ハートフロー・ジャパン合同会社 個人情報保護方針と手順

総則

本方針および手順は、個人情報保護に関するものであり、ハートフローの日本における個人情報(以下、本契約において定義される)の収集に適用され、個人情報の保護に関する法律および他の関連規則(指針を含む)(個人情報保護法および他の関連規則を総称して「個人情報保護規則」という)に基づき、常に適用される。

ハートフローは、本規程および/または適用される個人情報保護規程と矛盾する方法で、保有する個人情報にアクセスし、使用し、開示し、変更しまたは破棄してはならない。

ハートフローは、個人情報保護規程に基づき個人情報の保護に努める。

ハートフローは、個人情報保護規程に基づき、患者およびその代諾者に個人情報への適切なアクセスを提供する。

ハートフローは、個人情報の機密性、完全性、可用性を保護するために、引き続きリスクアセスメントを実施し、適用される個人情報保護規程の遵守状況を監視し、個人情報保護規則およびベストプラクティスに準拠するために、必要に応じて本規則の改訂を行う。

ハートフローの経営陣は、本規程、および個人情報保護規程、業務、技術、および/または法的規制またはガイダンスの重大な変更により必要となる変更または修正を適時に承認し、採択し、実施する。

定義

資本論：本規則において使用される用語は、本規則に定める意味を有する。

電子ポータブルデバイス：「電子ポータブルデバイス」とは、以下に定義する従業員が利用できる、または従業員が所有または使用する携帯端末またはモバイル端末のうち、個人情報を送信または保存するために使用できるものをいい、ラップトップ、タブレット、スマートフォン、携帯電話、コンパクトディスク、サムドライブ、Personal Digital Assistants（PDA）、パームトップコンピュータ、携帯/ハンドヘルド通信機器（例：携帯電話、ポケットベル、ラジオ）、カメラ（デジタルおよびアナログの両方）、その他類似の機器を含みますが、これらに限定されません。特に、電話の発着信、メッセージの送信、テキストメッセージの送信、イン

ターネットの閲覧、電子メールのダウンロードや閲覧・返信などを行う携帯機器に適用される。

医療提供者：個人情報取扱事業者である患者に対する日本を拠点とする治療の提供者。

ハートフロー提供デバイス：業務上の目的でハートフローが従業員に提供するデスクトップPCやノートPC、モバイル機器や電話機（電子ポータブルデバイスを含む）（例えば、従業員がハートフローの業務に従事している場合や、ハートフローの利益のために活動を行っている場合で、業務内容としてハートフローからそのような業務・活動を行うことを許可されている場合など）。

手順書：ハートフロー・ジャパン合同会社 個人情報保護手続き

患者：「患者」とは、ハートフローカスタマーで撮影された冠動脈 CT スキャンを通して医療提供者を介して治療を提供する医師の患者として、日本国内でハートフロー解析の対象となった個人を指す。「患者」には、そのような個人に委任された代理人も含まれる。

パーソナル・デバイス：「パーソナル・デバイス」とは、ハートフローが提供しない電子ポータブルデバイスを含み、従業員により所有され、維持される、または従業員により個人的に提供されるあらゆるデバイスを意味する。

個人情報：「個人情報」とは、要配慮個人情報（個人情報保護規則に定義されている）を含む、特定されたまたは特定可能な自然人（「情報主体」）に関するあらゆる情報を意味する。識別可能な自然人とは、特に名前、識別番号、位置情報、オンライン識別子などの識別子、または自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的アイデンティティに固有の 1 つ以上の要素を参照して、直接的または間接的に識別することができる人をいい、一般的なデータおよび自然人の病歴（個人情報保護規則に定義される）に関するデータを含みますが、これらに限定されない。

処理：「処理」とは、個人情報または一連の個人情報に対して実行される操作または一連の操作を意味し、収集、記録、組織化、構造化、保存、改変または改変、検索、相談、使用、送信による開示、配布またはその他利用可能にする自動化された手段によって行われるか否かを問わず、制限、消去または破棄および「プロセス」は、相応に解釈されるものとする。

業務従事者または従業員：「業務従事者」とは、ハートフローの役員、幹部、取締役、従業員、ボランティア、研修生、その他、ハートフローのために、またはハートフローのために、個人情報に関わる業務を行う独立した契約者を含み、ハートフローのために業務を行う行為がハートフ

ローの直接の支配下にある者をいい、ハートフローから報酬を得ているか否か、職階に関係なく、個人情報保護管理者を含みます。「従業員」とは、業務従事者の集合体を指す。

作業空間：「作業空間」とは、業務従事者が職務を遂行する物理的空間、および/またはハートフローの情報システムが保管または配置されている物理的空間をいう。

ワークステーション：「ワークステーション」とは、個人情報、電子健康記録、およびオンサイトおよびオフサイトのバックアップシステムを含むがこれらに限定されない、ハートフローの情報システムに従業員が物理的または電子的にアクセスすることができるワークスペース内の任意のステーションをいう。

個人情報保護責任者の責務

個人情報保護管理責任者等

ハートフローは組織全体で個人情報保護規程を継続的に遵守するためのプログラムを効果的に実施、管理、および維持するため、HeartFlow, Inc.のチーフエシックスコンプライアンスオフィサー(CECO)の指示に基づき、地域プライバシー教育担当者およびプライバシーコンサルテ
ィングオフィサー(以下、総称して「担当者」または「役員」)を任命している。役員の役割および責任は、CECOおよびこれらの手順に準拠する。地域プライバシー教育担当者は、プライバシーコンサルティングオフィサーを管理・監督する。プライバシーコンサルティング担当者は、個人情報の収集または使用に関連するすべての問い合わせを受け、この手順に記載された担当者の役割と責任に従って問い合わせを管理する。地域プライバシー教育担当者は、個人情報保護に関する社内教育を従業員に提供するものとする。役員のその他の役割と責任は以下の通りである：

地域プライバシー教育担当者：日本のハートフロー解析のチーフプライバシーオフィサーは、社内教育に責任を負う。担当者は、安全情報の報告に伴い、個人情報に関する事項を四半期毎にプライバシーコンプライアンス部長に報告する。

プライバシーコンサルティングオフィサー：顧客、患者、内部および外部の連絡窓口は、顧客/患者の問合せおよびその他の事故情報の存在および進捗状況を、安全情報の報告と併せて毎月「地域プライバシー教育担当者」に報告する。

>>ハートフロージャパン組織図

従業員の責任、個人情報へのアクセス、研修、制裁、報復の禁止

総則

ハートフローは、個人情報保護法への取り組みが成功するかどうかは、各従業員のコミットメント、誠実さ、パフォーマンスにかかっていると考えている。従って、ハートフローは、従業員一人ひとりが本規則および個人情報保護規程を常に遵守し、役員または本契約に基づき指名された被指名者が指示する更なる措置を実施することを要求する。

コンピュータ機器、ソフトウェア、オペレーティング・システム、ストレージ・メディア、当社クラウド・サービス(Google Apps、Workday 等)、電子メールを提供するネットワーク・アカウント、インターネット・ブラウジング、および FTP を含むがこれらに限定されない、ハートフロー提供デバイスおよびインターネット/イントラネット/エクストラネット関連システムは、通常の運営の過程において、会社およびそのクライアントおよびカスタマーの利益のために役立つビジネス目的のためにのみ使用される。

従業員は、常に個人情報を不正なアクセス、使用、開示、および/または破壊から保護し、守らなければならない。意図的に、または偶発的に、そのアクセスを保護することを怠ったことによって、いかなるシステムまたはユーザも、いかなる不正な個人にもアクセスすることは、厳密に禁止される。本規程に定める個人情報保護のための措置に加え、従業員等は、個人情報保護のための物理的なセキュリティ措置が各人によって維持されることを確保する責任を負う。

また、従業員は、以下の通り、すべての個人情報および/またはその他の機密情報または専有情報を確保するものとする：

- 個人情報が記録されている文書 ハードコピー を、特に訪問者等の不正な通行者の目に触れないように、平易に保管すること。また、利用・閲覧場所を離れる場合は、安全な場所に施錠すること；
- 権限のない人、特に訪問者が通過した場合に、個人情報を漏らさないように、または画面上の情報を隠すように、見える画面を備えたコンピュータ・モニタまたはその他の電子媒体を配置すること；
- プリンタ、複写機、ファックス等で個人情報を放置したり、利用できるようにしてはならず、引き出し、保管場所、最低限、はっきりと施錠し、見えない場所に保管するようにする

- 業務上の正当な理由なく、コピー機等の複製技術(スキャナ、デジタルカメラ等)を使用して個人情報をコピーしないこと;
- 個人情報の廃棄・破棄は、許可された場合にのみ、安全な廃棄箱に入れて行う；
- 業務を離れるときや公共の場所にいるときは、不正な情報を見られないように、コンピュータの画面をロックする。
- ウェブアプリケーション、データベース、またはその他の秘密アプリケーションへのセッションが終了し、非アクティブ/未使用セッションをアクティブにしない場合、セッションからログオフする。

従業員は、個人情報について、他の従業員、個人情報の対象となる人物、健康保険プランまたはその他の支払者と、電子的に、電話で、または直接話し合う正当なビジネス上の理由がなければならない。また、メンバーは、個人情報にアクセスする権限のない者または話し合いを受ける正当な業務上の理由がない者の立会いの下で、ハートフロー以外の個人情報について話し合うことはできない。ハートフロー内で個人情報について話し合う際には、他のメンバーや個人情報を聴取する正当な業務上の理由のない者が話し合いを聞くことができないように、あるいは情報を保持するおそれがないように合理的な努力をしなければならない。労働者は、個人情報保護規則を遵守するために本規則を修正・変更する必要があると思われる場合、本規則や個人情報保護規則について理解できない点や疑問点がある場合、および違反行為が発生したと思われる場合には、CECOに通知することを推奨する。メンバーは、ハートフローコンプライアイアンスホットラインを通じて匿名で通報することができるほか、プライバシーコンサルティング担当者に質問・報告することができる。

従業員は、ハートフローの情報システムにログインしている間、合理的な範囲で、勤務時間中に個人の電子メールアカウントにアクセスすることができる。ただし、業務従事者は、未知の送信者からの電子メールの添付ファイルや同封物のダウンロード、リンクの踏襲など、マルウェア、ウィルス、電子メール爆弾などによりハートフルのデータシステムの完全性が損なわれる可能性のある行為を行わないように注意し、個人情報の完全性および安全性に対する脅威から保護するために可能な限りの予防措置を講じなければならない。

ハートフローの地域プライバシー教育担当者からの承認がない場合、業務従事者はハートフロー ワークステーションからソーシャルメディアアカウント(Facebook、Twitter など)にアクセスすることはできない。また、ハートフロー事業者以外の営業時間中は、ハートフローデータ、ハートフローサーバ、ハートフローアプリケーションアカウントにアクセスすることはできない。

ハートフローは、本規程および個人情報保護規程の遵守を確認するために、ハートフロー提供機器および個人用機器に関わるネットワーク、システム、通信、活動、記録を監査・監視する権利を有する。

介護を必要とする特別な個人情報への従業員のアクセスの評価/付与

CECOは、雇用、請負業者、第三者ユーザー、業務従事者、および個人情報へのアクセスを正当に要求する、または要求する可能性のあるその他のすべての候補者が、関連する法令、規則および倫理指針に従い、ビジネス要件、アクセスされる情報の分類、および認識されるリスクに比例して、個人情報にアクセスする職務を行う前に、適切な経歴チェックの対象となることを保証する。個人情報へのアクセスを正当に要求する業務従事者および個人情報へのアクセス方法は、本規則に準拠する。

研修

本規程および個人情報保護規程に関する研修は、少なくとも次のタイミングで受講する:

- 個人情報へのアクセスを許可される前；
- 個人情報保護規程に重要な変更があった場合；
- 本規則の重要な変更を実施した場合
- 本規程の変更により、従業員の業務または業務が変更された場合
- セキュリティインシデントまたは違反が発生した場合など、地域プライバシー教育担当者により適切と判断された場合、および/または年１回、地域プライバシー教育担当者が、コンプライアンスを確保するために年１回の研修が適切または必要であると判断した場合。

地域プライバシー教育担当者または個人情報保護教育担当者は、ハートフローの従業員研修プログラムおよび資料を継続的に評価、モニタリングおよび更新する。これには、アラート、公報、その他の方法(対面での話し合いを含む)、ノートパソコンおよびその他のフィールド機器の適切な使用、電子メール通信、患者の全般的な秘密保持など、ならびに個人情報、セキュリティインシデントおよび/または違反の潜在的または実際の侵害に関する注意喚起を含む。
内容および頻度を含む研修についてのさらなる詳細は、本明細書に記載される。

執行及び制裁

地域プライバシー教育担当者は、本規則および個人情報保護規則の遵守を支援し、実施するために、必要に応じて、労働力の行動を監視および/または監査する。
業務従事者が本規則または個人情報保護規則に違反した場合、地域プライバシー教育担当者はCECO、人事部、管理または法律専門家と協議の上、必要に応じて、どのような制裁を労働力メンバーに課すべきかを決定する。業務従事者は、違反の重大性に応じて、以下のような制裁をうける:

- 軽微な違反または反復されない違反は、短期カウンセリングおよび、必要に応じて、追加のプライバシーおよび/またはセキュリティ研修を受ける
- 意図しない重大な違反が繰り返される場合は、停止又は終了の理由となり得る
- 故意の違反は、個人情報および情報資源へのすべてのアクセスの即時停止および終了をもたらし、雇用の終了につながる可能性がある

地域プライバシー教育担当者は、業務従事者に課された制裁を記録し、文書は業務従事者の人事記録に保管される。

威嚇または報復の禁止

ハートフローは、苦情の提出、報告書の提出など、個人情報保護規程に基づく権利を行使するために、業務従事者またはその他の個人からのサービスの提供を威嚇、威嚇、強制、差別、報復または差し控えないものとする。本非脅迫条項または報復条項に違反した業務従事者は、本手順に記載されるとおりに制裁される。

従業員は、報復行為または脅迫について、プライバシーコンサルティングオフィサー, Heartflow, Inc.の弁護士、CECO、または HeartFlow, Inc.の人事総務部門に通知しなければならない。

システムとワークスペースのセキュリティ

総則

ハートフローのシステムおよび職場のセキュリティに関する詳細は、ここに記載されており、常に業務従事者はこれを遵守しなければならない。

電子携帯機器の使用

「ハートフロー」の「パーソナル・デバイスの使用に関する方針」の詳細は、本契約および

「手順」に記載されており、常に「従業員」が遵守しなければならない。来場者、従業員ではない作業スペースを訪れるすべての人は、訪問者が個人情報を閲覧、閲覧および/または保持することを防止し、役員からのすべての要求および/または説明書に従うことを保証するために、従業員メンバーによって監督されなければならない。

個人情報の伝達の取扱い

電話、電子メール、ウェブアプリケーション、紙、ファックスによる個人情報の送信に関するハートフローの方針の詳細は、ここに記載されており、従業員は常に遵守しなければならない。

複写機・複写サービス業

個人情報は、ハートフローのコピー機に放置してはならない。

ハートフローの既存のコピー機能が業務に対応できない症例を除き、個人情報はコピーサービスに送信されない。その症例、ハートフローは、コピーサービスに適用される個人情報保護規則に準拠した形式でデータ処理契約を締結しなければならない。また、コピーサービスとの間での個人情報の転送および配信時に適切な保護策が使用されることを保証しなければならない。

リスクアセスメント、管理、調査、監査、電子システムの検査、文書化継続的評価

地域プライバシー教育担当者は、個人情報保護規程を遵守するために必要に応じて継続的に、個人情報の機密性、完全性および利用可能性に対する潜在的および実際のリスクまたは脆弱性「継続的評価を評価し、監視する：

- 個人情報の作業、慣行、使用、開示をモニタリング、監査、または評価し、従業員が本手順を遵守していることを確認する;
- ハートフロー操作の有効性・有効性の確認；
- 個人情報、セキュリティインシデント、および/または違反の不正アクセス、使用、または開示につながる可能性のあるハートフロープロセスの特定;
- 個人情報、その他のセキュリティ事故、および/または違反の不正アクセス、使用または開示の実際のリスクまたは潜在的リスクを軽減するための実践的な措置およびプロセスを特定する；
- 個人情報の不正開示、セキュリティ事故、および/または違反の事実または潜在的な不

- 正開示の報告に速やかに対応し、適用されるすべての個人情報保護規則を順守すること
- また、本手順および個人情報保護規則の遵守を確実にするために、下請業者またはその他の第三者ベンダーによる個人情報の実施、使用または開示をモニタリング、監査または評価すること

実施中の評価および関連活動は、本手順書の文書保管規定に従って文書化され、維持される。地域プライバシー・教育担当者は、適宜、法律顧問または CECOと協議の上、本手順書に必要な変更を加え、当社のリーダーシップにより適切に承認されたことを確認し、従業員に通知し、必要に応じて関連する研修を提供する。

ハートフローの代理人またはハートフローとの契約に基づく業務を遂行する者および事業体への個人情報のアクセスおよび開示サプライヤー、供給者、その他の労働力の一部でない者
個人情報保護規程は、提供者・仕入先(再委託先)が当社に提供するサービスの一環として、当社に代わって個人情報を取り扱う場合には、当社と文書による契約を締結することを義務付ける。

地域プライバシー教育担当者は、ハートフローが個人情報を提供する前に、データ処理契約が必要であるか、状況に応じて慎重であるかを判断し、そうである場合には、ハートフローが当該個人情報を提供する前に、当該個人または事業体と当該契約を締結することを保証する。言い換えれば、ハートフローは、個人情報保護規程に準拠した書面による情報処理契約を締結した場合に限り、患者様の許可なく、ハートフルのサービスを提供する事業者が個人情報にアクセスし、使用、維持、送信、作成することを許可する。

地域プライバシー教育担当者は、必要に応じて、サブプロセッサの経歴チェックを実施する。個人情報にアクセスする可能性のあるサブプロセッサを知った従業員は、事前に地域プライバシー教育担当者に、ハートフローとの有効な、最新の、締結されたデータ処理契約および/または秘密保持契約を適切な締結していることを確認することなく、いかなる状況においても、個人情報へのアクセスを提供してはならない。当該情報が決定できない場合、または当該契約の有効性について疑問がある場合、従業員は、顧問弁護士またはCECOの事務所を通じて許可が提供されない限り、当該人または事業体にいかなるアクセスも提供してはならない。

地域プライバシー教育担当者は、すべての既存のデータ処理契約および秘密保持契約の財産目録を作成し、維持するものとし、当該契約の終了条件または各データ処理契約および/または秘密保持契約が終了する日を記載するものとし、データ処理契約または秘密保持契約の終了後 10 年間、原本を保持するものとする。

個人情報に関する患者からの依頼

ハートフローは、すべての患者が、当社が保有する個人情報に関連して、個人情報保護規程に基づく一定の権利を有していることを認識する。適用される個人情報保護規則により制限されない限り、ハートフローは、個人情報取扱事業者としての患者が関連する医療提供者に対して行われる要求が、個人情報保護規則に準拠していることを保証するために、医療提供者および/またはハートフローカスタマーに対して合理的な支援を提供する。

「個人情報保護規程」に基づく「患者」からの要請には、「個人情報」のアクセス要求、「個人情報の変更要求」、「個人情報の削除要求」などが含まれるが、これらに限定されない。ハートフローは、個人情報の請求があった場合において、請求された個人情報がハートフローに保管されていないときは、必要に応じて、ヘルスケア・プロバイダーに対し、個人情報を保管するプロバイダー、個人、または事業体に指示を行う。

個人情報ハートフローに関する権利を行使する患者に関連して受領されたすべての要求は、地域プライバシー教育担当役員、最高倫理コンプライアンス担当役員、および当該要求が許可されるか否かを決定するプライバシーコンプライアンス担当取締役と相談する責任を負うプライバシーコンサルティングオフィサーに照会されなければならず、また当該要求が許可されるか否かを決定し、当該決定および許可されない場合は拒否理由を医療提供者に通知する。

患者の個人情報へのアクセスおよびコピーの要求に対する患者からの要求に応じて、業務従事者は、関連する医療提供者または顧客のサイトと必要かつ適切なすべてのチェックを行うことにより、要求の有効性を保証する。

記録の保存

ハートフローは、適用される「個人情報保護規則」の遵守を確実にするために、当該期間、「患者の個人情報」に関する記録を作成し、保管することとする。

国際データ転送

ハートフローは、個人情報保護規程に準拠する限り、日本国外の個人情報をアメリカ合衆国HeartFlow, Inc. に譲渡することができる。

苦情

患者は、個人情報の使用または開示に関してハートフローに苦情を申し立てることができる。当該苦情は、privacycompliance@heartflow.com のプライバシーコンサルティングオフィサーおよびCECOに指示または提出されなければならない。

プライバシーコンサルティングオフィサーは、弁護士と協議の上、弁護士の指示に基づき、苦情を文書化する。

プライバシーコンサルティングオフィサーは、苦情の対象となる患者の個人情報の使用または開示に関連するすべての該当情報について、弁護士と協議の上、弁護士の指示に基づき検討する。

プライバシーコンサルティングオフィサーは、取締役、コーポレートコンプライアンスおよびプライバシーの指揮監督の下、すべての苦情を遅滞なく審査する。苦情が回答を必要とし、連絡先情報が提供される場合、プライバシーコンサルティングオフィサーまたは被指名人は、患者に書面による回答を作成し、交付する。苦情が回答を必要としない場合、または連絡先情報が提供されない場合、プライバシーコンサルティングオフィサーまたは指名された者は、講じられた措置に関する書面による声明を作成し、提出された苦情に添付する。

使用または開示の違反が確認された場合、プライバシーコンサルティングオフィサーは、適宜、法律顧問またCECOと協議の上、違反の重症度、意図的であるか否か、違反が個人情報の不適切な使用、開示または開示のパターンを示しているか否か、および/またはコンピュータ・資源の悪用を示しているか否かなどの要因を含む事実および状況に基づき、該当する場合、責任ある労働力メンバーを承認するものとする。プライバシーコンサルティングオフィサーは、講じた措置を文書化し、苦情に関するすべての情報をハートフローのファイルに記録する。

プライバシーコンサルティングオフィサーは、弁護士またはCECOと協議の上、苦情にメリットがないと判断した場合、調査は文書化され、ハートフローのファイルに保管される。苦情の対象となる従業員は、いつでも、苦情調査の責任者と同じ責任者とはならない。苦情がプライバシーコンサルティングオフィサーに関するものである場合、弁護士またはCECOに通知し、苦情の調査または直接調査を行う。

セキュリティインシデントおよび/または違反の報告

地域プライバシー教育担当者は、報告、苦情、セキュリティ事故、および違反について直ちにま

たは可及的速やかに分析し、対応するとともに、報告義務のある事故をハートフローの弁護士、CECOおよびプライバシーコンプライアンス担当ディレクターに速やかに連絡する。

ハートフローは、個人情報違反の性質(旨を受ける個人のカテゴリーおよび概数ならびに関連記録を含む)、当該違反に関する調査に関する情報、個人情報違反の起こりうる結果、および個人情報違反の可能性のある旨を軽減するために講じた、または講じようとする措置を、不当に遅滞なくヘルスケア・プロバイダーに提供する。

ハートフローは顧問弁護士と協議の上、個人情報保護規則および またはプライバシーまたはセキュリティ事故または違反の通知を行う契約によりハートフローが要求される場合、個人情報保護規則、契約およびハートフローのセキュリティインシデントおよび違反に関する方針および手順により要求される様式および時間枠で通知することを保証する。具体的には、地域プライバシー教育担当者は、該当する個人情報保護規則に基づき、報告を行う期間を決定する。