Seq.No.	編	セクション	表題	項番	内容	CFS	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	管理編	1.1	なし	①	医療情報の安全管理に関する法令等を遵守すること。	C	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	管理編	1.1	なし	②	医療機関等で業務に従事する職員や関係するシステム関連事業者等に対して、医療情報システムに関係する法令等を遵守させること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	管理編	1.2.1	説明責任	①	医療情報システムの安全管理に関して、原則として文書化し、管理する体制を整えること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	管理編	1.2.1	説明責任	②	患者等への説明を適切に行うための窓口の設置等の対策を行うこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	管理編	1.2.1	管理責任	①	医療情報システムの安全管理に関する管理責任を適切に果たすために必要な組織体制を整備すること。	A,B,C,D,E,F	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	管理編	1.2.1	管理責任	②	定期的に管理状況に関する報告を受けて状況を確認するとともに、組織内において監査を実施すること。	C,G	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	管理編	1.2.1	定期的な	①	医療情報システムに関する安全管理を適切に維持するための計画を策定すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	管理編	1.2.1	定期的な	②	医療情報に関する安全管理を適切に維持するために、定期的な見直しを実施し、必要に応じて、改善措置を講じるよう、企画管理者及びシステム運用担当者に指示すること。	H,J,T,V	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
9	管理編	1.2.2	管理責任	①	情報セキュリティインシデントが生じた場合、患者の生命・身体への影響を考慮し、可能な限りの医療継続を図るとともに、その原因や対策等について患者、関係機関等に説明する体制を速やかに構築すること。	B,O,P,Q,R,S,W	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	1	0	0	0
10	管理編	1.2.2	善後策を	①	情報セキュリティインシデントが生じた場合、医療機関内、システム関連事業者及び外部関係機関と協働して、インシデントの原因を究明し、インシデントの発生や経緯等を整理すること。	P,R	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0
11	管理編	1.2.2	善後策を	②	情報セキュリティインシデントが生じた場合、その原因を踏まえた再発防止策を講じること。	T,V	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
12	管理編	1.2.2	善後策を	③	①②の対応を可能とするため、通常時から非常時を想定し、システム関連事業者や外部関係機関と協働関係を構築するとともに、再発防止策を検討できるよう、通常時から非常時を想定した体制や措置を講じておくこと。	B,F,J	0	1	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	管理編	1.3.1	なし	①	医療情報システムの安全管理について、システム関連事業者に委託する場合は、法令等を遵守し、委託先事業者の選定や管理を適切に行うこと。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	管理編	1.3.2	なし	①	業務等を委託する場合には、委託する業務等の内容及び責任範囲並びに役割分担等の責任分界を明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に契約等の取決めを実施し、保管すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	管理編	1.4	なし	①	医療情報を第三者提供する場合、法令等を遵守し、手続き等の記録等を適切に管理する体制を整備すること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	管理編	1.4	なし	②	医療情報を第三者提供する場合、医療機関等と第三者それぞれが負う責任の範囲をあらかじめ明確にし、認識の齟齬等が生じないよう、書面等により可視化し、適切に管理すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	管理編	2.1	なし	①	取り扱う医療情報に応じたリスク分析・評価を踏まえ、対応方針を策定し、リスク管理方針（リスクの回避・低減・移転・受容）を決定すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	管理編	2.1	なし	②	リスク分析を踏まえたリスク管理が必要な場面の整理、対策として求められる体制、並びにルール等の企画、整備及び管理について、企画管理者に指示すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	管理編	2.1	なし	③	経営層の方針及びリスク分析を踏まえ、具体的にシステム面からの最適なリスク管理措置を検討し、実装、運用するよう、企画管理者に指示すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	管理編	2.2.1	なし	①	リスク評価を踏まえ、医療情報の重要性及び医療の継続性並びに経営資源の投入及びリスク管理対策の実施の継続可能性等を鑑みて、リスク管理方針を決定すること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	管理編	2.2.1	なし	②	リスク評価結果及びリスク管理方針に関する説明責任を果たすこと。	D,E,F?	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	管理編	2.2.2	なし	①	リスク管理方針を踏まえ、医療情報及び医療情報システムといった医療機関等における情報資産のセキュリティに関する管理を、通常業務の一環として整え、ISMSを策定し、実施すること。	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	管理編	2.2.3	なし	①	医療機関等のリスク管理方針に基づき、システム関連事業者による適切なリスク管理を実施し、医療機関等の要求仕様への適合性を確認し、管理すること。	C?	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	管理編	3.1	なし	①	統制の体系を理解し、医療機関等における情報セキュリティ対策に関する統制の実効性を担保するために必要な規程類、管理体制等を整備するとともに、適切に統制が機能しているかを確認すること。	A,C	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	管理編	3.1.2	なし	①	医療機関の規模や組織構成、特性等を踏まえた統制の内容を検討すること。	B,C	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	管理編	3.1.2	なし	②	医療機関等において安全管理を直接実行する医療情報システム安全管理責任者及び企画管理者を設置すること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
27	管理編	3.1.2	なし	③	情報セキュリティに関する統制は、医療機関等内の組織や人事等の統制とは区別し、医療機関等全体における統制の一つと位置付けて、組織横断的に実施すること。	C,H?	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	管理編	3.1.2	なし	④	情報セキュリティ対策に関する統制の対象には、医療機関等に直接雇用されている職員だけでなく、システム関連事業者の担当者や派遣社員など、医療機関等が直接雇用していない者も含むこと。	G,H	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	管理編	3.2	なし	①	リスク評価及びリスク管理方針を踏まえて、情報セキュリティ方針を整備すること。	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
30	管理編	3.2	なし	②	情報セキュリティ方針に基づき、自医療機関等の実態を踏まえて、実施可能な範囲で、実効性のある、適切な情報セキュリティ対策を整備するよう、企画管理者に指示し、管理すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	管理編	3.2.2	なし	①	整備した規程類を適切に利用し、情報セキュリティ方針を遵守した対策が実施できるよう、通常時から情報セキュリティ対策に関する統制対象者すべてに対して定期的な教育・訓練を実施すること。	H	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	管理編	3.3.1	なし	①	医療機関等において医療情報システムに関する安全管理対策が適切に実施されていることを確認するため、企画管理者やシステム運用担当者に定期的に自己点検を行うよう指示し、その結果報告を受け、必要に応じて改善に向けた対応を指示すること。	J?	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
33	管理編	3.3.2	なし	①	医療機関等内で、企画管理者及びシステム運用担当者から独立した組織による内部監査、または医療機関等とは異なる機関による外部監査を実施し、管理責任を果たすこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	管理編	3.3.2	なし	②	内部監査または外部監査の結果を踏まえ、必要に応じて、安全管理措置の改善に向けた対応を企画管理者やシステム運用担当者に指示するとともに、その対応結果をフォローすること。	T,V ?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
35	管理編	3.4.1	なし	①	情報セキュリティインシデントの発生に備え、非常時における業務継続の可否の判断基準、継続する業務内容の選定等に係る意思決定プロセスを検討し、BCP等を整備すること。	B,J	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
36	管理編	3.4.1	なし	②	情報セキュリティインシデントにより、医療機関内の医療情報システムの全部または一部に影響が生じる場合に備え、医療情報システムの適切な復旧手順を検討するよう、企画管理者やシステム運用担当者に指示するとともに、当該復旧手順について随時自己点検を行うよう指示した上で、その結果報告を受け、必要に応じて改善に向けた対応を企画管理者やシステム運用担当者に指示すること。	B,J,U,V	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0
37	管理編	3.4.2	なし	①	情報セキュリティインシデントの発生に備え、システム関連事業者又は外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示すること。	A,C,F,H,Q	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
38	管理編	3.4.3	なし	①	情報セキュリティインシデントの発生に備え、厚生労働省、都道府県警察の担当部署その他の所管官庁に速やかに報告するために必要な手順や方法、体制などを整備するよう、企画管理者に指示すること。	O,Q?	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0
39	管理編	3.4.3	なし	②	情報セキュリティインシデントが発生した場合に、厚生労働省等への報告の他に、患者等に対する公表・広報を適切に行える体制を、通常時から整備すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	管理編	4.1	なし	①	医療情報システムの安全管理に必要な対策項目（下記参照）の概要を認識した上で、企画管理者やシステム運用者に対して、それぞれの対策項目に係る具体的な方法について整理する旨を指示し、それぞれの対策事項が対応できている旨を確認すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	管理編	4.1	なし	②	対応ができていない対策項目がある場合、その理由を確認し、対応の要否を判断の上、必要に応じて対応を指示すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	管理編	4.2	なし	①	医療情報システムの安全管理対策項目の特徴を認識し、企画管理者やシステム運用担当者に、必要に応じて、対策項目に掲げられる措置をとるよう指示すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	管理編	5.1	なし	①	委託する事業者を選定する場合には、本ガイドライン及び法令等が求める要件を満たすシステム関連事業者を選定するよう指示すること。	A,F,H	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	管理編	5.1	なし	②	委託する事業者を選定する場合には、JIS Q 15001、JIS Q 27001またはこれと同様の規格の認証を受けているシステム関連事業者を選定するよう指示すること。	A,F,H	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
45	管理編	5.2.1	なし	①	委託契約において、委託業務の内容やシステム関連事業者の体制、システム関連事業者との責任分界、システム関連事業者における情報の取り扱い等、医療機関が負う医療情報システムの管理に関して、協働する上で認識の祖語が生じないように、適切な契約の締結や管理を行うよう企画管理者に指示すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	管理編	5.2.2	なし	①	委託するシステム関連事業者に対して、業務実行体制を明確にし、医療情報の取扱い及び医療情報システムの管理に関して再委託を行う場合には、事前に医療機関等に情報を提供し、協議・合意形成を経た上で承認を得ること等を契約の内容に含めるよう、企画管理者に指示すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	管理編	5.3	なし	①	システム関連事業者に委託を行う際の責任分界の管理に関する重要性を認識し、医療機関と委託先事業者との間での責任分界を明確にし、認識の齟齬等が生じないよう書面等により可視化し、適切に管理することを、企画管理者やシステム運用担当者に支持すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48	企画管理編	1	なし	①	医療情報システムの管理に関する法令等について理解し、医療機関等の組織全体として法令等を遵守できるよう、必要な措置を講じること。	C	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
49	企画管理編	1	なし	②	委託先の医療情報システム・サービス事業者（以下「委託先事業者」という。）等に対しても①に関して必要な措置を講じるよう契約において求め、その対応状況を定期的に把握すること。委託先事業者が再委託先を用いる場合にも同様の対応をすること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
50	企画管理編	1	なし	③	医療機関等内における法令の遵守状況について経営層に報告し、経営層の確認をとること。また、順守状況に応じて必要な改善措置を講じること。	C	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
51	企画管理編	1	なし	④	医療情報システムの安全管理に係る法令等が求める内容を把握した上で、対応策を整理すること。必要に応じて、システム運用担当者と具体的な対策について検討を求めて、その結果を反映すること。	A,B,C,D,E,F?	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
52	企画管理編	1	なし	⑤	組織における情報セキュリティ方針。医療情報の取扱いや保護に関する方針及び医療情報システムの安全管理に関する方針を策定し。経営層の承認を得ること。	A,B,C,D,E,F?	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
53	企画管理編	1	なし	⑥	⑤で経営層の承認を得た方針を実行するために必要な体制、規程、技術的措置等の整備を行うこと。またこれらが適切に運用されているか確認すること。	G,H,I,J,K,L?	0	0	0	0	0	0	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
54	企画管理編	1	なし	⑦	患者等からの照会に対応するために必要な医療情報システムの安全管理に関する窓口等を整備すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
55	企画管理編	2	なし	①	医療機関等において生じる責任の内容を踏まえて、委託先事業者その他の関係者との間で責任分界に関する取決めを行うこと。また、重要な委託等に関する責任分界については、取決めに当たり、事前に経営層の承認を得ること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
56	企画管理編	2	なし	②	取決めを行う責任分界のうち技術的な部分に関しては、その具体的な内容を検討するようシステム運用担当者に指示を行い、その結果を責任分界の取決めに反映させること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
57	企画管理編	2	なし	③	責任分界を取り決める際には、あらかじめ必要な情報を収集した上で、医療機関等におけるリスク管理を踏まえた仕様の適合性に関する調整を委託先事業者等と行うこと。	D,E,F?	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
58	企画管理編	2	なし	④	委託事業者等と責任分界の取り決めを行う際には、委託先事業者が提供する医療情報システム・サービスの内容を踏まえて、安全管理に関する役割分担についても取り決めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	企画管理編	2	なし	⑤	委託先事業者等において複数の関係者が関与する場合には、その関係を整理し、医療機関等が直接責任分界を取り決める相手を特定すること。また、関与する関係者への管理なども責任分界の取り決めに定めること。さらに、責任分界の取決めに際しては、委託先事業者間での役割分担なども含めて、取り決め内容に漏れがないよう留意すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
60	企画管理編	2	なし	⑥	第三者提供を行う際の責任分界については、技術的な内容と手続き的な部分の役割分担を含めて取り決めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
61	企画管理編	3	なし	①	医療情報システムの安全管理の責任を担う者としての位置づけ、その業務範囲と権限を明確にし、その内容について経営層の承認を得ること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
62	企画管理編	3	なし	②	情報システム管理委員会等の組織が構成されている場合には、その業務内容、権限等の運営に関する規定を策定し、経営層の承認を得ること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	企画管理編	3	なし	③	安全管理に関する技術的な対応を行う担当者を任命し、その業務内容、権限、業務上の義務等を明確にし、経営層の承認を得ること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
64	企画管理編	3	なし	④	非常時の対応を想定して、安全管理に必要な体制を構築すること。特に医療機関等において発生した情報セキュリティインシデントに対処するための体制として情報セキュリティ責任者(CISO)やCSIRTなどの要否を検討し、必要な措置を講じ、その結果を経営層に報告し、承認を得ること。	B,H,J	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
65	企画管理編	3	なし	⑤	法律上の対応を含め医療情報の漏洩が生じた際の必要な体制の構築や手順の策定等の必要な措置を講じ、その結果を経営層に報告し、承認を得ること。	B,J	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
66	企画管理編	3	なし	⑥	医療機関等内における医療従事者や職員等に対して、医療情報の安全な取扱いに必要な教育や訓練を講じるための体制を整備すること。	H	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
67	企画管理編	3	なし	⑦	医療情報の取扱いに関して委託等を行う場合には、委託先事業者を含めた安全管理に関する体制を整備すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
68	企画管理編	3	なし	⑧	医療情報の取扱いの安全性が確保できるよう、内部検査及び監査等の体制を構築すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
69	企画管理編	3	なし	⑨	患者等からの相談や苦情への対応を行うための体制を構築すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
70	企画管理編	3	なし	⑩	①～⑨までの対応については、整備した内容を可視化できるようにすること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
71	企画管理編	4	なし	①	医療機関等が医療情報システムの安全管理に関して定める各種方針等を実現するために必要な規程等の整備を行い、経営層の承認を取ること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	企画管理編	4	なし	②	規程等に基づいて、医療情報の取扱いや医療情報システムの構築、運用を行うために必要な規則類の整備を行うこと。規則類は必要に応じて見直しを行うこと。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
73	企画管理編	4	なし	③	医療情報システムの構築、運用における通常時の対応に必要なマニュアル類や各種資料の整備を担当者に指示し、確認すること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
74	企画管理編	4	なし	④	非常時における医療情報の運用等に関するマニュアル類や各種資料の整備を担当者に指示し、整備状況を確認の上、経営層に報告すること。	A,B,C,D,E,F,J	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
75	企画管理編	5	なし	①	医療情報システムの安全管理の状況を把握するために必要な証跡について整理し、当該証跡の整備について必要な対応を行うこと。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76	企画管理編	5	なし	②	証跡の整備に当たっては、証跡により管理する安全管理の対象の目的や特性に応じたものとすることに留意すること。また証跡の改竄等を防止する措置を講じること。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
77	企画管理編	5	なし	③	収集した証跡に対するレビュー等を行い、医療情報システムの安全管理の状況を把握し、必要があれば証跡の整備に関する改善を行うこと。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
78	企画管理編	5	なし	④	法令で求められる医療情報の管理に関する証跡を、必要に応じて、説明責任等を果たせるように管理すること。	K,L	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
79	企画管理編	6	なし	①	医療機関等内でリスクマネジメントが適切に実施されているかどうかを管理し、その状況を経営層に報告すること。また、リスクマネジメントに不備がある場合には、改善策を検討し、必要な措置を講じること。	C,D,E,F	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80	企画管理編	6	なし	②	医療情報システムで取り扱う医療情報及び関連する情報を全てリストアップし、安全管理上の重要度に応じて分類し、常に最新の状態が維持されていることを確認すること。	A,D,E,F	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
81	企画管理編	6	なし	③	医療情報システムで取り扱う情報及び関連する情報に関するリストを作成し、必要に応じて速やかに確認できる状態で管理すること。	A,D,E,F	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
82	企画管理編	6	なし	④	安全性が損なわれた場合の影響の大きさに応じて医療情報システムで取り扱う情報及び関連する情報の安全管理上の重要度を分類すること。	A,B,C,D,E,F	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	企画管理編	6	なし	⑤	②～④を踏まえて、リスク分析やリスク評価を担当者と協働して行うこと。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
84	企画管理編	6	なし	⑥	経営層がリスク評価を踏まえたリスク判断をする際に必要な資料を整理すること。	A,B,C,D,E,F	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
85	企画管理編	6	なし	⑦	リスク評価の結果、リスク管理の方針に関する説明責任に関する資料等を整理し、経営層が説明責任を果たすために必要な対応を行うこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
86	企画管理編	6	なし	⑧	リスク評価の結果を経営層に報告し、承認を得ること。また承認を踏まえて安全管理対策を講じること。	C,D,EF	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87	企画管理編	6	なし	⑨	PDCA(Plan-Do-Check-Act)モデルに基づくISMS(Information Security Management System: 情報セキュリティマネジメントシステム）を構築し、管理すること。また、ISMSが適切に実施されていることを確認し、経営層にその状況を報告すること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	企画管理編	6	なし	⑩	PDCAモデルの実施において不備等が認められる場合には、その原因を確認した上で改善策を講じ、経営層に報告し、承認を得ること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
89	企画管理編	7	なし	①	医療情報を取り扱う者を職員として採用するに当たっては、雇用契約に雇用中及び退職後の守秘・非開示に関する条項を含める等の安全管理対策を実施すること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
90	企画管理編	7	なし	②	個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施すること。また、教育・訓練の実施状況について定期的に経営層に報告すること。	C,H	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
91	企画管理編	7	なし	③	医療機関等の事務、運用等を外部の事業者に委託する場合には、委託契約の契約書に守秘・非開示に関する内容を含めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
92	企画管理編	7	なし	④	③の委託契約の際に、当該委託先事業者の就業規則に①及び②の対応を含めるよう求めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
93	企画管理編	7	なし	⑤－1	外部の事業者との契約に基づいて医療情報を外部保存する場合、以下の対応を行うこと。重要度の高い委託の場合は、経営層に丁寧に報告し、承認を得ること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
94	企画管理編	7	なし	⑤－2	一保存した医療情報の取扱いについて監督できるようにするため、外部保存の委託先事業者及びその管理者、電子保存作業従事者等に対する守秘義務に関連する事項やその事項に違反した場合のペナルティを契約書等で定めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	企画管理編	7	なし	⑤－3	一医療機関等と外部保存の委託先事業者を結ぶネットワークインフラに関しては、委託先事業者にも本ガイドラインを遵守させること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
96	企画管理編	7	なし	⑤－4	一総務省・経済産業省の定めた「懲労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」を遵守することを契約等で明確に定め、少なくとも定期的に報告を受ける等して遵守状況を確認すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
97	企画管理編	7	なし	⑤－5	一外部保存の委託先事業者の選定に当たっては、システム関連事業者の情報セキュリティ対策状況を示した資料を確認すること。（例えば、「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」の提供を求めて確認することなどが挙げられる。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
98	企画管理編	7	なし	⑤－6	一外部保存の委託先事業者に、契約書等で合意した保守作業に必要な情報以外の情報を閲覧させないこと。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
99	企画管理編	7	なし	⑤－7	一保存した情報（Cookie、匿名加工情報等、個人を特定しない情報を含む。本稿において以下同じ。）を独断で分析、解析等を実施してはならないことを契約書等に明記し、外部保存の委託先事業者に遵守させること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	企画管理編	7	なし	⑤－8	一保存した情報を外部保存の委託先事業者が独自に提供しないよう、契約書等で情報提供のルールについて定めること。外部保存の委託先事業者に情報の提供に係るアクセス権を設定する場合は、適切な権限を設定させ、情報漏洩や、誤った閲覧（異なる患者の情報を見せてしまう又は患者に見せてはいけない情報が見えてしまう等）が起こらないよう求めること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
101	企画管理編	7	なし	⑤－9	一保存された情報を格納する情報機器等が、国内法の適用を受けることを確認すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
102	企画管理編	7	なし	⑥	外部保存の委託先事業者を選定する際は、少なくとも次に掲げる事項について確認すること。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
103	企画管理編	7	なし	⑥－1	a:医療情報等の安全管理に係る基本方針・取扱規程等の整備状況		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
104	企画管理編	7	なし	⑥－2	b:医療情報等の安全管理に係る実施体制の整備状況		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
105	企画管理編	7	なし	⑥－3	c:不正ソフトウェア等のサイバー攻撃による被害を防止するために必要なバックアップの取得及び管理の状況		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
106	企画管理編	7	なし	⑥－4	d:実績等に基づく個人データ安全管理に関する信用度		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

| | | |

201	企画管理編	15	なし	④	医療情報システムが情報を保管する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップの頻度や方法等を明確にすること。これらを運用管理規定に定め、その運用を関係者全員に周知徹底すること。	G,H,I,J	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
202	企画管理編	15	なし	⑤	記録媒体の劣化への対応を図るための一連の運用の流れを運用管理規定に定めるとともに、関係者に周知徹底すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
203	企画管理編	15	なし	⑥	システム運用に関する安全管理対策として必要な項目を担当者と協働して検討すること。特に医療情報システムの脆弱性（不正ソフトウェア対策ソフトウェアやサイバー攻撃含む）への対策に関する項目については、定期的に見直しを図ること。	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
204	企画管理編	15	なし	⑦	医療機関等において利用するネットワークについて、リスク評価を踏まえつつその選定を担当者と協働して検討し、その結果を経営層に報告の上、承認を得ること。なお、選定にあたっては、医療機関等において医療情報システムに関する整備計画等を策定している場合には、これと整合性をとること。また、ネットワークの安全性確保を目的とした実装と運用設計を行った場合には、その内容を理解の上、経営層に報告し、承認を得ること。	A,L(M,N)	1	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
205	企画管理編	15	なし	⑧	保守に関する安全管理対策として必要な項目を担当者と協働して検討すること。また、必要に応じて、保守を行うシステム関連事業者と契約やSLA等により管理項目について取り決めを行うこと。	A,C,F,H,K	1	0	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
206	企画管理編	15	なし	⑨	医療情報システムの動作確認や保守においては、原則として個人情報を含む医療情報を用いないことを運用管理規定等に含めること。また、やむを得ず医療情報を用いる場合には、漏洩等が生じないために必要な対策を講じる旨を示し、その具体的な手順の策定を担当者に指示すること。	I,K	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
207	企画管理編	15	なし	⑩	医療情報システムで用いるシステム、サービス、情報機器等の品質を適切に管理し、必要に応じて、改善措置を講じること。品質の管理方法については、担当者と協働して検討すること。	A		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
208	企画管理編	15	なし	⑪	情報機器、ソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。	A		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
209	企画管理編	15	なし	⑫	システム構成やソフトウェアの品質管理に関する対応を運用管理規定で定めるとともに、具体的な手順の作成と実施を担当者に指示すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
210	企画管理編	15	なし	⑬	医療情報システムが法令等で求められている要件を満たすように適切に管理すること。特に「施行通知」、「外部保存通知」などで定める要件を満たしていることを確認し、調達においては当該要件を満たす内容とすること。具体的な確認項目や、医療情報システムにおける実装内容については、担当者に確認の上、必要な検討を行うよう指示すること。	A		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
211	企画管理編	15	なし	⑭	①〜⑬において、担当者が整備した対策について、関連規定等に反映すること。また、システム運用の実施状況については、定期的に担当者から報告を受け、その状況を反映の上、経営層に報告し承認を得ること。	A,C	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
212	企画管理編	16	なし	①	紙媒体で作成した医療情報を含む文書等をスキャナ等で読み取り、電子化する場合には、これに必要な情報機器等の条件や手順等を運用管理規定等に定めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
213	企画管理編	16	なし	②	スキャナにより読み取った電子情報と元の文書等から得られる情報と同党であることを担保する情報作成管理者を配置すること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
214	企画管理編	16	なし	③	紙媒体で作成した医療情報を含む文書等をスキャナにより電子化する場合、スキャナによる読み取りにかかる責任を明確にするため、作業責任者（実施者又は情報作成管理者）が電子署名法に適合した電子署名を遅滞なく行う旨を、運用管理規定等に定めること。なお、電子署名については「14.法令で定められた記名・押印のための電子署名」を参照すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
215	企画管理編	16	なし	④	情報作成管理者に対して、スキャナによる読み取り作業が運用管理規定に基づき適正な手続きで確実に実施されるために必要な措置を講じるよう指示し、その結果の報告を求めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
216	企画管理編	16	なし	⑤	診療等の都度スキャナ等で電子化して保存する場合、情報が作成されてからまたは情報を入手してから一定期間以内にスキャンを行うことを運用管理規定等に定めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
217	企画管理編	16	なし	⑥	過去に蓄積された紙媒体等をスキャナ等で電子化して保存する場合、以下の措置を講じること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
218	企画管理編	16	なし	⑥－１	・対象となる患者等に、スキャナ等で電子化して保存することを事前に院内掲示等で周知し、異議の申立てがあった場合、その患者等の情報は電子化を行わないこと。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
219	企画管理編	16	なし	⑥－２	・必ず実施計画書を作成すること。実施計画書には次に掲げる事項を含めること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
220	企画管理編	16	なし	⑥－２－１	ー運用管理規程の作成と妥当性の検証方法（評価は、大規模医療機関等にあっては、外部の有識者を含む公正性を担保した委員会等で行うこと（倫理委員会を用いることも可））	G?	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
221	企画管理編	16	なし	⑥－２－２	ー作業責任者	H	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
222	企画管理編	16	なし	⑥－２－３	ー相互監視を含む実施体制	G?　なし？	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
223	企画管理編	16	なし	⑥－２－４	ー実施記録の作成と記録項目（次項の監査に耐えうる記録を作成すること）	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
224	企画管理編	16	なし	⑥－２－５	ー事後の監査人と監査項目	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
225	企画管理編	16	なし	⑥－２－６	ースキャン等で電子化を行ってから紙やフィルムの破棄までの期間及び破棄方法	I,J	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
226	企画管理編	16	なし	⑥－３	・事後の監査は、システム監査技術者やCertified Information Systems Auditor(ISACA認定)等の適切な能力を持つ外部監査人によって実施すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
227	企画管理編	16	なし	⑦	企画管理者は、紙の調剤済み処方箋をスキャナ用で電子化して保存する場合、以下の措置を講じること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
228	企画管理編	16	なし	⑦－１	・紙の調剤済み処方箋の電子化のタイミングに応じて、⑤または⑥の措置を講じること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
229	企画管理編	16	なし	⑦－２	・「電子化した紙の調剤済み処方箋」を修正する場合、「「元の」電子化した紙の調剤済み処方箋」を電子的に修正し、「「修正後の電子化した紙の調剤済み処方箋」の電子署名の検証が正しく行われる形で修正すること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
230	企画管理編	16	なし	⑧	企画管理者は、運用の利便性のためにスキャナ等で電子化を行うが、紙等の媒体もそのまま保存を行う場合、以下の措置を講じること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
231	企画管理編	16	なし	⑧－１	・情報作成管理者が、スキャナによる読み取り作業が適正な手続きで、確実に実施される措置を講じる旨を運用管理規程等に定めること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
232	企画管理編	16	なし	⑧－２	・電子化した後、元の紙媒体やフィルムの安全管理を行うこと。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
233	システム運用	1	なし	①	法令上求められる医療情報システムに関する要件等について、企画管理者の整理に基づいて、必要な技術的な対応を抽出し、各システムの整備において措置を行うほか、必要な手順、資料の作成を行うこと。	C,I,J	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
234	システム運用	2	なし	①	医療情報システムにおいて採用するシステム、サービス、情報機器等の機能仕様及び利用方法に関する資料を整備し、常に最新の状態を維持すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
235	システム運用	2	なし	②	医療情報システムに関する全体構成図（ネットワーク構成図・システム構成図等）、及びシステム責任者・関係者一覧（設置事業者、保守事業者）を作成し、常に最新の状態を維持すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
236	システム運用	2	なし	③	医療情報システムの維持及び運用に必要な手順を整備し、常に最新の状態を維持すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
237	システム運用	2	なし	④	医療情報システムの利用者が常に医療情報システムの利用ができるよう、マニュアル等の整備を行うこと。	H?	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
238	システム運用	2	なし	⑤	非常時や情報セキュリティインシデントが生じた場合の手順等を作成し、企画管理者の承認を得ること。	J	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
239	システム運用	3	なし	①	医療情報システムに関する情報システム・サービスの委託において、技術的な対応の役割分担を検討するため、情報システム・サービス事業者（以下「事業者」という。）から必要な情報等の収集を行うとともに、提供された情報の内容が正確であることを事業者に確認すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
240	システム運用	3	なし	②	事業者と技術的な対応に関する責任分界を調整する際に、要求仕様との適合性に関する確認を行い、医療機関等において実施する技術的な対応におけるリスク評価との間で齟齬が生じないことを確認し、齟齬がある場合には、必要な調整を行うこと。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
241	システム運用	3	なし	③	通常時の運用や、非常時の運用において発生する技術的な対応に関する役割分担を、委託先である事業者との間で調整し、その結果を企画管理者に報告すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
242	システム運用	3	なし	④	サイバー攻撃等が生じた場合に、技術的な対応や対外的な説明に関して必要な役割について、事業者と調整し、その結果を企画管理者に報告すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
243	システム運用	3	なし	⑤	第三者提供を行う際の責任分界について、企画管理者と協議の上で、医療機関等のリスク評価に従った範囲で、技術的な対応に関する責任分界の範囲を検討し、企画管理者に報告すること。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
244	システム運用	4	なし	①	企画管理者の指示に基づき、医療機関等で取り扱う情報を適切に管理するための手順等を作成し、運用すること。その際、情報種別による重要度を踏まえるほか、患者情報については、患者ごとに識別できるような措置を講じること。	A,G,I	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
245	システム運用	4	なし	②	事業者から技術的対策等の情報を収集すること。例えば、総務省・経済産業省の定めた「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「サービス仕様適合会辞書」を利用することが考えられる。	A,C,F,H	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
246	システム運用	5	なし	①	システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えるようにすること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
247	システム運用	5	なし	②	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ること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
248	システム運用	5	なし	③	データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと。保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持すること。	G,I,J	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
249	システム運用	5	なし	④	電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である情報機器、ソフトウェア、関連情報等は常に整備された状態にすること。	I	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
250	システム運用	6	なし	①	システム運用担当者は、医療情報システムの安全管理に関する技術的な対応を検討する際に、下記の体系に従った内容を参考として検討すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
251	システム運用	6	なし	①－１	ークライアント層		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
252	システム運用	6	なし	①－１－１	・情報の持ち出し・管理・破棄等に関する安全管理措置	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
253	システム運用	6	なし	①－１－２	・利用機器・サービスに関する安全管理措置	A,I,J,L	1	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
254	システム運用	6	なし	①－２	ーサーバ側		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
255	システム運用	6	なし	①－２－１	・ソフトウェア・サービスに対する要求事項	I,J,L	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
256	システム運用	6	なし	①－２－２	・事業者による保守対応等に対する安全管理措置	A,C,K?	1	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
257	システム運用	6	なし	①－２－３	・事業者選定と管理	A,C,F	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
258	システム運用	6	なし	①－２－４	・システム運用管理（通常時・非常時等）	A,B?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
259	システム運用	6	なし	①－３	ーインフラ		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
260	システム運用	6	なし	①－３－１	・物理的安全管理装置（サーバールーム等、バックアップ）	A,G,H,I,J？	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
261	システム運用	6	なし	①－３－２	・ネットワークに関する安全管理措置	G,I,J,L	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
262	システム運用	6	なし	①－３－３	・インフラ運用管理（通常時・非常時等）	A,B?	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
263	システム運用	6	なし	①－４	ーセキュリティ		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
264	システム運用	6	なし	①－４－１	・認証・認可に関する安全管理措置	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
265	システム運用	6	なし	①－４－２	・電子署名、タイムスタンプ	G,L?	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
266	システム運用	6	なし	①－４－３	・証跡のレビュー、システム監査	G,L？	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
267	システム運用	6	なし	①－４－４	・外部からの攻撃に対する安全管理措置	J,L？	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
268	システム運用	7	なし	①	医療情報及び情報機器の持ち出しについて、運用管理規定に基づき、手順の策定と管理を行い、その状況を定期的に企画管理者に報告すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
269	システム運用	7	なし	②	保守業務を行う事業者に対して、原則として個人情報を含むデータの持ち出しを禁止すること。やむを得ず持ち出しを認める場合には、企画管理者の承認を得て許諾すること。	I,K,L	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
270	システム運用	7	なし	③	医療情報及び情報機器等の持出しに際しての盗難、置き忘れ等に対応する措置として、医療情報や情報機器等に対する暗号化やアクセスパスワードの設定等、容易に内容を読み取られないようにすること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
271	システム運用	7	なし	④	持ち出した利用者が情報機器を、医療機関等が管理しない外部のネットワークや他の外部媒体に接続したりする場合は、不正ソフトウェア対策ソフトやパーソナルファイアウォールの導入等により、情報端末が情報漏洩、改ざん等の対象にならないような対策を実施すること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
272	システム運用	7	なし	⑤	持ち出した情報機器等について、公衆無線LANの利用がなされた場合には、利用後に端末の安全性が確認できる手順を策定すること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
273	システム運用	7	なし	⑥	持ち出した医療情報を取り扱う情報機器には、必要最小限のアプリケーションのみをインストールするとともに、原則として情報機器に対する変更権限がないような設定を行うこと。業務に使用しないアプリケーションや機能については、削除または停止するか、業務に対して影響がないことを確認すること。	I,L	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
274	システム運用	7	なし	⑦	医療情報が格納された可搬媒体及び情報機器の所在を台帳等により管理する手順を作成し、これに基づき持出し等の対応を行う。併せて定期的に棚卸を行う手順を作成する。	A,I,L	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
275	システム運用	7	なし	⑧	セキュリティ対策を十分に行うことが難しいウェアラブル端末や在宅設置のIoT機器を 患者等に貸し出す際には、事前に、情報セキュリティ上のリスクと、患者等が留意すべきことについて患者等に説明し、同意を得ること。また、機器に異常や不具合が発生した場合の問い合わせ先や医療機関等への連絡方法について、患者等に情報提供すること。	なし	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
276	システム運用	7	なし	⑨	破棄に関する規程を踏まえて、把握した情報種別ごとに具体的な破棄の手順を定めること。手順には破棄を行う条件、破棄を行うことができる職員、具体的な破棄方法を含めること。また情報の破棄については、企画管理者に報告すること。	I,J	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
277	システム運用	7	なし	⑩	情報処理機器自体を破棄する場合、必ず専門的な知識を行うものが行うこと。また、破棄終了後に、残存し、読み出し可能な医療情報がないことを確認すること。	I,J	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
278	システム運用	7	なし	⑪	外部保存を受託する事業者に破棄を委託した場合は、確実に医療機器が破棄されたことを、証憑または事業者の説明により確認すること。	I?	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
279	システム運用	7	なし	⑫	保守作業等のどうしても必要な場合を除いてリモートログインを行うことができないように、適切に管理されたリモートログインのみに制限する機能を設けなければならない。	G,K	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
280	システム運用	7	なし	⑬	利用者による外部からのアクセスを許可する場合は、盗聴、なりすまし防止及びアクセス管理を実現したVPN技術により安全性を担保した上で、仮想デスクトップ等を利用する運用の要件を設定すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
281	システム運用	7	なし	⑭	患者等に医療情報を閲覧させる場合、医療情報を開示しているコンピュータシステムを通じて、医療機関等の内部のシステムに不正な侵入が起こらないように、例えば、システムやアプリケーションを切り分け、ファイアウォール、アクセス監視、通信のTLS暗号化、PKI（Public Key Infrastructure:公開鍵暗号基盤）認証等の対策を実施すること。	G,I,L	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
282	システム運用	7	なし	⑮	医療情報を格納する記録媒体や情報機器の盗難や紛失（ネットワークサービスの利用等による漏洩の可能性の発生含む）が生じた場合に、行うべき手順を作成するとともに、可能な範囲で紛失や盗難に対応した措置を事前に講じること。	G,I,J,L	0	0	0	0	0	0	1	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
283	システム運用	8	なし	①	システム構築時、適切に管理されていない記録媒体の使用時、外部からの情報受領時には、コンピュータウィルス等の不正なソフトウェアが混入していないか確認すること。適切に管理されていないと考えられる記録媒体を利用する際には、十分な安全確認を実施し、細心の注意を払って利用すること。	I,J,L,N	0	0	0	0	0	0	0	0	1	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
284	システム運用	8	なし	②	常時不正なソフトウェアの侵入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。	L,M,N	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
285	システム運用	8	なし	③	医療情報システムに接続するネットワークのトラフィックにおける脅威の拡散等を防止するために、不正ソフトウェア対策ソフトのパターンファイルやOSのセキュリティ・パッチ等、リスクに対してセキュリティ対策を適切に適用するこ	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
286	システム運用	8	なし	④	メールやファイル交換にあたっては、実行プログラム（マクロ等含む）が含まれるデータやファイルの送受信禁止、又はその実行停止の実施、無害化処理を行うこと。なお、保守等でやむを得ずファイル送信等を行う場合、送信側で無害化処理が行われていることを確認すること。	I,J,K,L	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
287	システム運用	8	なし	⑤	情報機器に対して起動パスワード等を設定すること。設定に当たっては製品等の出荷時におけるパスワードから変更し、推定しやすいパスワード等の利用を避けるとともに、情報機器の利用方法等に応じて必要があれば、定期的なパスワードの変更等の対策を実施すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
288	システム運用	8	なし	⑥	IoT機器を利用する場合、次に掲げる対策を実施すること。検査装置等に付属するシステム・機器についても同様であ		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
289	システム運用	8	なし	⑥－１	IoT機器により医療情報を取り扱う場合は、製造販売業者から提供を受けた当該医療機器のサイバーセキュリティに関する情報を基にリスク分析を行い、その取扱いに係る運用管理規程を定めること。	D,E,F	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
290	システム運用	8	なし	⑥－２	IoT機器には、製品出荷後にファームウェア等に関する脆弱性が発見されることがある。システムやサービスの特徴を踏まえ、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、運用するこ	D,E,F,J	0	0	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
291	システム運用	8	なし	⑥－３	使用が終了した又は不具合のために使用を停止したIoT機器をネットワークに接続したまま放置すると不正に接続されるリスクがあるため、対策を実施すること。	D,E,G	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
292	システム運用	8	なし	⑦	企画管理者と協働して、医療情報システムで用いる情報機器等やソフトウェアの棚卸を行うための手順を策定し、定期的に実施すること。棚卸の際には、情報機器等の滅失状況なども併せて確認すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
293	システム運用	8	なし	⑧	BYODの実施に関する規程に基づいて、具体的な手順と設定を行い、企画管理者に報告すること。	A,G	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
294	システム運用	8	なし	⑨	BYODであっても、医療機関等が管理する情報機器等と同様の対策が講じられるよう、手順を作成すること。	A,G	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
295	システム運用	9	なし	①	システムがどのような情報機器、ソフトウェアで構成され、どのような場面、用途で利用されるのかを明らかにするとともに、システムの機能仕様を明確に定義すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
296	システム運用	9	なし	②	情報機器、ソフトウェアの改訂履歴、その導入の際に実際に行われた作業の妥当性を検証するためのプロセスを規定すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
297	システム運用	9	なし	③	医療情報システムで利用するシステム、サービス、情報機器等の品質を定期的に管理するための手順を作成し、これに従い必要な措置を講じ、企画管理者に報告すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
298	システム運用	9	なし	④	医療情報システムの目的に応じて速やかに検索表示又は書面に表示できるような措置を講じること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
299	システム運用	10	なし	①	動作確認等の保守作業で事業者が個人情報を含むデータを使用するときは、保守終了後に確実にデータを消去することを求め、その結果の報告を求めること。	G,I,K	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
300	システム運用	10	なし	②	診療録等の外部保存を受託する事業者においては、診療録等の個人情報の保護を厳格に行う必要がある。受託する事業者の管理者であっても、保存を受託した個人情報に、正当な理由なくアクセスできない仕組みが必要である。	G,I,K	0	0	0	0	0	0	1	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
301	システム運用	10	なし	③	保守を実施するためにサーバに事業者の作業員（保守要員）がアクセスする際には、保守要員の専用アカウントを使用させ、個人情報へのアクセスの有無並びに個人情報にアクセスした場合の対象個人情報及び作業内容を記録すること。なお、これは利用者を模して操作確認を行う際の識別・認証についても同様である。	G,I,K,L	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
302	システム運用	10	なし	④	リモートメンテナンス（保守）によるシステムの改造・保守作業が行われる場合には、必ずアクセスログを収集し、保守に関する作業計画書と照合するなどにより確認し、当該作業の終了後速やかに企画管理者に報告し、確認を求めること。	G,K,L	0	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
303	システム運用	10	なし	⑤	リモートメンテナンス（保守）において、やむを得ず事業者が、ファイルを医療機関等へ送信等を行う場合、送信側で無害化処理が行われていることを確認すること。	G,I,K,L	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
304	システム運用	10	なし	⑥	診療録等を保管している設備に障害が発生した場合等で、やむを得ず診療録等にアクセスをする必要がある場合も、医療機関等における診療録等の個人情報と同様の秘密保持を行うと同時に、外部保存を委託した医療機関に許可を求めなければならない。	G,I,K,L	0	0	0	0	0	0	1	0	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
305	システム運用	11	なし	①	非常時の医療情報システムの運用について、次に掲げる対策を実施すること。		0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
306	システム運用	11	なし	①－１	ー「非常時のユーザアカウントや非常時用機能」の手順を整備すること。	J,P,Q	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0
307	システム運用	11	なし	①－２	ー非常時機能が通常時に不適切に利用されることがないようにするとともに、もし使用された場合に使用されたことが検知できるよう、適切に管理及び監査すること。	M,N,P,Q	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0
308	システム運用	11	なし	①－３	ー非常時ユーザアカウントが使用された場合、正常復帰後は継続使用ができないように変更すること。	J,P,U	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0

309	システム運用 11	なし	①－4	―医療情報システムに不正ソフトウェアが混入した場合に備えて、~~開発先への連絡手段~~や組織での運用等の代替手段を準備すること。	J,P,Q	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0
310	システム運用 11	なし	①－5	―サイバー攻撃による被害拡大の防止の観点から、論理的／物理的に機成分割されたネットワークを整備すること。	A,J	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
311	システム運用 11	なし	①－6	―重要なファイルは定期的にバックアップを複数の方式で確保し、その一部は不正ソフトウェアの混入による影響が波及しない方法で管理するとともに、バックアップからの重要なファイルの復元手順を整備すること。	J,L,P	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0
312	システム運用 11	なし	①－7	医療情報システムの稼働状況などを把握するため、パフォーマンス管理、死活監視などを行うこと。	M,N	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
313	システム運用 12	なし	①	医療情報及び医療情報システムを保管する場所について、リスク評価を踏まえて、その場所の選定を企画管理者と協議して検討し、決定すること。検討に際しては、医療情報を始めとする情報機器・記録媒体を物理的に保管するための施設が、**災害**（地震、水害、落雷、火災等並びにそれに伴う停電等）に耐えうる機能・構造を備え、災害による障害（加害等）について対策が講じられている建築物に設置することなどを考慮すること。 医療情報を保護する施設について、医療情報を始めとする情報機器や記録媒体の設置場所等のセキュリティ境界への入退管理が、個人認証システム等による制限に基づいて行われていることを確認すること。また調査、部屋への不正な侵入を防ぐため、防犯カメラ、自動侵入監視装置等が設置されていることを確認すること。	J,P,Q A,D?	0 1	0 0	0 0	0 1	0 0	0 0	0 0	0 0	0 0	1 0	0 0	0 0	0 0	0 0	0 0	1 0	1 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0	0 0
314	システム運用 12	なし	②	個人情報が保管されている情報機器等の重要な情報機器には盗難防止措置を講じること。	G,J	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
315	システム運用 12	なし	③	医療情報及び医療情報システムのバックアップは、公開管理者が定める運用管理規程等と整合性がとれる措置とし、確保したバックアップは非常時に利用できるよう、適切に管理すること。	A,G	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
316	システム運用 12	なし	④	記録媒体、ネットワーク回線、設備の劣化による情報の読み取り不能または不完全な読み取りを防止するため、記録媒体が劣化する前に、当該記録媒体に保管されている情報を新たな記録媒体又は情報機器に復写等の情報の保管措置を講じること。	J,L	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
317	システム運用 12	なし	⑤	利用者が医療情報を入力・参照する端末から長時間離席する際など、正当な利用者以外の者による入力・参照が生じないよう対策を実施すること。	G	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
318	システム運用 13	なし	①	ネットワーク利用に関連する具体的な責任分界、責任の所在の範囲を明らかにし、公開管理者に対して報告すること。	A	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
319	システム運用 13	なし	②	セッション乗っ取り、IPアドレス詐称等のなりすましを防止するため、原則として医療機関等が組織等を管理する、サセキュアなネットワークを利用すること。	G,L,L,M,N	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
320	システム運用 13	なし	③	オープンなネットワークかもオープンでないネットワークへの接続までの間にチャネル・セキュリティの確保を組特してネットワークを構成する場合には、選択するサービスのチャネル・セキュリティの確保の範囲を電気通信事業者に確認すること。 オープンでないネットワークを利用する場合は、必要に応じてデータ送信元と送信先での、ルータ等の組点の出入り口・使用機器・使用機器上の機能単位・利用者等の選択するネットワークに応じて、必要な単位で、互いに確認し、採用する通信方式や、採用する認証手段を決めること。採用する認証手段は、PKIによる認証、Kerberosのような鍵配布、事前配布された共通鍵の利用、ワンタイムパスワード等、容易に解読されない方法が望ましい。 ルータ等のネットワーク機器について、安全性が確認できる機器を利用し、不正な機器の接続や不正なデータやソフトウェアの混入が生じないよう、セキュリティ対策を実施すること。特にVPN接続による場合は、当該内のルータを経由して異なる施設間を結ぶ通信経路の間で決定性ができないように相互を設定すること。 オープンなネットワークにおいて、IPsecによるVPN接続等を利用せずHTTPSを利用する場合、TLSのプロトコルバージョンをTLS1.3以上に限定した上で、クライアント証明書を利用したTLSのクライアント認証を実施すること。ただしシステム・サービス等の対応が困難な場合にはTLS1.2の設定によることも可能とする。その際、TLSの設定はサーバ/クライアントともに「TLS暗号設定ガイドライン3.0.3版」に規定される最も安全性高い高い「高セキュリティ型」に準じた適切な設定を行うこと。なお、SSL-VPNは利用する具体的な方法によっては他サーバへの対策が不十分なものが含まれるため、使用する場合には適切な手法の選択及び必要な対策を行うこと。また、ソフトウェア型のIPsecまたはTLS1.2以上による接続する場合、セッション間の回り込み（正規のルートでないクローズドセッションへのアクセス）等による攻撃への適切な対策を実施すること。	A,G,L A,G,L,L A,G,L,L A,G,L,M,N A,G,L,L A,G,L,L A,G,L,L A,G,L,L,M,N A,G,L,L A,G,L,L A,G,L,L A,G,L,L