について権限者の設定は経営者の他にどの役職までに限定するのが望ましいか？現場責任者に権限がない場合に想定されるリスクと理由について教えて頂けますと幸いです。	役職で限定するよりもシステムやセキュリティ判断や対応が行える人など、権限は可能な限り限定すべきです。現場責任者で作業を行う場合に必要な変更が行いにくくなるなどの影響があるのではないかと思われます。

#	ご質問	回答
4	どの様な端末環境を想定しての質問でしょうか。電子カルテシステムがオンプレミス or クラウドどちらの運用を想定していますか。そもそも電子カルテ端末が1人1台を想定しているのでしょうか。アカウント管理等1台を複数の職員が使用する場合、ログインアカウントは職員個々に設定しているものなのでしょうか。	オンプレ、クラウド双方です。組織で利用しているシステムのアカウントで医療情報システム対象の全てです。
5	日立の電カル（Open-Karte)を使ってますが、アカウント管理できるシステムがないので対応できません。電カルのメーカーを変えるしかないでしょうか？	アカウント管理ができる仕組みの方が望ましいとはお思いますが、AD等を用いてのアカウント管理など、既存のサービス等で行えるアカウント管理を実施しましょう。
6	利用者とはサーバOSログインアカウントと情報システム利用アカウントのどちらを指していると理解すれば良いでしょうか。	双方です。今年度はサーバ側の想定です。
7	立入検査対策コースの研修ありがとうございます。大変参考になりました。 当院は、電子カルテではなく紙カルテを使用しており、会計システム（レセプトコンピュータ）で請求をしています。①「２(４)利用者の職種・担当業務別の情報区分の毎のアクセス利用制限を設定している」でレセコンの立上げ時にパスワードを設定することはできるのですが、医事課以外のスタッフが使用することはないため、個人のアクセス管理はできていません。立上げ時にパスワードを設定していれば「はい」でよろしいでしょうか。②「2(5)退職者や使用していないアカウント等、不要なアカウントを削除している」で①と同様で個人アカウントを設定しておらず、ネットワークにも接続していないので削除するものがない場合は「はい」でよろしいでしょうか。	①ログインIDやパスワードも個別に設定し、誰が使用・アクセスしているのかなどが把握できる環境であれば「はい」となります。 ②グループアカウントではなく、基本的には各アカウントの付与を行い管理する必要があります。根本的なアカウント設定に課題があると思われ、「いいえ」になると思われます。
令和5年度中 ＞2 医療情報システムの管理・運用＞（５） 退職者や使用していないアカウント等、不要なアカウントを削除している。		
1	使用していないアカウントを削除しないで無効化するとは、具体的にはどういうことでしょうか？	例えば、一時的な休職などで組織には属しているが一定期間使用しないアカウントを削除するのではなく、無効化するなどの運用が行われている場合があります。
2	電子カルテ上で、退職者等のアカウントを削除することは、診療履歴や連続性を踏まえれば避けた方が良いのではないか。アカウント無効ではダメなのか。また、本研修の資料を院内で共有したいが、PDF等で頂くことはできないか。	アカウント無効化でも問題はないものと考えます。
令和5年度中 ＞2 医療情報システムの管理・運用＞（６） アクセスログを管理している。		
1	異常なアクセスと正常なアクセスの区別はどのような観点で判断するのでしょうか？ また、複数のサーバや数百台の端末の実行ログを人の目で24時間365日ログ調査することは事実上不可能です。例にあった異常なアクセス回数もその一つと思いますが、それだけではないですし、関連機器のログを保存する仕組みと異常時に発報するシステムが必要だと思います。そのようなシステムの具体名(複数推奨)や費用感を明示していただきたく思います。（可能であれば、経営層研修時に必要経費として理解できるように啓蒙していただければ幸いです。	24時間365日の監視体制を求めているわけではなく、できる範囲でログを管理し運用することが大切です。既存のセキュリティ製品の例として、ADやFW、セキュリティ対策ソフトなどの活用でもログ運用の1つの形です。またセキュリティパッチや定義ファイルの更新についてはガイドラインにあるよう常に最新の保つように記載しておりますので、ご対応をお願いします。
2	アクセスログの管理ですが、一台のマシンを複数人で使用している場合 また、一人に一台のPCがない場合、アクセス管理等はどのようにすると良いでしょうか?	端末の操作ログとアプリ側の操作ログを突合できるようにしておいてください。
3	アクセスログの管理は、医療情報システムのどこまでが範囲となりますか？ たとえばモダリティ装置は、画像システムと接続されています。一部のモダリティは保守のため各社とオンライン接続されておりＯＳはWindowsです。その場合、リモート機器だけでなく、モダリティ装置自体のログの管理も行わないといけないのでしょうか？ 最後に、本年度は、モダリティは端末扱いとなり回答の範囲外となるのでしょうか？	はい、ご記載の通りモダリティも含まれます。今年度の対象範囲外です。
4	アクセスログはシステムそれぞれ作成され、一日でも膨大な件数となる。これを、日々管理・チェックするには労力がかかりすぎると感じる。具体的に、どのような方法でログを収集し、どのレベルで管理・チェックを行うのか、例を挙げていただけますと幸いです。	まずはFWなどのセキュリティ製品のログ状況を優先的に行うことが望ましいでしょう。医療システムを対象としたものではないですが、一般的な内容してこちらをご参照ください。 https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/admin/22.html
5	アクセスログを管理する方法として、標準のWindowsのログでは管理が難しい点もあると思います。より管理がしやすいアプリなどありましたらご紹介していただきたいです。	個別アプリ等のご紹介は差し控えさせていただきます。
6	システム責任者について、専門性の知識を持たない、責任者でもよいのか？ リモートメンテナンス（保守）とはどこまでのものを指すのか？ 業者に確認すべきか？ アクセスの利用権限については、当院は電子カルテではなく、部門システム（医療情報システム）の運用となるが、PCを皆で利用しており、各個人ごとにログインID等を付与していない。その場合、ログの管理にもつながるのだが、そのPCにその時間、何をしていたかぐらいしかわからないと思うのだが、それでもここでいうログの管理に該当するのか？	組織の考え方によって責任者は異なると思われます。基本的には最低限の知識を持ち、判断できる人または委譲できる人が望ましいでしょう。リモートメンテナンスとはネットワークを通じ外部から患者情報を含むシステムに遠隔でアクセスし、操作できる状況です。基本的にはベンダーに確認したほうが良いと思われます。
令和5年度中 ＞2 医療情報システムの管理・運用＞（７） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。		
1	【2 医療情報システムの管理・運用＞(7)セキュリティパッチ】&【2 医療情報システムの管理・運用＞(8) 接続元制限を実施】 医療情報システムの導入・更新の間隔は5～7年であることが多いが，すでに導入・更新されているシステムの場合，導入・更新時の契約事項にセキュリティパッチにすべてのプログラムが対応できるように随時対応する旨が含まれておらず，今後，1～2年内（令和6年度まで）に対応するというのは現実的に難しい．そもそも国内の電子カルテのメインベンダーはどこも，システム導入時のＯＳのまま動かすことでしか，すべてのプログラムの動作保証をしないことを前提にしており，最新のセキュリティパッチをあてることを保守の範囲内とは考えてないところが多いので，ベンダーと相談しても，次回のシステム更新の時期までの解決は見出せそうにありません．もしそのような対応をベンダーに求めるにしても，莫大な追加費用がかかることが見込まれるが，昨今のコロナ後の病院の収支を考えると，そうした費用を捻出することは，ほぼ不可能です．前にも後にも進めないこのような現場での状況をご存じのうえで，今回のご提案をされているのでしょうか．とても現実的とは思えません．しかも，セキュリティパッチのために，インターネット経由での日常的な更新を推奨しておられますが，メインシステム・サブシステムすべてにそうしたパッチ更新のための外部接続を増やすということは，ゼロトラストの考え方からいくと，セキュリティ上のリスクをかえって増やすようにも思います．そのあたりのバランスはどのようにお考えなのでしょうか．	【医療情報～】 本来の運用保守の契約がどのようになっていたのか、まずは確認とベンダーとの議論が必要だと思います。また厚生労働省のセキュリティガイドラインや通達においてもソフトウェアの更新においては従前から対応を促しています。費用を一病院に求めるベンダーの対応にも課題があると思われます。実際に提供しているベンダーは導入タイミングがそれぞれ異なりますので、それぞれのタイミングでのOSや最新のビルドで納品をしていると思われます。このように考えると同じOSだとしても新しいものを利用されている可能性があり、導入・稼働実績もあると考えることができます。そのため、当時のOSでサポートが切れているOSを使わせ続け、病院側にリスクを受容させている姿勢にも課題があると思われ、ベンダーと議論いただくことが必要と思われます。さらに、OSのパッチ適用が難しいとしてもセキュリティ製品やネットワーク機器の更新はエンドポイントほどの影響は考え難く、まずは更新できるソフトウェアを見定めることも必要と思われます。また古いOSを使用し続けなければならない場合は不正な通信やインシデントを検知できる体制を確保することができれば、イベントやインシデントに気づくことが可能であり、医療情報システムの安全性を確保することも可能です。 最後に、ゼロトラストはそもそもクローズドの世界での議論ではなく、基本的にはオープンの世界での話であり、また根本的にクローズドの考え方は昨今のソフトウェアやシステム構成からは考え難いのが現状です。端末やネットワークはいわば包丁を使うことであり、適切に使えば脅威になることはありませんが適切に利用しないために昨今ではサイバー攻撃を受けています。つまり、ゼロトラストは様々なものをつなげ、様々なデータソースを用いて各組織のポリシーを作り、それぞれのリソースに対するすべてのアクセスを許可、拒否するものです。また医療DXの流れからもつなげない接続を伴わないシステムは考え難いでしょう。 *通達：薬生機審発１０２０第１号（平成 29 年１０月２０日）「医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて」 https://www.jaame.or.jp/mdsi/pdf/other/291020kiki102001.pdf?fbclid=IwAR081ytXZLMOWsQB4y_6PmxBa5vKGTonkiv0aBd7vHR7INOA5E_4WU96JFs

#	ご質問	回答
2	どのように交渉を行っても対応に応じてくれない医療機器ベンダーが多数存在する。 ガイドラインでセキュリティパッチの適用をするよう促されていると伝えても、現状のOSの構成で認可を受けた医療機器のため、変更は絶対にできないと言われる。 どうすればよいでしょうか。	厚生労働省の通達をベンダーにお伝えください。
3	UTM（FW）や保守回線用ルータのファームをアップデートするのは重要かと思いますが、スイッチングHUBのファームウェアまでアップデートする必要はあるのでしょうか。	「ある」と考えます。
4	サイバーセキュリティ対策チェックリストのうち、『2 医療情報システムの管理・運用』の『ネットワーク機器について、以下を実施している。』の『(7)セキュリティパッチを適用している』及び『(8)接続元制限を実施している。』については、ネットワーク末端の無線ルーターなどの一部の機器については確認、適用しきれていないものがあるものの、ファイアウォール機器、コアスイッチ、フロアスイッチ等の主要なネットワーク機器については、いずれも適用、実施しております。この対応状況ですとはチェックリスト「はい」もしくは「いいえ」のどちらになるでしょうか？	「いいえ」となります。基本的にはすべての資産の脆弱性対応をお願いします。
5	セキュリティパッチの適用で、インターネット接続が前提となる発言があったが、現在閉域網で利用している医療機関は、具体的にどのようなセキュリティ対策を追加すれば外部接続しても良いのか基準や指針を示して欲しい。また、その際発生する費用について、モデルケースで良いので示して欲しい。単純に閉域網神話は捨ててと言われても困る。	医療情報システムの安全管理に関するガイドラインをご覧いただくとよいかと考えます。
6	ソフトウェアを更新する必要があるが、動作確認等のため、一時的にシステムが使用できなくなることがネックとなり実施が難しい場合、どのように進めていくのが良いか御教示ください。	参照環境を用いての検証や動作確認を行い、本番環境に影響が出ない形での検証が望ましいと思われます。
7	各ベンダーが存在するサーバーのセキュリティパッチ対策は、閉域網の概念で対応していたがこれをまとめて対応するとなるとどうすればよいのか？	マイクロソフト社の製品でWSUSを用いるなど、一元的にパッチやモジュール更新が行えます。このような対応を含め、外部接続を含めた対応の検討を行う必要があると思われます。
8	保健所職員です。病院監視の際に、全ての病院から「セキュリティパッチを当てることにより、システムが数時間障害状態になるインシデントは広く一般にみられる。病院の場合、これが人命を損なう程度の脅威をもたらしうるため、パッチを当てること自体がリスクである、という強い警戒がある。たとえ夜間に適用作業を行うにせよ、入院患者を危険に晒すことには変わりがない。また、特に救急病院の場合、夜間であろうがいつであろうが危険である。よってセキュリティパッチの適用自体を危険視している」という相談を受けております。 １．長時間障害のリスクと患者への生命レベルでの脅威をもってしても、セキュリティパッチを当てることは強行すべき、ということになるのでしょうか。 ２．上記の弊害を理由に、病院が納得しない場合、どのような説得を行うべきでしょうか。 ３．万一、セキュリティパッチ適用による長時間障害インシデントが発生した場合、その場においてはどのように対応すべきでしょうか。 ４．また、事後的な病院への補償等の体制は何かしら予定されているのでしょうか。	１．環境に依存すると思います。 ２．完全なる閉域網であれば更新をしなくても良いとは思いますが、そのような環境ではないと思います。計画停電時を活用した更新を行っているなど、他機関では工夫をして更新しています。 ３．そうならないように事前に検証をしていただく必要があると思います。 ４．各契約に異なると思われます。
9	令和6年チェックリストにおける、医療情報システムの管理・運用の「（７）セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。」に関して、ほとんどのシステムベンダーから【不可能】という回答がされると想定されます。（サーバー・クライアントどちらも） 理由としては、システムベンダーの保守契約書には「OSのセキュリティパッチは導入時のバージョンでの動作を保証するものであり、それ以降のセキュリティパッチに関しては保証しない」と明記されていることが多いからです。加えて最新のセキュリティパッチに対する動作検証には数ヶ月の期間を要するものだと思われますので現実的にも難しいと思われます。また、もし最新のセキュリティパッチをサーバーにあてるとなると、その度にシステムを停止して再起動する必要が出てくると思われます。電子カルテなどコアなサーバーは停止することが難しいため、１年に１度程度しか難しいと思われます。 セキュリティパッチの適用に関して許容範囲等があれば教えていただきたく。	記載の契約であれば更新は難しいかもしれませんが、厚生労働省としてはソフトウェアの更新を促しています。参照サーバの活用など冗長構成の検討が必要だと思われます。また頻度については組織によっても異なるため、ガイドラインに記載があるよう最新の状態をできる限り保つようにしてください。 *通達：薬生機審発１０２０第１号（平成 29 年１０月２０日）「医療機器プログラムの一部変更に伴う軽微変更手続き等の取扱いについて」 https://www.jaame.or.jp/mdsi/pdf/other/291020kiki102001.pdf?fbclid=IwAR081ytXZLMOWsQB4y_6PmxBa5vKGTonkiv0aBd7vHR7INOA5E_4WU96JFs
その他		
1	立入検査における本チェックリストの対象範囲は患者情報を扱うものということでしたが、放射線画像診断機器やエコー、心電図等の医療機器も対象に含まれているのでしょうか。 医療機器ベンダーから、本チェックリストの対象ではないと言われることが多々あります。 病院から医療機器ベンダーに伝えても、できないの一点張りのベンダーが多い状況で、病院への指導を行う前に、医療機器ベンダー等への指導や法整備が先ではないでしょうか	患者情報が含まれるものは対象です。
2	警察のサイトを見て、インシデント発生時の緊急連絡先をまとめようとしていたが、厚生労働省など他にも連絡先があることがわかりました。リストの抜けがあるかもしれないので、ランサムウェア被害が発生した時の連絡先のサンプルをいただきたいです。	https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html 医療機関等がサイバー攻撃を受けた場合の厚生労働省連絡先 医政局特定医薬品開発支援・医療情報担当参事官室 TEL： 03-6812-7837 MAIL： igishitsu×mhlw.go.jp ※迷惑メール防止のため、メールアドレスの一部を変えています。 「×」を「@」に置き換えてください。
3	病院情報とは切り離した運用ですが、がん登録のような患者情報を扱う機器も対象となりますか。	患者情報が含まれるものは対象です。
BCP		
1	サイバー攻撃を想定したBCPの作成に難渋しています。参考となるフォーマットや作成例をご教示いただけますと幸いです。	参考に、当該事業内の研修をご覧いただけましたらと考えます。
2	医療機関におけるサイバーセキュリティに対応するBCPモデルがあれば参考にさせていただき、急ピッチで全施設へモデルの展開、アップデートを図っていきたいと考えている。	

#	ご質問	回答
ペナルティに関する事項		
1	システムの作りの都合等で、サイバーセキュリティ対策チェックリストの項目内容を満たせないということはチェックリストの内容的に往々にして発生するかと思うのですが、メーカーが対応するまでは永久に「はい」にならなくても問題ないのでしょうか。また、チェックリストで「いいえ」の項目が残っている場合でも特に罰則等は無いという認識で間違いないでしょうか。	現状罰則はございませんが、立入検査で指摘があった内容について改善がみられない場合等において、法第24条第２項における改善命令が出されます。
2	その他： 年度末までに、当該チェックリストへの対応がなされなかった場合は、どのような対応をなされるご予定でしょうか？ チェックリストへの対応について、「いいえ」の場合は年度末までに「はい」となるように取組み、各施設にて自己点検を行うとのことですが、 翌年の立入り検査の際に、確認をなされるということでしょうか？それとも例え「いいえ」だったとしても特に確認はなされないのでしょうか？ もし翌年確認がなされるのであれば、「いいえ」の場合は、改善指導ということになるかと思いますが、それでも改善できなければ、 監査の対象となるのでしょうか？また、その後はよりすすんで、取消処分、戒告、注意といった行政措置の執行ということになる内容なのでしょうか？ どうぞよろしくお願いいたします。	