令和４年６月17日	資料１
第８回匿名医療・介護情報等の提供に関する委員会	

HIC解析環境の利用にあたり検討すべき事項

令和４年６月17日
厚生労働省保険局医療介護連携政策課
保険データ企画室
厚生労働省老健局老人保健課

HIC解析環境の利用にあたり検討すべき事項

○HICでは、申出ごとに抽出されたNDBデータ及び介護DBデータは利用者の端末ではなくクラウド上に格納されており、利用者は自身で環境を構築することなく、リモート接続により解析を行う仕組みとなっている。

○また、HIC利用環境へのアクセスにおいては、外部からのアクセスが前提とされおり、安全管理の観点から、従前のオンプレミスの環境とは異なる仕様が求められている。

○こうした仕組みを前提として、適切な安全管理措置を講じつつ、HICの利便性の向上を図る観点から、「匿名レセプト情報・匿名特定健診等情報の提供に関するガイドライン」（NDBガイドライン）及び「匿名介護情報等の提供に関するガイドライン」（介護DBガイドライン）から見直しを行うべき点を明らかにしつつ、HICガイドラインの策定について検討していくこととしてはどうか。

【現行の安全管理措置（まとめ）】

入退室管理	利用場所の施錠、取扱者の名札等の着用、台帳等による入退室管理及び入退室の記録を定期的にチェックし、その妥当性の確認、入退室管理の保管（1年）
データ保護	クリアスクリーン等による窃視防止
	匿名レセプト情報等、中間生成物等が格納された記録媒体の管理
盗難・紛失	専用端末の窃盗防止用ワイヤー等設置による盗難防止
認証・識別	ＭＦＡ（二要素認証）による利用者識別の推奨
ウィルス対策	外部からの情報受領時には、不正なウィルスの混入を防止
消去	利用終了後は専用ソフトウェア等を利用し、復元不可能な形で消去
ログ管理	アクセスの記録及び定期的なログの確認・保管

HICガイドラインの策定に向けて検討すべき事項

【論点１】

HICは、クラウド上の解析環境にリモート接続する方式であり、従前のオンプレミスの環境と異なり、利用者端末にデータが格納されていない。こうした観点を踏まえ、現行のNDBガイドライン及び介護DBガイドラインにおける物理的安全管理措置・技術的安全管理措置から変更すべき事項はないか。

（例）・ 利用者以外の出入りが基本的にない安全な環境で利用することを求めれば、名札の着用や入退室記録の管理まで求める必要はないのではないか

・ 利用終了後のデータ消去は運用保守事業者が解析環境を削除することにより行うこととされていることから、利用終了時の復元不可能な形でのデータ削除は不要となるのではないか

【論点２】

HIC利用環境へのアクセスにおいては、従前のオンプレミスの環境と異なり、二要素認証等による利用者の認証や、情報漏洩対策として無操作状態から自動的にログオフをする仕組み等がある。こうした観点を踏まえ、NDBガイドライン及び介護DBガイドラインにおける物理的安全管理措置・技術的安全管理措置から変更すべき事項はないか。

（例）・ 利用者以外の出入りが基本的にない安全な環境で利用することを求めるとともに、情報漏洩対策を徹底するために、スクリーンショット・カメラによる画面の撮影を新たに禁止することとしてはどうか

・ 併せて、公衆無線LANからHIC解析環境への接続の禁止や、無線LAN接続における不正アクセス対策を新たに求めることとしてはどうか

・ HIC解析環境はインターネット回線での接続となるため、セキュリティ対策は常にアップグレードを求めることとしてはどうか

HICガイドラインの策定に向けて検討すべき事項

【論点３】

HICは利用端末にデータが格納されていない。一方、提供されるデータの種類は下記の参考に示すように個人特定の蓋然性が異なる。これらを踏まえ、物理的安全管理措置について、提供されるデータの種類に応じた措置の在り方を検討してはどうか。

（参考）現行の第三者提供で提供されるデータ

	特別抽出	集計表情報	サンプリングデータセット
概要	データベースに格納されている全データのなかから、申出者の要望に基づいて、該当する個票の情報を抽出し、提供	申出者の要望に基づき、データを加工して作成した集計表を提供	探索的研究へのニーズに対応し、抽出率を1/10～1/100に設定かつ項目削除等を施し、安全性に十分配慮した、単月分のデータセット
提供データ	個票	集計表	個人特定等の安全性に十分配慮した個票

（例）・ 提供されるデータが集計表の場合には、パーティション等設置による窃視防止まで求める必要はないのではないか

・ 提供されるデータが集計表・サンプリングデータセットである場合には、専用端末のワイヤー等設置による盗難防止まで求める必要はないのではないか

【論点４】

その他、NDBガイドラインおよび介護DBガイドラインから変更すべき事項はないか

HIC解析環境の仕様

利用者の認証	本人確認	二要素認証（知識：IDパスワード・所有物：ワンタイムパスワード）
	パスワードポリシー	8文字以上20文字以下
		90日毎の変更を必須
		4回失敗したらログイン不能
	IDパスワードの再発行	ヘルプデスクに再発行依頼
	サービスの利用	6ヶ月更新
	サーバーの真正性証明	クライアント証明書は独自に設置した認証局にて発行
情報漏洩対策		無操作状態から1時間経過した場合、自動的にログオフ
アクセス方式		Amazon WorkSpacesを経由してEC2にアクセス（リモートデスクトップ）
不正アクセスの感知		正常でない利用方法、不正なログオン等が認められれば、サービスの利用停止
アクセスログの管理		運用保守業者で管理
データの持ち込み		可（利用者がHICポータルでデータの持ち込み申請・アップロードし、 事務局の確認後に運用保守業者が当該利用者の解析環境にアップロード）
最終生成物の持ち出し		ダウンロード機能あり （事務局の確認（公表物確認を想定）後にHICポータル経由でダウンロード可能）
利用終了後のデータの消去		運用保守業者が消去（解析環境の削除）

（参考）今後のスケジュールと解析環境の試行的利用（案）

第8回 匿名医療情報等の提供に関する専門委員会 一部改変

	2022年度	2023年度	2024年度
ポータル機能	調査研究・設計・開発	運用開始	順次、機能やコンテンツを拡充
探索的利用環境	データの仕様検討	運用開始	
HIC解析環境	試行的利用 HICガイドライン検討・作成	本格利用	

※2023年度中の開始可能となったタイミングで順次開始

【解析環境の試行的利用】

- 一部のNDB・介護DBの提供申出に対して、匿名医療情報等の提供に関する専門委員会及び匿名介護情報等の提供に関する専門委員会にて個別審査を実施した上で、安全性に十分な配慮を行いながらHIC解析環境の試行的利用を開始してはどうか。
- 試行的利用においては、匿名レセプト情報・匿名特定健診等情報の提供に関するガイドライン（以下、「NDBガイドライン」という。）及び匿名介護情報等の提供に関するガイドライン（以下、「介護DBガイドライン」という。）について、インターネット接続に関する部分を除いて、基本的に準用することとしてはどうか。（NDBガイドライン及び介護DBガイドラインの改正）
- その上で、NDBガイドライン及び介護DBガイドラインはHIC解析環境の実情に合っていないとの指摘もあることから、試行的利用者からの意見を踏まえて、本格利用に向けて、新しくHIC解析環境の利用に関するガイドラインを作成することを検討してはどうか。

（参考）NDBガイドラインの安全管理措置

第6　提供申出に対する審査
4　審査基準
（4）　匿名レセプト情報等の利用場所、保管場所及び管理方法
③　匿名レセプト情報等の利用に際し講じなければならない安全管理措置
iii）　物理的安全管理措置
a）　匿名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）　匿名レセプト情報等が参照可能な区画を明示し、取扱者以外の者の無断立ち入りを防ぐ対策を講ずること。また、匿名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、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よう、施錠等の対策を講ずること。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にはこの限りではない。
c）　匿名レセプト情報等を物理的に保存している区画への入退管理を実施すること。例えば、以下の措置を実施すること。
・　入退者には名札等の着用を義務付け、台帳等に氏名等を記入することにより入退の事実を記録すること。
・　入退者の記録を定期的にチェックし、その妥当性を確認すること。
・　入退管理記録は、利用終了後少なくとも1年は保管すること。
d）　情報システム等の匿名レセプト情報等が存在する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。
f）　オンサイトリサーチセンターを利用する場合には、入退室管理を含めオンサイトリサーチセンターによって定められた運用管理規程に従い、匿名レセプト情報等を利用すること。
g）　匿名レセプト情報等の消去にあたっては、専用ソフトウェア等を用い、復元不可能な形で行うこと。
iv）　技術的安全管理措置
a）　匿名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取扱者の識別と認証を行うこと。
b）　上記a）の取扱者の識別・認証に用いる手段として、セキュリティ強度を考慮し、ICカード等のセキュリティ・デバイス＋パスワード、ICカード＋バイオメトリクス(指紋、静脈、虹彩のような取扱者の生体的特徴を利用した生体計測)やユーザID・パスワード＋バイオメトリクスといった2つの独立した要素を用いて行う方式(二要素認証)を採用することを求める。この場合は、必ずしもパスワードの定期的な変更は必要ない。
ただし、何らかの事情で上記の実装が困難な場合は、ユーザIDとパスワードを組み合わせた認証を行うこと。その場合は、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。なお、下記の要件を含め、適切に設定された13文字以上のパスワードを用いる場合は定期的な変更は求めない。
・　類推しやすいパスワードを使用しないこと。
・　匿名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(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。
・　取扱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、取扱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、取扱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。)
c）　取扱者が匿名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取扱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ずること。
d）　匿名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取扱者のログイン時刻、アクセス時間並びにログイン中に操作した取扱者が特定できるようにすること。
e）　匿名レセプト情報等を利用する情報システムはアクセス記録機能を備えたものであること。仮に当該機能がない場合には、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。 なお、記録等は利用終了後少なくとも1年は保管すること。
f）　匿名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、改ざん及び追加等を防止する対策を講ずること。
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、匿名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、システム構築時に、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には、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）　匿名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。
j）　匿名レセプト情報等の利用終了後には、情報システム内に記録された匿名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の安全対策に十分配意すること。

（参考）介護DBガイドラインの安全管理措置

第6　提供申出に対する審査
4　審査基準
（4）　匿名要介護認定情報等の利用場所、保管場所及び管理方法
③　匿名要介護認定情報等の利用に際し講じなければならない安全管理措置

ⅲ）物理的安全管理措置

a）匿名要介護認定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）匿名要介護認定情報等が参照可能な区画を明示し、取扱者以外の者の無断立入りを防ぐ対策を講ずること。また、匿名要介護認定情報等を参照できる端末が設置されている区画は、運用管理規程に基づき、許可された者以外立入ることが出来ないよう、施錠等の対策を講ずること。
ただし、本対策項目と同等レベルの他の取り得る手段がある場合にはこの限りではない。

c）匿名要介護認定情報等を物理的に保存している区画への入退管理を実施すること。例えば、以下の措置を実施すること。
・入退者には名札等の着用を義務付け、台帳等に氏名等を記入することにより入退の事実を記録すること。
・入退者の記録を定期的にチェックし、その妥当性を確認すること。
・入退管理記録は、利用終了後少なくとも1年は保管すること。

d）情報システム等の匿名要介護認定情報等が存在する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。

f）匿名要介護認定情報等の消去にあたっては、専用ソフトウェア等を用い、復元不可能な形で行うこと。

ⅳ）　技術的安全管理措置

a）匿名要介護認定情報等を利用する情報システムへのアクセスにおける取扱者の識別と認証を行うこと。

b）上記a）の取扱者の識別・認証に用いる手段として、セキュリティ強度を考慮し、ICカード等のセキュリティ・デバイス＋パスワード、ICカード＋バイオメトリクス（指紋、静脈、虹彩のような取扱者の生体的特徴を利用した生体計測）やユーザID・パスワード＋バイオメトリクスといった2つの独立した要素を用いて行う方式（二要素認証）を採用することを求める。この場合は、必ずしもパスワードの定期的な変更を求めない。ただし、何らかの事情で上記の実装が困難な場合は、ユーザIDとパスワードを組み合わせた認証を行うこと。その場合は、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。なお、下記の要件を含め、適切に設定された13文字以上のパスワードを用いる場合は定期的な変更は必要ない。
・類推しやすいパスワードを使用しないこと。
・匿名要介護認定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はパスワードを必ず暗号化（不可逆変換が望ましい。）した状態とするよう、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。
・取扱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、取扱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、本人以外が知り得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、取扱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。）。

c）取扱者が匿名要介護認定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取扱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ずること。

d）匿名要介護認定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取扱者のログイン時刻、アクセス時間並びにログイン中に操作した取扱者が特定できるようにすること。

e）匿名要介護認定情報等を利用する情報システムはアクセス記録機能を備えたものであること。仮に当該機能がない場合に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。
なお、記録等は利用終了後少なくとも1年は保管すること。

f）匿名要介護認定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、改ざん及び追加等を防止する対策を講ずること。

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、匿名要介護認定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、システム構築時に、やむを得ず適切に管理されていないメディアを使用する場合には、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）匿名要介護認定情報等の保存・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。

j）匿名要介護認定情報等の利用終了後には、情報システム内に記録された匿名要介護認定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の安全対策に十分配意すること。

（参考）高齢者の医療の確保に関する法律・法律施行規則

高齢者の医療の確保に関する法律
（安全管理措置）
第十六条の五
匿名医療保険等関連情報利用者は、匿名医療保険等関連情報の漏えい、滅失又は毀損の防止その他の当該匿名医療保険等関連情報の安全管理のために必要かつ適切なものとして厚生労働省令で定める措置を講じなければならない。

高齢者の医療の確保に関する法律施行規則
（法第十六条の五の厚生労働省令で定める措置）
第五条の九　法第十六条の五の厚生労働省令で定める措置は、次に掲げる措置とする。
一　次に掲げる組織的な安全管理に関する措置
イ　匿名医療保険等関連情報の適正管理に係る基本方針を定めること。
ロ　匿名医療保険等関連情報を取り扱う者の権限及び責務並びに業務を明確にすること。
ハ　匿名医療保険等関連情報に係る管理簿を整備すること。
ニ　匿名医療保険等関連情報の適正管理に関する規程の策定及び実施並びにその運用の評価及び改善を行うこと。
ホ　匿名医療保険等関連情報の漏えい、滅失又は毀損の発生時における事務処理体制を整備すること。

二　次に掲げる人的な安全管理に関する措置
イ　匿名医療保険等関連情報を取り扱う者が、次のいずれにも該当しない者であることを確認すること。
（1）法、健康保険法、介護保険法、統計法、個人情報の保護に関する法律、行政機関の保有する個人情報の保護に関する法律又は独立行政法人等の保有する個人情報の保護に関する法律若しくは個人情報の保護に関する法律又はこれらの法律に基づく命令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から起算して五年を経過しない者
（2）暴力団員等
（3）匿名医療保険等関連情報等を利用して不適切な行為をしたことがあるか、又は関係法令の規定に反した等の理由により匿名医療保険等関連情報等を取り扱うことが不適切であると厚生労働大臣が認めた者
ロ　匿名医療保険等関連情報を取り扱う者に対する必要な教育及び訓練を行うこと。

三　次に掲げる物理的な安全管理に関する措置
イ　匿名医療保険等関連情報を取り扱う区域を特定すること。
ロ　匿名医療保険等関連情報を取り扱う区域として特定された区域への立入りの管理及び制限をするための措置を講ずること。
ハ　匿名医療保険等関連情報の取扱いに係る機器の盗難等の防止のための措置を講ずること。
ニ　匿名医療保険等関連情報を削除し、又は匿名医療保険等関連情報が記録された機器等を廃棄する場合には、復元不可能な手段で行うこと。

四　次に掲げる技術的な安全管理に関する措置
イ　匿名医療保険等関連情報を取り扱う電子計算機等において当該匿名医療保険等関連情報を処理することができる者を限定するため、適切な措置を講ずること。
ロ　匿名医療保険等関連情報を取り扱う電子計算機等が電気通信回線等に接続している場合、不正アクセス行為(不正アクセス行為の禁止等に関する法律(平成十一年法律第百二十八号)第二条第四項に規定する不正アクセス行為をいう。)を防止するため、適切な措置を講ずること。
ハ　匿名医療保険等関連情報を取り扱う電子計算機等が電気通信回線に接続していることに伴う匿名医療保険等関連情報の漏えい、滅失又は毀損を防止するため、適切な措置を講ずること。

五　次に掲げるその他の安全管理に関する措置
イ　匿名医療保険等関連情報の取扱いに関する業務を委託するときは、当該委託を受けた者が講ずる当該匿名医療保険等関連情報の安全管理のために必要かつ適切な措置について必要な確認を行うこと。
ロ　イの委託を受けた者に対する必要かつ適切な監督を行うこと。
ハ　匿名医療保険等関連情報を取り扱う者としてあらかじめ申し出た者以外の者が当該匿名医療保険等関連情報を取り扱うことを禁止すること。
（令二厚労令一六二・追加、令四厚労令六四・一部改正）

（参考）介護保険法・法律施行規則

介護保険法
（安全管理措置）
第百十八条の六
　匿名介護保険等関連情報利用者は、匿名介護保険等関連情報の漏えい、滅失又は毀損の防止その他の当該匿名介護保険等関連情報の安全管理のために必要かつ適切なものとして厚生労働省令で定める措置を講じなければならない。

介護保険法施行規則
（法第百十八条の六の厚生労働省令で定める措置）
法第百十八条の六の厚生労働省令で定める措置は、次に掲げる措置とする。
一　次に掲げる組織的な安全管理に関する措置
イ　匿名介護保険等関連情報の適正管理に係る基本方針を定めること。
ロ　匿名介護保険等関連情報を取り扱う者の権限及び責務並びに業務を明確にすること。
ハ　匿名介護保険等関連情報に係る管理簿を整備すること。
ニ　匿名介護保険等関連情報の適正管理に関する規程の策定及び実施並びにその運用の評価及び改善を行うこと。
ホ　匿名介護保険等関連情報の漏えい、滅失又は毀損の発生時における事務処理体制を整備すること。

二　次に掲げる人的な安全管理に関する措置
イ　匿名介護保険等関連情報を取り扱う者が、次のいずれにも該当しない者であることを確認すること。
（1）法、健康保険法、高齢者の医療の確保に関する法律、統計法、個人情報の保護に関する法律、行政機関の保有する個人情報の保護に関する法律又は独立行政法人等の保有する個人情報の保護に関する法律又はこれらの法律に基づく命令の規定に違反し、罰金以上の刑に処せられ、その執行を終わり、又は執行を受けることがなくなった日から起算して五年を経過しない者
（2）暴力団員等
（3）匿名介護保険等関連情報等を利用して不適切な行為をしたことがあるか、又は関係法令の規定に反した等の理由により匿名介護保険等関連情報等を取り扱うことが不適切であると厚生労働大臣が認めた者
ロ　匿名介護保険等関連情報を取り扱う者に対する必要な教育及び訓練を行うこと。

三　次に掲げる物理的な安全管理に関する措置
イ　匿名介護保険等関連情報を取り扱う区域を特定すること。
ロ　匿名介護保険等関連情報を取り扱う区域として特定された区域への立入りの管理及び制限をするための措置を講ずること。
ハ　匿名介護保険等関連情報の取扱いに係る機器の盗難等の防止のための措置を講ずること。
ニ　匿名介護保険等関連情報を削除し、又は匿名介護保険等関連情報が記録された機器等を廃棄する場合には、復元不可能な手段で行うこと。

四　次に掲げる技術的な安全管理に関する措置
イ　匿名介護保険等関連情報を取り扱う電子計算機等において当該匿名介護保険等関連情報を処理することができる者を限定するため、適切な措置を講ずること。
ロ　匿名介護保険等関連情報を取り扱う電子計算機等が電気通信回線等に接続している場合、不正アクセス行為(不正アクセス行為の禁止等に関する法律(平成十一年法律第百二十八号)第二条第四項に規定する不正アクセス行為をいう。)を防止するため、適切な措置を講ずること。
ハ　匿名介護保険等関連情報を取り扱う電子計算機等が電気通信回線に接続していることに伴う匿名介護保険等関連情報の漏えい、滅失又は毀損を防止するため、適切な措置を講ずること。

五　次に掲げるその他の安全管理に関する措置
イ　匿名介護保険等関連情報の取扱いに関する業務を委託するときは、当該委託を受けた者が講ずる当該匿名介護保険等関連情報の安全管理のための必要かつ適切な措置について必要な確認を行うこと。
ロ　イの委託を受けた者に対する必要かつ適切な監督を行うこと。
ハ　匿名介護保険等関連情報を取り扱う者としてあらかじめ申し出た者以外の者が当該匿名介護保険等関連情報を取り扱うことを禁止すること。
（令元法九・追加、令二厚労令一六二・追加）