諸外国におけるPIAについて

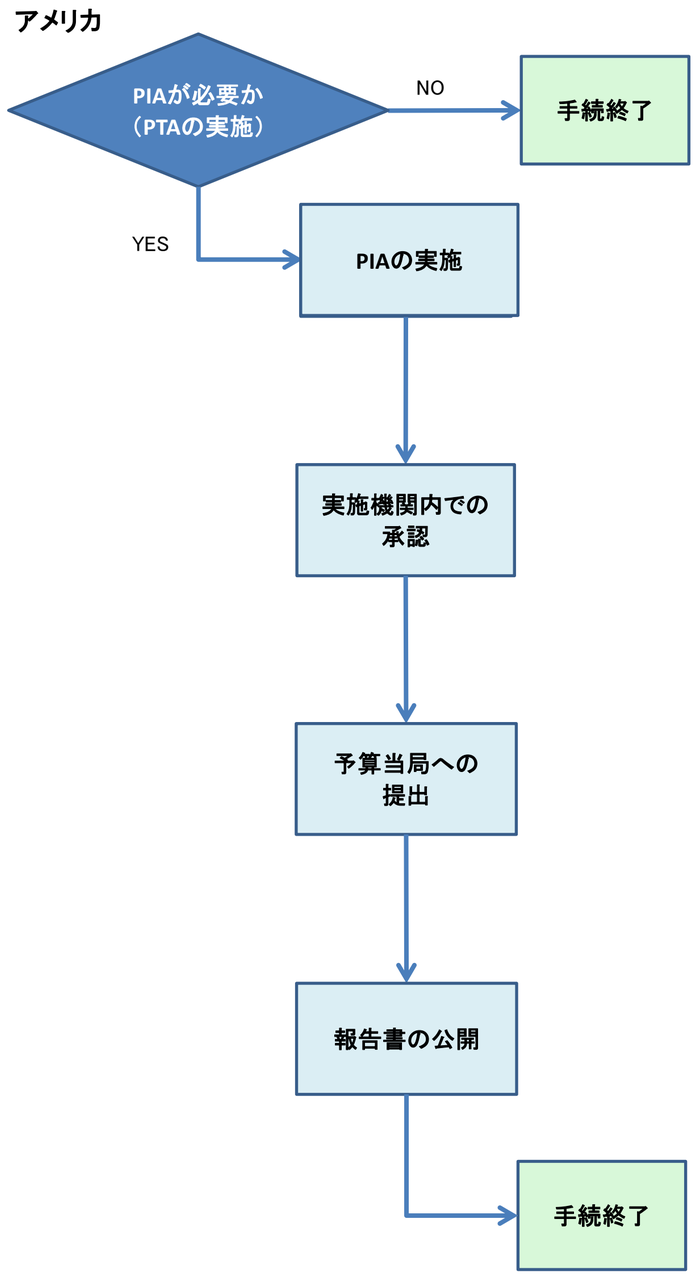
参考資料2

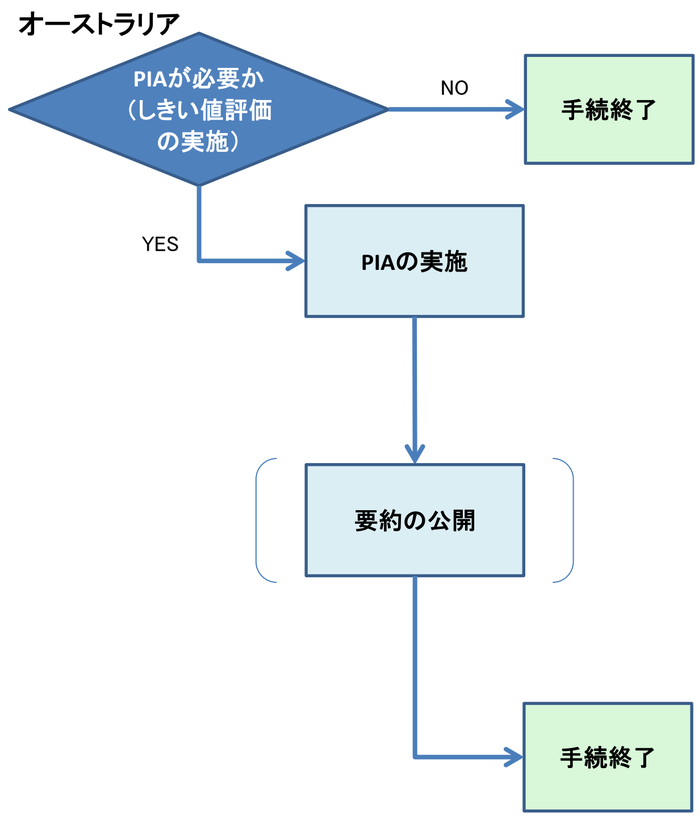
	日本（大綱）	アメリカ	オーストラリア	イギリス
制度名称	情報保護評価	PIA	PIA	PIA
法律上の根拠	番号法	電子政府法第208条 国土安全保障法222条	なし	なし
行政機関の実施義務	あり	あり		あり （内閣府が中央政府機関に対しPIAの実施を義務付け）
対象	「番号」に係る個人情報を取り扱うシステム ※システム改修も含む	個人識別情報を含むプログラム、システム、技術、規則（※1） ※新たなプライバシーリスクを生起するシステム改修も含む（※3）	個人情報を取り扱う提案、レビュー、システム、データベース、プログラム、アプリケーション、サービス、取組み ※システム改修も含む	個人のプライバシーに対して本質的なリスクとなりうるシステム・方針・手続等の新設又は変更 ※システム改修も含む
実施機関	システムの開発・改修を行う行政機関	システムの開発・改修を行う行政機関	システムの開発・改修を行う行政機関	システムの開発・改修を行う行政機関
承認方法	第三者機関が承認する	・実施機関内のレビュー官が承認する ・その後、行政管理予算局に提出され、予算措置の判断材料とされる	・承認はなし	・承認はなし
公開		原則公開	第三者機関によって要約開示が推奨されている	原則公開
非公開事由		公表が以下を生起し得る範囲で、非公開とできる ・セキュリティ上の懸念 ・機密情報（国家セキュリティ情報）の暴露 ・機微情報（国家利益、法執行又は競争に潜在的損害を与えるものなど）の暴露	セキュリティ、商業上の保秘、競争上の理由等から非公表とされる場合がある	・セキュリティ上又は商業上機微な情報については非公開とできる ・但し、非公開情報は可能な限り部分的に留めるべきとされ、たとえば別添部分にのみ非公開情報を記載し、別添部分のみ非公開とすることなどが例として挙げられている
第三者機関の役割（第三者機関名）	情報保護評価に対する承認	― （第三者機関なし）	PIAに対する助言 （Office of the Australian Information Commissioner (OAIC)）	PIAに対する助言 （Information Commissioner's Office(ICO)）
指針（作成者）	・情報保護評価ガイドライン（第三者機関）	・PIAガイダンス（国土安全保障省） ・PIAテンプレート（国土安全保障省） ・電子政府法におけるプライバシー条項の実施のためのOMBガイダンス（行政管理予算局） ・その他、独自のPIAガイダンス・テンプレートを定めている省も存在する	・PIAガイド（第三者機関）	・PIAハンドブック（第三者機関）
全体フロー		①プライバシーしきい値分析（Privacy Threshold Analysis,「PTA」）を行う（※5） →PIAが必要か判断する ※なおPTAは3年で失効するため要更新 ②PIAを実施する ③PIAを更新する	①しきい値評価（Threshold Assessment）を行う →PIAが必要か判断する ②PIAを実施する	①PIAスクリーニング判断を行う →PIAが必要か、必要な場合どのようなPIAが必要か判断する ②場合に応じて以下を行う A)フルスケールPIAを行う B)スモールスケールPIAを行う C)PIAを実施しない ③プライバシー法令遵守チェック・データ保護遵守チェックを行う
その他			しきい値評価は、PIAが必要か否かの判断に資するものであるが、どのような場合にPIAを実施しなければならないかに関しての明確なルールはなく、かかる点については個々のプロジェクトにおいて個別に検討しなければならない。	

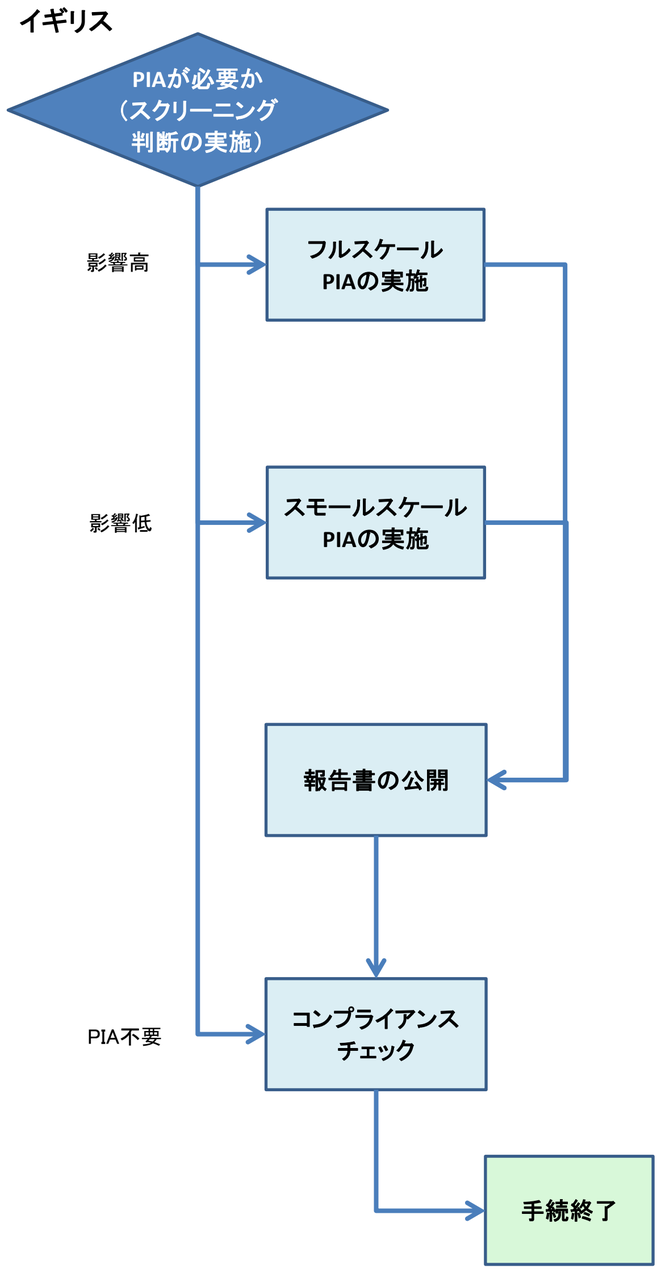
諸外国におけるPIAについて

	カナダ（連邦）	カナダ（ブリティッシュコロンビア州）	カナダ（アルバータ州）
制度名称	PIA	PIA	PIA
法律上の根拠	なし	情報公開・プライバシー保護法	健康情報法 （健康情報のみを対象とする）
行政機関の実施義務	あり （プライバシー影響評価指令に規定）	あり	あり
対象	①個人に直接影響を与える意思決定過程で個人情報を使用するとき ②行政目的で個人情報を使用する既存プログラムや活動を大幅に修正するとき ③プログラムや活動を政府の別組織や民間部門に外部委託又は移転し、プログラムや活動に大幅な変更をもたらすとき ※システム改修も含む	すべての新しいプロジェクト、プログラム、アプリケーション、システム、法律（Enactment）、及び改修されたプロジェクト、プログラム、アプリケーション、システム（※4） ※システム改修も含む	①個人を特定する健康情報の収集、使用又は開示に関連する実務又は情報システムの新設・変更 ②データマッチング（複数のデータを結合することで新しい情報を生成することをいう。）を行う場合 ※①のうちの変更については、健康情報に係るプライバシーに対し新しいリスクをもたらす変更であれば、PIAが必要とされる。
実施機関	システムの開発・改修を行う行政機関	システムの開発・改修を行う行政機関	システムの開発・改修を行う行政機関
承認方法	・実施機関内の責任者が承認する ・第三者機関が、プライバシー法所管機関として、PIAの提出を受ける ・PIA報告書はカナダ財務委員会にも提出され、カナダ財務委員会は、個人情報バンクへのレビュー及び承認の観点から、PIAの義務的要件が完了しているかのみ確認する	・実施機関内の責任者が承認し署名する ・ブリティッシュコロンビア州チーフインフォメーションオフィサーオフィス（第三者機関ではない。）によるレビューを経る	・承認はなし（法令で要求される、プライバシー保護のために適切なレベルを確保する義務は行政機関にあるため、第三者機関はPIAを「認可」することはできない。但し第三者機関は、行政機関がプライバシー保護について合理的な努力を行っていると考えられる場合にはPIAを「受領」する） ・第三者機関によるレビューを経る
公開	部分公開		第三者機関は、受領したすべてのPIAの登録を行っており（OIPC PIA Registry）、プロジェクトの概要について第三者機関のWebサイト上で閲覧することができる
非公開事由	PIA報告書につき、公開又はその他の行政機関と共有する際は、セキュリティ要件やその他機密性、法的考慮を行うものとされている		
第三者機関の役割 （第三者機関名）	プライバシー法の観点からPIA報告書の提出を受け、また追加資料を要求することができる （Office of the Privacy Commissioner of Canada）	（Office of the Information and Privacy Commissioner（OIPC））	PIAに対するレビュー・コメント （Office of the Information and Privacy Commissioner（OIPC））
指針（作成者）	・PIA指令（カナダ財務委員会） ・PIAガイドライン（カナダ財務委員会）	・中核政策及び手続マニュアル （会計検査院） ・PIAツール（労働・市民サービス省IM/ITプライバシー法令部門） ・PIAツール（森林国土資源省）	・PIA要件 （第三者機関）
全体フロー	①個人情報を収集するか判断する →PIAが必要か判断する ②予備PIAを行うか任意に判断する →予備PIAとは、詳細情報がわからない設計段階で行うPIAである。予備PIAを実施してもプライバシーへ及ぼす影響がある場合は、詳細事項が決定された後にPIAを実施しなければならない ③PIAを実施する	①個人情報を収集するか判断する →PIAが必要か判断する ②予備PIAを実施する ③本PIAを実施する ④ブリティッシュコロンビア州チーフインフォメーションオフィサーオフィスによるレビューを受ける	①PIA報告書を作成する ②幹部の署名が付されたPIA報告書を第三者機関に提出する ③第三者機関の受領を確認する（※6） ④定期的なPIAの再実施を行う
その他		PIAを完成させても、第三者機関は、PIAによってカバーされている問題やPIA自体について調査したりコメントしたりすることができる旨がブリティッシュコロンビア州チーフインフォメーションオフィサーオフィスWebサイト上で明記されている。	PIAを実施したことは関連法令の適用除外事由とならない旨がWebサイト上で明記されている。

諸外国におけるPIAの実施枠組み

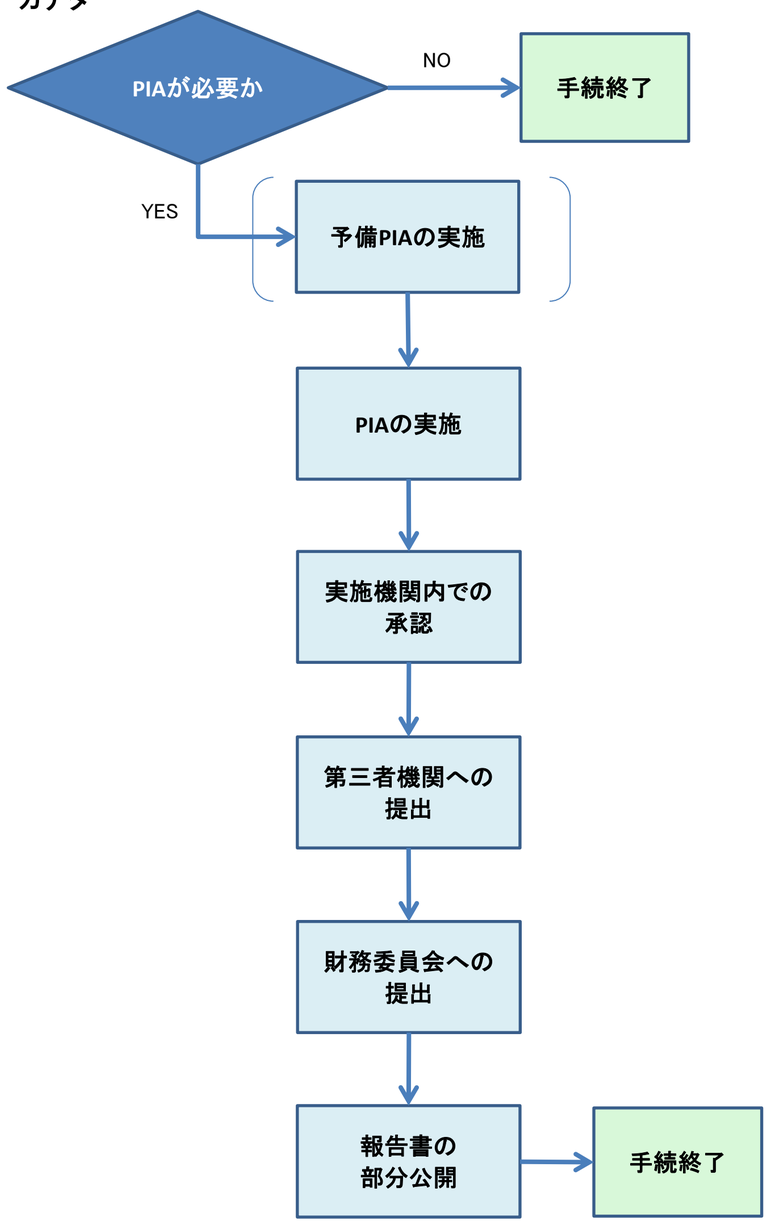




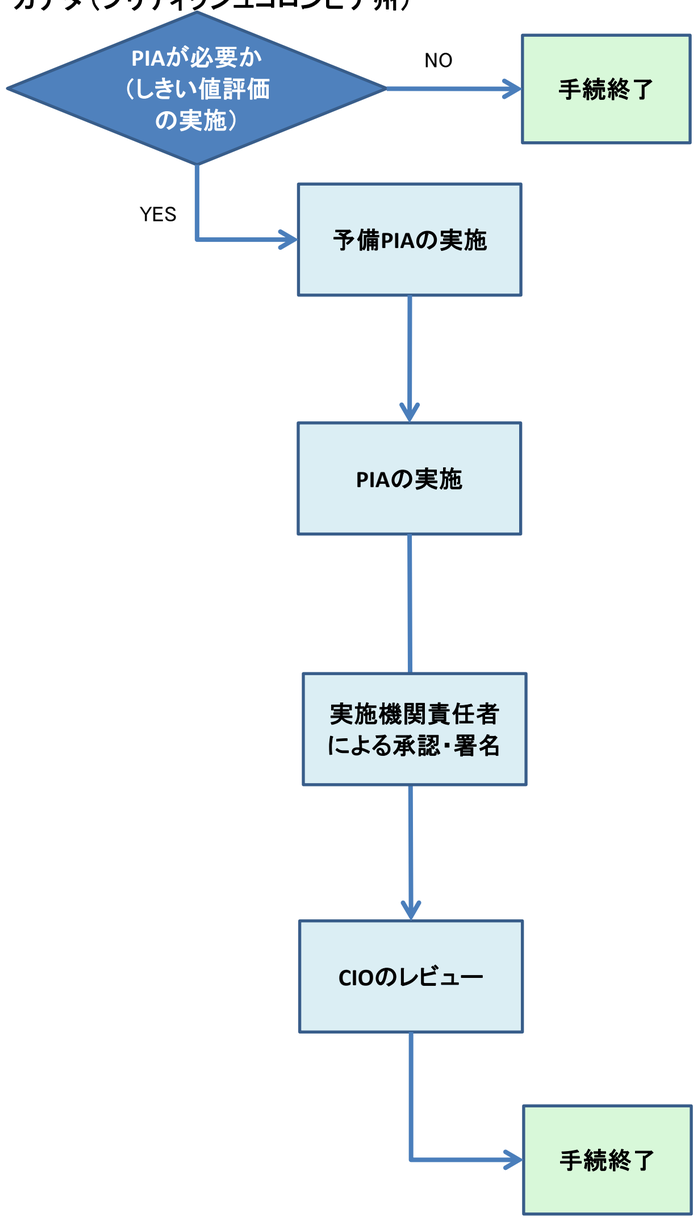


諸外国におけるPIAの実施枠組み

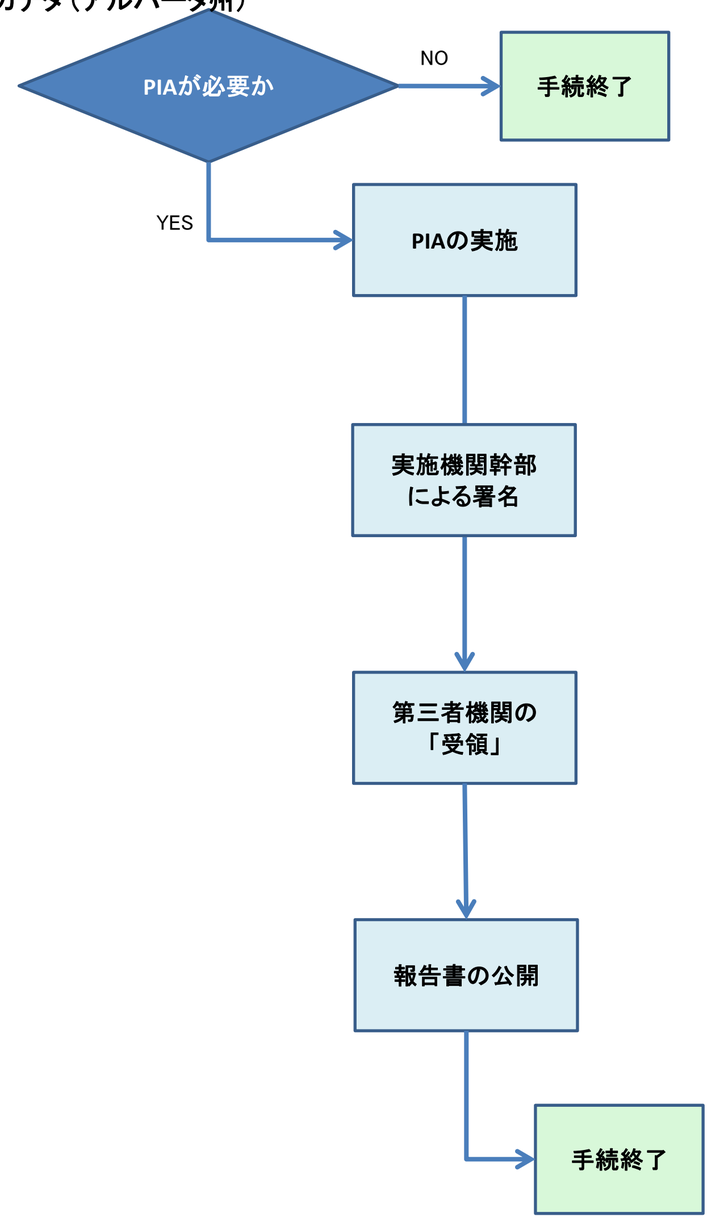
カナダ



カナダ（ブリティッシュコロンビア州）



カナダ（アルバータ州）



（注１）公開情報を基に、内閣官房社会保障改革担当室が作成。
（注２）諸外国におけるPIAについては現在も引き続き調査中であり、本資料は改訂の可能性を有するものである。

（※1）国土安全保障省によるPIAガイダンスによれば、「個人識別情報を含むプログラム、システム、技術又は規則」に対してPIAが要求されるが、その対象を詳述すると以下の通りである。
① 個人識別情報を収集、保持又は配布する情報技術の開発又は調達（電子政府法202条）
② 情報技術を用いて収集、保持又は配布され、かつ連邦の機関若しくは従業員（※5）以外の10名以上の特定の個人に対して個人識別可能な質問がなされたか、個人識別可能な報告要件が課された場合に、特定の個人に対して物理的又はオンライン上で連絡をとることができる個人識別情報を含む情報の新しい収集（電子政府法202条）（※2）
③ 国土安全保障省の新しい規則及び個人情報プライバシー
なお、一時的に保持する情報であっても、プライバシーへの問題がある技術（RFID、バイオメトリックスキャン、データマイニング、地理的追跡など）の場合は、PIAが要求されることがある 。また技術に変更がない場合でも、情報収集源に変更がある場合には、PIAが要求される 。

（※2）行政管理予算局OMBガイダンスでは、「連邦の機関又は従業員以外の10名以上の個人についての、個人識別可能な情報の新しい電子的な収集」と要約されている。

（※3）行政管理予算局OMBガイダンスでは、具体例として以下が挙げられている 。
① 紙ベースの記録を電子的システムに変換するとき
② 情報収集を匿名的態様から非匿名的態様に変更するとき
③ システム管理の重大な変更（たとえば、複数のデータストアにアクセスできるようなリレーショナルデータベース技術やWebベースの処理を新たに採用する場合、かかる変更は、データの暴露を起こしやすいオープンな環境や方法を生起するのでリスクがある）
④ 重大な統合（個人識別情報を保有する政府のデータベースと他のデータベースとの統合、中央化、マッチングその他重大な操作）
⑤ 公衆がアクセスするシステムに、ユーザ認証技術（パスワード、電子認証、バイオメトリックスなど）を採用するとき
⑥ 個人識別情報を含む既存データベースに商業情報源又は公的情報源を体系的に統合するとき（既存技術を用いてかかる情報源に対しアドホックに問い合わせを行う場合は、PIAは要求されない）
⑦ 省庁間での新たな利用（分野横断的な電子政府行動の場合は、主官庁がPIAを実施すること）
⑧ 内部フロー又は収集（情報の新たな、かつ重大な利用や開示をもたらすビジネスプロセスの変更、又は個人識別情報の追加項目のシステムへの統合をもたらすビジネスプロセスの変更）
⑨ データ特徴の変更（個人識別可能な新たな情報が収集に加えられることで、個人のプライバシーに対するリスクがもたらされるとき（健康情報や経済情報の追加など））

（※4）すべてのものがいったんPIAの対象となるが、個人情報が収集されない場合は、PIAのうち基本情報についてのみ対応すれば足りる。

（※5）各省内で、PIAに係る要件や手続きをカスタマイズして定めている省も存在し、たとえば内務省（Department of Interior）では、従業員の個人識別情報についてもPIAの対象とし、かつPTAの前にPreliminary Reviewフェーズを設け、従業員を含む個人について識別可能情報を保持するか否かをPreliminary Reviewで確定し、保持しない場合にはその後のPIA手続きは不要とのスキームを採用している。

（※6）第三者機関では、ポートフォリオオフィサー（Portfolio Officer）がレビューを行う。
ポートフォリオオフィサーは、PIAに関し説明や明確化を求めることができる。
第三者機関によるレビュー及びコメント内容を実装前に反映できるよう、提出者は、十分な時間的余裕をもってPIAの提出を行う必要がある。
第三者機関は、45営業日以内に当初のレビュー案を示すよう努めているが、レビュー提示までに要する期間は、第三者機関からの質問に対する提出者側の反応速度によって変動する。
ポートフォリオオフィサーは、提出者に確認の書面を送付することでPIAを受領する。PIAの受領は承認ではなく、提出者が健康情報法の要件を検討し、プライバシー保護のために合理的な努力を行っている旨のポートフォリオオフィサーの意見を示しているにすぎない。
ポートフォリオオフィサーの示す期限までに、ポートフォリオオフィサーによるすべての質問に回答しない場合は、PIA報告書は未受領となる。