Q番号	調査項目
Q1	回答者の情報（氏名、所属、連絡先）
Q2	医療情報システム安全管理責任者（システム管理者）を設置しているか。
Q3	サイバー攻撃またはサイバー攻撃の兆候を認めた際に連絡するべき医療情報システムの保守ベンダー・所管官庁等の連絡先を把握しているか。
Q4	厚生労働省などから発出されるサイバー攻撃に係る注意喚起や脆弱性情報を日頃から収集・確認しているか。
Q5	自組織が使用している情報機器・システム・サービスが「医療情報システムの安全管理に関するガイドライン」に準拠しているかを確認するために、一般社団法人保健医療福祉情報システム工業会（JAHIS）および一般社団法人日本画像医療システム工業（JIRA）が策定した「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)」（厚生労働省標準）を用いて点検しているか。
Q6	サイバー攻撃等によるシステム障害発生時に備え、事業継続計画（BCP)を策定しているか
	Ｑ６－１は、Ｑ６に対して「はい」を選択した方が対象となる質問です。 「いいえ」を選択した場合は、Ｑ７に進んでください。
Q6-1	事業継続計画（BCP)において策定された対処手順が適切に機能するか、訓練等により確認しているか。
Q7	自組織において、電子カルテシステムを使用しているか。 ※電子カルテシステムは「オーダリング機能、画像管理等の部門システム及び診療録を電子的に記録する機能を備えた統合的な医療情報システム」を指す。
	Ｑ８は、Ｑ７に対して「はい」を選択した方が対象となる質問です。 「いいえ」を選択した場合は、Q11に進んでください。
Q8	電子カルテシステムのバックアップデータ作成について、当てはまるものを選択してください。 ①バックアップデータを１つ作成している ②バックアップデータを２つ以上作成している ③バックアップデータを作成していない
	Ｑ９およびＱ９－１は、Ｑ８に対して「②バックアップデータを２つ以上作成している」を選択した方が対象となる質問です。 「①バックアップデータを１つ作成している」を選択した場合はQ10に、「③バックアップデータを作成していない」を選択した場合はQ11に進んでください。
Q9	バックアップデータの作成方式について、当てはまるものを選択してください。 ①「追記可能な設定がなされた媒体」と「追記不能設定がなされた媒体」を組み合わせて取得している。 ②「追記可能な設定がなされた媒体」または「追記不能設定がなされた媒体」のどちらか一方のみで取得している。
Q9-1	バックアップデータのうち、一つは、端末及びサーバ装置やネットワークから切り離された環境（オフライン）で保管しているか。
	Q10からQ10－２は、Ｑ８に対して「①バックアップデータを１つ作成している」または「②バックアップデータを２つ以上作成している」を選択した方が対象となる質問です。

Q10	電子カルテシステムのバックアップデータの更新頻度について、当てはまるものを選択してください。 ①１か月以内に１回 ②１か月～３か月以内に１回 ③３か月～半年以内に１回 ④半年～１年以内に１回 ⑤バックアップデータを更新していない
Q10-1	バックアップデータは、複数の時点による保存（世代管理）をしているか。
Q10-2	バックアップデータは、漏洩対策を講じているか。 (例：バックアップデータの暗号化、秘密分散管理、アクセス権限の設定)
	Q11からQ13は、令和４年11月10日に厚生労働省より発出された事務連絡「医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）」を参照の上、回答すること。
Q11	「１　サプライチェーンリスク全体の確認」に記載の内容をもとに、関係事業者のセキュリティ管理体制を確認し、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施したか。
Q12	「２　リスク低減のための措置」に記載の内容を確認し、自組織に必要な措置を講じたか。
Q13	「３　インシデントの早期検知」に記載の内容を確認し、各種ログの確認・通信の監視などを行ったか。
	Q14およびQ15は、回答にあたり院内のサーバ室等を点検し、リモートゲートウェイ装置（以下「VPN機器」）が存在するか保守ベンダー含め確認した上、回答してください。 確認の結果、VPN機器が設置されていない場合は、次問以降の回答は不要ですので、回答を提出してください。
Q14	自組織内のVPN機器の設置場所を把握しているか。 ※自組織が設置したものだけでなく、保守点検等を目的に、保守ベンダーや業務外注事業者が設置したVPN機器を含む。
Q15	VPN機器は、Fortinet製品を使用しているか。使用している場合、機種名・台数・OSのバージョンをすべて記載すること。
	Q16からQ16－２は、Fortinet製品のVPN機器を使用している病院が対象となる質問です。回答にあたっては、令和４年12月16日に厚生労働省より発出された事務連絡「FortiOSに関する脆弱性情報への対応について（注意喚起）」を参照の上、回答してください。 Fortinet製品以外のVPN機器を使用している病院は、Q17に進んでください。 なお、Fortinet製品およびFortinet製品以外の複数のVPN機器を設置されている病院におかれても、Fortinet製品以外のVPN機器についてQ17にご回答ください。
Q16	Fortinet製品の脆弱性情報に基づき、対象となるソフトウェアが使用されているか及びサポート期限が切れていないか確認したか。または、医療情報システムの保守ベンダーに確認を依頼したか。
Q16-1	（Q16において確認した、対象のソフトウェアを使用していた病院は回答すること） 最新のソフトウェアにバージョンアップを実施したか。
Q16-2	VPN機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施しているか。
	Q17からQ17－２は、Fortinet製品以外のVPN機器を使用している病院は回答してください。 Fortinet製品のVPN機器が設置されている場合は、次問以降の回答は不要ですので、回答を提出してください。
Q17	VPN機器のメーカー名・機種名・台数・OSのバージョンをすべて記載すること。

Q17-1	VPN機器は最新のソフトウェアが使用されているか、また、サポート期限を把握し、アップデートを適切に行っているか。
Q17-2	VPN機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施しているか。