参考資料2

様式１　『~~レセプト~~簡易データ情報等の提供に関する申出書「7　~~レセプト~~簡易データ情報等の利用場所、保管場所及び管理方法　②　管理方法等」（セキュリティ要件チェック項目）」の修正（案）

	２５年８月版	検討事項	２６年１月一部修正（案）
①　基本的な事項	□ｉ）レセプト情報等の利用場所は国内であること。 □ii）レセプト情報等を複写した情報システムを利用、管理及び保管する場所は、あらかじめ申し出られた施錠可能な物理的なスペースに限定されており、原則として持ち出されないこと。 □iii）レセプト情報等を複写した情報システムは、インターネット等の外部ネットワークに接続しないこと。 □iv）提供されたレセプト情報等は、あらかじめ申し出られた利用者のみが利用することとし、そのほかの者へ譲渡、貸与又は他の情報との交換等を行わないこと。	これらの要件が、レセプト情報等ではなくサンプリングデータセット情報、基本データセット情報、集計表情報などに適用されることから、「レセプト情報等」→「簡易データ情報等」（仮）と改めた。（以下同様）	□ｉ）簡易データ情報等の利用場所は国内であること。 □ii）簡易データ情報等を複写した情報システムを利用、管理及び保管する場所は、あらかじめ申し出られた施錠可能な物理的なスペースに限定されており、原則として持ち出されないこと。 □iii）簡易データ情報等を複写した情報システムは、インターネット等の外部ネットワークに接続しないこと。 □iv）提供された簡易データ情報等は、あらかじめ申し出られた利用者のみが利用することとし、そのほかの者へ譲渡、貸与又は他の情報との交換等を行わないこと。
②　~~レセプト~~簡易データ情報等の利用に限らず所属機関が一般的に具備すべき条件（必ずしも所属機関全体で具備する必要はなく、部、課又は研究室等、申出者の利用形態を勘案して適切な単位で対応すること。）	ｉ）個人情報保護方針の策定・公開 □a）個人情報保護に関する方針を策定し、公開していること。 □b）個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。 □c）提供されるレセプト情報等についても当該方針に従った対応を行うこと	「個人情報保護方針」については、所属機関におけるもののみを求めることとした。	ｉ）所属機関における個人情報保護方針の策定・公開 □a）個人情報保護に関する方針を策定し、公開していること。 □b）個人情報を取り扱う情報システムの安全管理に関する方針を策定していること。
	ii）情報セキュリティマネジメントシステム（ISMS）の実践（必ずしも ISMS 適合性評価制度における認証の取得を求めるものではない。） □a）情報システムで扱う情報をすべてリストアップしていること。 □b）リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。	提供対象が「レセプト情報等」が「簡易データ情報等」と代わったものの、相応の情報セキュリティマネジメントシステムの運用自体は求めることを想定しているので、修正は行っていない。	ii）情報セキュリティマネジメントシステム（ISMS）の実践（必ずしも ISMS 適合性評価制度における認証の取得を求めるものではない。） □a）情報システムで扱う情報をすべてリストアップしていること。 □b）リストアップした情報を、安全管理上の重要度に応じて分類を行い、常に最新の状態を維持していること。
	iii）組織的安全管理対策（体制、運用管理規程）の実施 □a）情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし所属機関が小規模な場合において役割が自明の場合は、明確な規程を定めなくとも良い。 □b）個人情報が参照可能な場所においては、来訪者の記録・識別、入退を制限する等の入退管理を定めること。 □c）情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。 □d）個人情報の取扱いを委託する場合、委託契約において安全管理に関する条項を含めること。 □e）運用管理規程等において次の内容を定めること。 ・理念（基本方針と管理目的の表明） ・利用者等の体制 ・契約書・マニュアル等の文書の管理 ・リスクに対する予防、発生時の対応の方法 ・機器を用いる場合は機器の管理	「簡易データ情報等」を「実質的個人識別可能性」のないデータ（第 17 回有識者会議）として位置づけていることに鑑み、「個人情報の取扱い」に関する事項を削除した。ただし、情報システムの運用責任者の設置、情報システムへのアクセス制限、準備すべき運用管理規程の要件についてはそのままとし	iii）組織的安全管理対策（体制、運用管理規程）の実施 □a）情報システム運用責任者の設置及び担当者（システム管理者を含む）の限定を行うこと。ただし所属機関が小規模な場合において役割が自明の場合は、明確な規程を定めなくとも良い。 □b）情報システムへのアクセス制限、記録、点検等を定めたアクセス管理規程を作成すること。 □c）運用管理規程等において次の内容を定めること。 ・理念（基本方針と管理目的の表明） ・利用者等の体制 ・契約書・マニュアル等の文書の管理 ・リスクに対する予防、発生時の対応の方法 ・機器を用いる場合は機器の管理

	・個人情報の記録媒体の管理（保管・授受等）の方法 ・監査 ・苦情・質問の受付窓口	た。	・記録媒体の管理（保管・授受等）の方法 ・監査 ・苦情・質問の受付窓口
	ⅳ）人的安全対策の措置 □a）利用者が所属する組織の管理者は、個人情報の安全管理に関する施策が適切に実施されるよう措置するとともにその実施状況を監督する必要があり、以下の措置をとること。 ・法令上の守秘義務のある者以外を事務職員等として採用するにあたっては、雇用及び契約時に守秘・非開示契約を締結すること等により安全管理を行うこと。 ・定期的に従業者に対し個人情報の安全管理に関する教育訓練を行うこと。 ・従業者の退職後の個人情報保護規程を定めること。 □b）利用者が所属する組織の事務、運用等を外部の事業者に委託する場合は、これらの機関の内部における適切な個人情報保護が行われるように、以下の措置を行うこと。 ・受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること。 ・保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。 ・清掃等の直接情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。 ・委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の個人情報保護に関する対策及び契約がなされていることを条件とすること。 □c）プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が個人情報にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。	上に同じ。但し、「簡易データ情報等」が個人情報に準ずる情報か否かに関わらず、外部委託の際や他者が接触しうる際には、データのセキュリティが適切に保たれるべきであると考え、それらについての要件はそのままとした。	ⅳ）人的安全対策の措置 □a）利用者が所属する組織の事務、運用等を外部の事業者に委託する場合は、これらの機関の内部における適切な情報保護が行われるように、以下の措置を行うこと。 ・受託する事業者に対する包括的な罰則を定めた就業規則等で裏付けられた守秘契約を締結すること。 ・保守作業等の情報システムに直接アクセスする作業の際には、作業者・作業内容・作業結果の確認を行うこと。 ・清掃等の直接情報システムにアクセスしない作業の場合においても、作業後の定期的なチェックを行うこと。 ・委託事業者が再委託を行うか否かを明確にし、再委託を行う場合は委託事業者と同等の情報保護に関する対策及び契約がなされていることを条件とすること。 □b）プログラムの異常等で、保存データを救済する必要があるとき等、やむをえない事情で外部の保守要員が簡易データ情報等にアクセスする場合は、罰則のある就業規則等で裏づけられた守秘契約等の秘密保持の対策を行うこと。
	ⅴ）情報の破棄の手順等の設定 □a）個人情報保護方針の中で把握した情報種別ごとに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従業者の特定、具体的な破棄の方法を含めること。 □b）情報処理機器自体を破棄する場合、必ず専門的な知識を有するものが行うこととし、残存し、読み出し可能な情報がないことを確認すること。 □c）外部保存を受託する機関に破棄を委託した場合は、「医療情報システムの安全管理に関するガイドライン（第４．１版　平成 22 年２月）」の「6.2 人的安全対策　(2) 事務取扱委託業者の監督及び守秘義務契約」に準じ、さらに委託する利用者等が確実に情報の破棄が行われたことを確認すること。	情報の破棄については、具体的手順については資料 5 の運用管理規程等を参考に、実行可能な範囲で最低限、破棄の手順を定めることのみを要件とした。	ⅴ）情報の破棄の手順等の設定 □a）対象となる情報種別ごとに破棄の手順を定めること。
	ⅵ）運用管理について レセプト情報等を含めた個人情報の取扱いについて、この「（４）データの利用場所、保管場所及び管理方法」に規定された内容のうち提供依頼申出者が対応を行っていると申し出た事項が適切に運用管理規程等に含められていること。		ⅵ）運用管理について 簡易データ情報等を含めた個人情報の取扱いについて、この「（４）データの利用場所、保管場所及び管理方法」に規定された内容のうち提供依頼申出者が対応を行っていると申し出た事項が適切に運用管理規程等に含められていること。
③　~~レセプト~~簡易データ情報等の利用に際し具備すべき条件（必ずしも所属機関全体で具備する必要はなく、部、課又は研究室等、申出者の利用形態を勘案して適切な単位	ⅰ）物理的安全対策 □a）レセプト情報等が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。 □b）レセプト情報等を参照できる端末が設置されている区画は、業務時間帯以外は施錠等、運用管理規程に基づき許可された者以外立ち入ることが出来ない対策を講じること。ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。	入退室管理を厳密に求めないとともに、当該施設への立ち入りは、所属機関において許可されている者であれば立ち入りを認める	ⅰ）物理的安全対策 □a）簡易データ情報等が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。 □b）簡易データ情報等を参照できる端末が設置されている区画は、業務時間帯以外は施錠等、当該施設において区画内への立ち入りが許可されている者以外立ち入ることが出来ない対策を講じること。ただし、本対策項目と同等レベルの他の取りうる手段がある場合はこの限りではない。

で対応すること。）	□c）レセプト情報等の物理的保存を行っている区画への入退管理を実施すること。例えば、以下のことを実施すること。 ・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。 ・入退者の記録を定期的にチェックし、妥当性を確認する。 □d）レセプト情報等が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。 □e）窃視防止の対策を実施すること。	こととした。 窃視については、「簡易データ情報等」を「実質的個人識別可能性」のないデータとして位置づけていることに鑑み、要件から外した。	□c） 簡易データ情報等が存在する PC 等の重要な機器に盗難防止用チェーンを設置すること。
	ⅱ）技術的安全対策 □a）レセプト情報等を利用する情報システムへのアクセスにおける利用者の識別と認証を行うこと。 □b）上記 a)の利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。 □c）利用者がレセプト情報等を利用する情報システムの端末から長時間、離席する際に、あらかじめ認められた利用者以外の者が利用する恐れがある場合には、クリアスクリーン等の防止策を講じること。 □d）レセプト情報等を利用する情報システムへのアクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した利用者が特定できること。 □e）レセプト情報等を利用する情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。 □f）レセプト情報等を利用する情報システムにアクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を講じること。 □g）上記 f）のアクセスの記録に用いる時刻情報は信頼できるものであること。 □h）原則としてレセプト情報等を利用する情報システムには、適切に管理されていないメディアを接続しないこと。ただし、システム構築時、やむをえず適切に管理されていないメディアを使用する場合、外部からの情報受領時にはウイ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メディアを利用する際には、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。常時ウイルス等の不正なソフトウェアの混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・維持を行うこと。 □i）パスワードを利用者識別に使用する場合 システム管理者は以下の事項に留意すること。 ・レセプト情報等が複写された情報システムが複数の者によって利用される場合にあっては、当該システム内のパスワードファイルでパスワードは必ず暗号化（可能なら不可逆変換が望ましい）され、適切な手法で管理及び運用が行われること。（利用者識別に IC カード等他の手段を併用した場合はシステムに応じたパスワードの運用方法を運用管理規程にて定めること） ・利用者がパスワードを忘れたり、盗用されたりする恐れがある場合で、システム管理者がパスワードを変更する場合には、利用者の本人確認を行い、どのような手法で本人確認を行ったのかを台帳に記載（本人確認を行った書類等のコピーを添付）し、本人以外が知りえない方法で再登録を実施すること。 ・システム管理者であっても、利用者のパスワードを推定できる手段を防止すること。（設定ファイルにパスワードが記載される等があってはならない。） また、利用者は以下の事項に留意すること。	「簡易データ情報等」を「実質的個人識別可能性」のないデータとして位置づけていることに鑑み、クリアスクリーン等の防止策については求めないこととした。 対象となる操作端末へのアクセス記録を、最低限の要件として求めることとした。但し、そのアクセス記録の管理については、申出者の情報セキュリティマネジメントシステムのなかで適時実施することを求めるにとどめ、アクセスログの改ざんや時刻情報の正確性、パスワード管理の詳細についてまでは、具体的な要件として求めないこととした。	ⅱ）技術的安全対策 □a）簡易データ情報等を利用する情報システムへのアクセスにおける利用者の識別と認証を行うこと。 □b）上記 a)の利用者の識別・認証にユーザ ID とパスワードの組み合わせを用いる場合には、それらの情報を、本人しか知り得ない状態に保つよう対策を行うこと。 □c）簡易データ情報等を利用する情報システムへのアクセスの記録及び定期的なログの確認を行うこと。アクセスの記録は少なくとも利用者のログイン時刻、アクセス時間、ならびにログイン中に操作した利用者が特定できること。 □d）簡易データ情報等を利用する情報システムにアクセス記録機能があることが前提であるが、ない場合は業務日誌等で操作の記録（操作者及び操作内容）を必ず行うこと。 □e）原則として簡易データ情報等を利用する情報システムには、適切に管理されていないメディアを接続しないこと。ただし、システム構築時、やむをえず適切に管理されていないメディアを使用する場合、外部からの情報受領時にはウイ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メディアを利用する際には、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。常時ウイルス等の不正なソフトウェアの混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・維持を行うこと。 □f）パスワードを利用者識別に使用する場合 利用者は以下の事項に留意すること。

	・パスワードは定期的に変更し（最長でも 2 ヶ月以内）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。 ・類推しやすいパスワードを使用しないこと □j）レセプト情報等の保存・利用に際しては、インターネット等の外部ネットワークに接続した情報システムを使用しないこと。 □k）レセプト情報等の利用の終了後には、情報システム内に記録されたレセプト情報等及び中間生成物を消去することに加え、消去後に当該機器を外部ネットワークに接続する際にはあらかじめコンピューターウイルス等の有害ソフトウェアが無いか検索し、ファイアウォールを導入するなど、安全対策に十分配意すること。		・パスワードは定期的に変更し（最長でも 2 ヶ月以内）、極端に短い文字列を使用しないこと。英数字、記号を混在させた 8 文字以上の文字列が望ましい。 ・類推しやすいパスワードを使用しないこと □g）簡易データ情報等の保存・利用に際しては、インターネット等の外部ネットワークに接続した情報システムを使用しないこと。 □h）簡易データ情報等の利用の終了後には、情報システム内に記録された簡易データ情報等及び中間生成物を消去することに加え、消去後に当該機器を外部ネットワークに接続する際にはあらかじめコンピューターウイルス等の有害ソフトウェアが無いか検索し、ファイアウォールを導入するなど、安全対策に十分配意すること。
	ⅲ）情報及び情報機器の持ち出しについて 提供されたレセプト情報等の利用、管理及び保管は、事前に申し出られた場所でのみ行うこととし、外部への持ち出しは行わないこと。ただし、外部委託や共同研究の場合など、やむをえず、あらかじめ申し出られた利用者の間で最小限の範囲で中間生成物等の受け渡しを行う場合には、利用者が以下の措置を講じており、レセプト情報等の受け渡しに準用していること。 □a）組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。 □b）運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。 □c）情報を格納した媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程等に定めること。 □d） あらかじめ運用管理規程等で定めたレセプト情報等の盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。 □e）利用者は、レセプト情報等が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。 □f）レセプト情報等の持ち出しに利用する情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避け、定期的にパスワードを変更する等の措置を行うこと。 □g）盗難、置き忘れ等に対応する措置として、レセプト情報等に対して暗号化したり、アクセスパスワードを設定する等、容易に内容を読み取られないようにすること。 □h）レセプト情報等が保存された情報機器を、他の外部媒体と接続する場合は、コンピューターウイルス対策ソフトの導入を行う等して、情報漏えい、改ざん等の対象にならないような対策を施すこと。 □i）レセプト情報等の持ち出しについて個人保有の情報機器（パソコン等）を使用する場合にあっても、上記の f)、g)、h）と同様の要件を遵守させること。	情報セキュリティマネジメントシステムにおいて、個人保有の情報機器が使用されることを想定していないため、具体的なセキュリティ要件としては明記しないこととした。	ⅲ）情報及び情報機器の持ち出しについて 提供された簡易データ情報等の利用、管理及び保管は、事前に申し出られた場所でのみ行うこととし、外部への持ち出しは行わないこと。ただし、外部委託や共同研究の場合など、やむをえず、あらかじめ申し出られた利用者の間で最小限の範囲で中間生成物等の受け渡しを行う場合には、利用者が以下の措置を講じており、簡易データ情報等の受け渡しに準用していること。 □a）組織としてリスク分析を実施し、情報及び情報機器の持ち出しに関する方針を運用管理規程で定めること。 □b）運用管理規程には、持ち出した情報及び情報機器の管理方法を定めること。 □c）情報を格納した媒体もしくは情報機器の盗難、紛失時の対応を運用管理規程等に定めること。 □d） あらかじめ運用管理規程等で定めた簡易データ情報等の盗難、紛失時の対応を従業者等に周知徹底し、教育を行うこと。 □e）利用者は、簡易データ情報等が格納された可搬媒体もしくは情報機器の所在を台帳を用いる等して把握すること。 □f）簡易データ情報等の持ち出しに利用する情報機器に対して起動パスワードを設定すること。設定にあたっては推定しやすいパスワード等の利用を避け、定期的にパスワードを変更する等の措置を行うこと。 □g）盗難、置き忘れ等に対応する措置として、簡易データ情報等に対して暗号化したり、アクセスパスワードを設定する等、容易に内容を読み取られないようにすること。 □h）簡易データ情報等が保存された情報機器を、他の外部媒体と接続する場合は、コンピューターウイルス対策ソフトの導入を行う等して、情報漏えい、改ざん等の対象にならないような対策を施すこと。