データ保護契約

Dell Inc.とその直接子会社、間接子会社（「**デル**」）およびプロバイダは、プロバイダがデルのデータを処理することを許可するプロバイダ契約を締結しています。本データ保護契約（「**DPA**」）は、プロバイダによるデルのデータの処理を管理するものであり、参照することによりプロバイダ契約の一部となります。プロバイダ契約期間中は常に、あるいはプロバイダがデルのデータにアクセスできるかまたはデルのデータを保持している場合はその期間後も、プロバイダは本DPAを順守するものとし、その代表者に本DPAを順守させるものとします。DPA、NDAまたはプロバイダ契約あるいはそれらすべての間で矛盾が生じた場合は、本DPAが優先されるものとします。

1. **定義。**本契約に定義されていない用語はプロバイダ契約に規定されている意味を有します。
   1.1. 「**適用法**」とは、国際、連邦、地方、州、郡、市、および区のすべての省庁、部局、機関、課、委託機関、ならびにそれらのその他の下部部門、あるいはその他の政府機関、公共機関、または準公共機関の、すべての適用法、法規、条例、規則、規定、命令、指示、および同様な政府の要求を意味します。
   1.2. 「**データ漏えい**」とは、デルのデータの偶発的であるか、違法か、または無許可の破壊、変更、公開、悪用、損失、窃盗、アクセス、コピー、使用、改変、処分、侵害、またはデルのデータへのアクセス、あるいは、デルのデータを処理またはソリューションを提供するにあたり、プロバイダが実施する物理的、技術的、または組織的な保障措置を侵害または弱体化させるすべての行為または不作為を意味します。
   1.3. 「**デルのデータ**」とは、デル、その顧客、委任代理人または下請け業者、あるいはそれらすべてによってプロバイダに提供された、または、ソリューションの提供に関連してプロバイダによって処理されたデータのことを意味します。これらには、（a）デルのネットワークを通じてプロバイダに提供されたか、またはプロバイダがアクセスした、あるいはホスティング用または代行サービス用としてプロバイダに提供されたか、またはプロバイダがアクセスしたすべての非公開情報およびデータ、（b）機密性が非常に高いデータ、（c）個人データ、または（d）ユーザー追跡データ、あるいはそれらすべてが含まれます。
   1.4. 「**命令**」とは、個人データの処理に関する個人の保護と、適宜行われる修正または入れ替えに応じたかかる情報の自由な移動に関するEU指令95/46/ECを意味します。
   1.5. 「**EEA**」とは、欧州連合加盟国とノルウェイ、アイスランド、およびリヒテンシュタインを意味します。
   1.6. 「**機密性が非常に高いデータ**」とは、プライバシー保護法（命令を含む）で定義されている社会保障またはその他の政府発行の識別番号、医療または健康情報、口座保護情報、個人の金融口座情報、貸方/借方/贈与またはその他のペイメントカード情報、口座のパスワード、個人の信用および収入情報、知的財産、専有ビジネスモデル、価格設定、顧客のインフラストラクチャ/システム情報またはデータフロー、機密扱いの個人データを意味します。
   1.7. 「**含む**」とは、当該語に先行するいかなる記述、定義、用語または語句の一般性も含むが、それに限定されるか影響することがないことを意味します。また、「含む」とその派生語はそのように解釈されるものとします。
   1.8. 「**プロバイダ**」とは、プロバイダ契約に基づいてデルがソリューションを購入する当事者およびその代表者を意味します。
   1.9. 「**プロバイダ契約**」とは、デルがプロバイダからソリューションを購入するために従うデルとプロバイダの間の契約であり、基本関係契約を含みます。
   1.10. 「**個人データ**」とは、単独で、または他の情報とともに、身元確認済みまたは身元確認可能な自然人に関連付ける情報またはデータ、あるいはプライバシー保護法に基づいて定義された個人情報と見なされるデータを意味します。
   1.11. 「**プライバシー保護法**」とは、プライバシー、データ保護、情報セキュリティの義務、または個人データの処理、あるいはそれらすべてに関する（命令を含む）立法化されたすべての修正条項または規制修正条項あるいは承継を含むすべての法律、法規、命令または規則を意味します。
   1.12. 「**処理**」、「**処理された**」または「**処理する**」とは、使用した目的および手段に関係なく、デルのデータに行われた操作または一連の操作を意味し、アクセス、受領、収集、記録、整理、調整、変更、取得、コンサルテーション、保持、保管、転送、開示（伝送、流布、または使用可能にすることによる開示を含む）、アライメント、結合、使用、ブロッキング、消去、破壊を含みます。
   1.13. 「**代表者**」とは、プロバイダまたはすべての従業員、役員、代理人、コンサルタント、監査人、下請け業者、委託者、あるいはソリューションの提供に関連してプロバイダを代表するか、またはプロバイダの表見代理権限の下で活動するその他の第三者あるいはそれらすべてを意味します。本契約における「プロバイダ」という言及には代表者も含まれます。
   1.14. 「**下請け業者**」とは、プロバイダのために、またはプロバイダの代理として活動するすべての下請け業者を含む第三者または事業体を意味し、デルまたはプロバイダがデルに対するその契約上の義務を譲渡または委任した先にソリューションを提供します。「下請け業者」にはプロバイダの従業員は含まれません。
   1.15. 「**ソリューション**」とは、プロバイダ契約に従ってデルまたはデルの顧客に提供されるすべてのハードウェア、ソフトウェア（サードパーティ製コンポーネントを含む）、サービスとしてのソフトウェア、サービス、あるいはホスティングサービスを意味します。

1.16. 「**ユーザー追跡データ**」とは、コンテンツ、宣伝またはその他の活動に対する（またはそれとのやり取り）、あるいは行動広告に関連する追跡活動に関連するユーザーの情報、やり取りまたは動作、ユーザークリックあるいは反応を記録するオンラインユーザーまたはモバイルユーザーに関連付けられたデータを意味します。

2. **機密情報。**デルのデータはすべて、（a）NDA、あるいは（b）プロバイダとデルがNDAを締結していない場合はプロバイダ契約に定義されている「機密情報」です。NDAまたはプロバイダ契約における「機密情報」の定義のいかなる除外もデルのデータの定義に適用されないものとします。デルのデータがアーカイブ、バックアップ、またはビジネス継続性/災害対策のシステムに保持されている場合を含め、かかるデルのデータがプロバイダの手元または管理下にある限り、プロバイダはデルのデータを機密情報として取り扱うものとします。

3. **プロバイダの義務**

3.1. 処理。デルはプロバイダに対し、（a）プロバイダ契約、（b）デルまたはその代理人の書面による指示、（c）プライバシー保護法、および（d）本DPA（総称して「**適用される契約**」）に基づき、準拠して、プロバイダのデルに対する義務を遂行することを唯一かつ排他的な目的としてデルのデータの処理を指示し、許可します。プロバイダがユーザーのオンラインまたはモバイルの活動を追跡する場合は、個人データに関連する本DPA記載の義務および要件はユーザー追跡データに及びます。

3.2. 開示および使用に関する制限。プロバイダは、（a）ソリューションの提供に関連して知る必要に応じている場合、（b）ソリューションの提供に必要な範囲おいてである場合、（c）適用される契約により許可されているとおりである場合、または（d）適用法によって求められている場合を除き、デルのデータを転送または開示しない、あるいはその代表者または第三者による処理を許可しないものとします。プロバイダが適用法によってデルのデータの転送、開示、または第三者による処理を許可するよう求められた場合、プロバイダはかかる要件に先立ってデルに速やかに通知し、デルと協力してかかる転送、開示、または処理の規模および範囲を限定します。

3.3. 返却および破壊。プロバイダ契約の終了またはデルからの書面による要求のいずれか早い時点で、プロバイダはその下請け業者によるかかるすべての個人データの使用をすべて中止させ、デルに返却させるか、あるいはデルの指示で処分、破壊、または永続的に匿名性を保持できる状態にし、そのいずれの場合においても本契約に記載されているセキュリティ対策を使用することを保証するものとします。プロバイダによるデルのデータの破壊が適用法で許可されていない場合、プロバイダは適用可能な契約によって求められている以外のいかなる目的についてもデルのデータを使用しないものとし、適用可能な契約の規定に常に拘束され続けるものとします。

3.4. 通知および支援。プロバイダが、ソリューションに関連する個人データに関して要求、照会、または苦情の連絡を個人から受けた場合、プロバイダは速やかに（a）いかなる場合も2暦日以内にかかる要求、照会、または苦情に関する書面による通知をデルに提供し、（b）かかる要求、照会、または苦情に対して速やかに、かつプライバシー保護法が求めるいかなる時間枠内において対応するためにデルが必要とするすべての合理的な協力、支援、情報、プロバイダが所有、保管または管理している個人データへのアクセスを必要に応じてデルに提供するものとします。プロバイダは、デルの書面による指示がない限り、かかる要求、照会、または苦情に対応しないものとします。

4. **国際的な移転。**プロバイダは、デルによる事前の書面による合意を得てEEA諸国からEEA以外の国に個人データを移転することができます。ただし、かかる移転がソリューションに関連して求められている場合、EU標準契約条項に記載されている条件（管理者から処理業者）の対象となり、プロバイダはかかる条項に記載されている「データインポータ」に課せられるすべての義務に準拠します。アジア太平洋地域内の国については、適用される契約で求められている場合を除き、個人データがプロバイダによって当初収集された国から外へ伝送される場合は、プロバイダはデルの書面による合意を事前に得るものとします。

5. **適切な保障措置。**プロバイダは、適切かつ業界基準の物理的、組織的、技術的なプロセス、セキュリティ基準、ガイドライン、管理、および手順（「**ポリシー**」）を有し、保守して、いかなるデータ漏えいからも保護するものとします（「**適切な保障措置**」）。プロバイダは定期的に、かついかなる場合も年に1回以上、適切な保障措置の有効性を評価し、テストし、監視するものとし、かかる結果が合理的に保証されるように適切な保障措置を速やかに調整および更新するものとします。プロバイダは、要求に応じて、適切な保障措置の説明を書面にてデルに提供するものとします。プロバイダは、適切な保障措置の実施、証明、有効性、および改善に関連する文書および報告をデルが利用できるようにするものとします。プロバイダは、プロバイダおよびその下請け業者が以下に示すポリシーを必ず実施して保守することを表明して保証し誓約します。

5.1. リスク管理。組織的および事務的なリスクを年に1回以上評価し、システムおよび技術的なリスクは四半期に1回以上の評価を行います。

5.2. 資産管理。（a）デルのデータの処理に使用するすべての装置およびメディアを特定し、（b）すべての装置およびメディアに対する責任を1人以上の保管者へ割り当て、（c）正確性を期すため、ならびに装置およびメディアの紛失を特定するために資産目録の定期的な見直しを求めます。

5.3. アクセス制御およびアイデンティティ管理に関するポリシー。デルのデータにアクセスする前に、（a）文書化された責務および最小特権の原則に準拠してデータおよびシステムへのすべてのアクセス権を個人に割り当て、（b）すべてのユーザーアカウントおよび管理者アカウントを個人に割り当てて、強力なパスワードを設定し、パスワードを循環させ、失敗した認証をロックし、セッションタイムアウトを行うように求め、（c）特権が付与されたアクセスアカウントの発行には管理者による承認を必要とし、厳格なセキュリティ基準を順守します。

5.4. 認識およびトレーニングに関するポリシー。（a）情報セキュリティの脅威とベストプラクティス、（b）デルのデータを保護するために確立されている情報セキュリティポリシー、手順、および管理、（c）デルのデータの保護における各代表者の役割と責務に取り組みます。

5.5. 説明責任に関するポリシー。（a）すべてのアカウント活動はそのアカウントを使用している個人にまで遡ることができ、（b）すべての特権アカウントの活動およびデルのデータに影響を及ぼすすべてのアカウント活動の時刻、日付、および活動の種類が記録され、（c）記録されたすべてのアカウント活動が積極的に監視され、分析のために簡単に取得でき、（d）ポリシー違反の結果が確立され、伝達され、対処されることを保証します。

5.6. 緊急時対応計画に関するポリシー。（a）洪水、竜巻、地震、台風、氷雨を伴う暴風などの自然の脅威事象、（ii）化学物質の流出および機械的または電気的な障害などの偶発的な脅威事象、ならびに（iii）プライバシーおよびセキュリティの侵害、爆弾の脅威、暴行および窃盗などの故意の行為を含め、不測の事態を適切に処理するための役割および責任を定義し、明確なガイダンスとトレーニングを提供します。

5.7. システム保守に関するポリシー。（a）定期的なスキャン、侵入テスト、リスク分析、時宜にかなったパッチ適用などの構造化された脆弱性管理、（b）目的の文書化、セキュリティに対する影響分析、テスト計画と結果、すべての変更に関する許可などの変更管理、（c）安全な基準構成を含む構成管理、（d）許可されていない変更を検出し、アラートを生成するための監視に関連します。

5.8. システムおよび通信の保護に関するポリシー。（a）デルのデータを処理するシステムへのアクセスを制限し監視する物理的な管理、（b）悪意のあるソフトウェアや悪意のある人物から保護する技術的および運営上の管理、（c）信頼できない公共のネットワークを通じての送信、および機密性が非常に高いデータの場合は、それが保管されているすべての場所にあるときのデータの強力な暗号化、（d）定期的な暗号化キーの循環および管理、（e）機密性が非常に高いデータおよび個人データの実働以外の環境における処理の禁止、（f）定期的なセキュリティ管理の見直しおよび有効性テスト、（vii）リモートアクセスおよびモバイルデバイスに関する強力な技術的および運用上の管理を含む、デルのデータの機密性、完全性および可用性を保持します。

5.9. メディアの保護に関するポリシー。（a）すべてのモバイルデバイスおよびリムーバブルストレージ上でのデルのデータに対する強力な暗号化、（b）デルのデータを適宜保管しているメディアに関する安全なサニタイズおよび破壊方法の要件、および（c）紙を含め、暗号化されていないデルのデータが含まれているすべてのメディアを安全な場所に保管する要件を含めて、デルのデータが含まれているメディアを安全に取り扱うことを保証します。

6. **ペイメントカード情報。**プロバイダ契約に関連してペイメントカード情報を処理する前に、プロバイダはPCIデータ・セキュリティ・スタンダード（「**PCI DSS**」）に準拠し、自らの費用負担で準拠し続ける必要があります。プロバイダは、ペイメントカード情報を処理する前およびその後は年に1回、コンプライアンス/自己評価質問表に関するPCIレポートおよびPCIの四半期に1回のネットワークスキャン報告書においてそれらの情報は最新であり、PCIに準拠し続けていることを言明する証明書とともに、デルの合理的な求めに応じてかかる証明書を裏付ける文書をデルに提出する必要があります。プロバイダが何らかの時点でPCI DSSに準拠していない場合、またはコンプライスに関する十分な証拠を提示できないまたはその意思がない場合、プロバイダはプロバイダ契約に違反しているものとし、デルはデルが責任を負うことなくプロバイダ契約を即時に終了することができます。

7. **インフラストラクチャのセキュリティおよび接続性。**（a）アプリケーション、Webサイト、データ、またはシステムのホスティングがソリューションに含まれている場合、（b）ソリューションの提供にネットワーク接続が必要である場合、または（c）ソリューションがプロバイダの環境の整合性に依存している場合は、次の要件が適用されるものとします。

7.1. ネットワークアクセス。デルのデータをプロバイダとデル間で伝送するための接続およびメカニズムは、デルのI/Tが承認した安全なソリューションを利用して行うものとします。アクセスの期間はアクセスが必要な場合のみに限定されるものとします。プロバイダは適切な保障措置を使用して、侵害、不正アクセス、またはその他の損害からデルのネットワークを保護してソリューションに関連するプロバイダのネットワークおよびI/T環境の安全を確保するものとします。プロバイダは要求に応じてデルに対しソリューションをサポートするプロバイダのI/Tネットワークの概要を示す基本的なネットワークダイアグラムを提供するものとします。

7.2. 監査。プロバイダは要求に応じて、SSAE 16または前年度内に実施した情報セキュリティ監査などのソリューションに該当する管理体制の監査報告書を提供するものとします。監査にはプロバイダの該当する全般的管理体制およびセキュリティプロセスの評価と、プライバシー保護法および業界基準への準拠を保証する手順を含めるものとします。監査はプロバイダの費用負担で、プロバイダが進めているプロバイダの一般的なセキュリティ管理を評価する情報セキュリティプログラムの一環とするものとします。

7.3. テスト。プロバイダの内部的な管理プログラムに加え、プロバイダは本DPAに関連するものとして独立した浸潤テストをその環境で年に1回以上実行し、四半期に1回以上の頻度でセキュリティ脆弱性スキャンを実施します。プロバイダは特定されたすべての脆弱性をリスクに応じ、またはデルとの合意のとおりの時間枠内において修正するよう尽力します。

8. **ソリューションのセキュリティ**

8.1. 脆弱性。プロバイダは、開発中およびリリース後のソリューションにおけるセキュリティの脆弱性を特定するための管理体制を整えるものとします。プロバイダはデルに対し、（a）公に認知されている脆弱性/ゼロデイ攻撃については認知から5営業日以内に、（b）内部的には認識されているものの、まだ公に開示されていない脆弱性/ゼロデイ攻

撃については発見後10営業日以内に書面による通知を提供するものとします。プロバイダは、ソリューションにおいて明確化されたすべての脆弱性をプロバイダの費用負担にて修正し、共通脆弱性評価システムにて定義されている基本評価4以上の脆弱性をリスクに応じ、またはデルとの同意のとおりの時間枠にて修正するよう尽力します。プロバイダによるオープン・ソース・コードの使用によって、本契約書に記載されている脆弱性の特定および修正に対するプロバイダの責任は変更されることはないものとします。

8.2. コーディングプラクティス。プロバイダは、（a）業界のセキュアコーディングのプラクティス（例えば、Microsoftのソフトウェア開発ライフサイクル、CigitalのSoftware Security Touchpoints、OWASPの基準、またはSans Top 25など）を使用し、（b）ソリューションは業界のセキュアコーディングのプラクティスに基づいて設計し、（c）開発ライフサイクル全体を通じて情報セキュリティに対処することに合意します。ソリューションのプロセス、直接的な機能、およびその他の必要な活動は、すべてのPCI基準とプライバシー保護法に準拠するものとします。

8.3. セキュリティ評価。プロバイダは、（a）顧客のシステムに同梱またはインストールされたWebサイトを含み顧客に対応する、または（b）機密性が非常に高いデータを処理するすべてのソリューションについての独立したセキュリティ評価の結果および修正の取り組みを提出するものとします。この評価の範囲および修正の取り組みについては、デルの合意を得た上で、かかるソリューションの受領前にデルが満足するように対処する必要があります。

9. **データ漏えい。**プロバイダは、実際の、または合理的に疑われるデータ漏えいが認識されてから24時間以内にデルに通知するものとします。かかる通知は、少なくともEメールを使用し開封確認メッセージを設定してprivacy@dell.com宛に提供するとともにデル内のプロバイダの主たる営業窓口にコピーを提供する必要があります。データ漏えいの調査および修正を促進するため、プロバイダはデルに全面的に協力するものとします。プロバイダは、デルの書面による同意を最初に得ずにデータ漏えいを第三者に通知しないものとします。ただし、プライバシー保護法により厳しく求められている場合を除きます。この場合、プロバイダは法律により禁止されていない限り、かかる第三者への通知よりも前にデルに通知し、デルと協力してプライバシー保護法で求められている範囲までに情報の開示を制限します。機密性が非常に高い個人データまたはユーザー追跡データの処理に関連し、プロバイダが受け取ったすべての苦情の詳細は、プロバイダのデルの営業窓口に速やかに送信するものとします。プロバイダはデータ漏えいによる損害の対応、修正、または軽減、あるいは個々のデータ主体または規制機関による苦情の追跡によりデルが被ったすべての費用をデルに補償するものとします。プロバイダは、デルおよびプライバシー保護法による指示を含め、データ漏えいを修正または軽減するための必要かつ適切なすべての修正措置を取るものとします。

10. **代表者および下請け業者**

10.1. 制限事項。プロバイダ契約により明示的に許可されていない限り、プロバイダはデルのデータの下請け業者によるまたは下請け業者に対する（a）移転、（b）開示、（c）下請け契約、あるいは（e）処理を許可しないものとします。

10.2. 下請け業者および代表者の要件。プロバイダは、適切な経歴確認の実施を含めて、デルのデータにアクセスできる代表者および下請け業者の信頼性を確保するための合理的なあらゆる措置を講じるものとします。プロバイダは、代表者および下請け業者がプライバシー保護法に基づいてデルのデータを取り扱い、安全に処理するよう、適切な訓練を受けていることを保証するものとします。プロバイダがデルによって下請け業者へのデルのデータの移転を許可されている場合、下請け業者はプロバイダがデルであり、下請け業者がプロバイダであるかのように、本DPAの第4節「国際的な移転」を順守するものとします。

10.3. 下請け契約。プロバイダおよび代表者とデルのデータの処理を承認された下請け業者によるそれらの間での契約（「**下請契約**」）には、本DPAと実質的に同等な制限と条件を含めるものとします。プロバイダは、代表者および下請け業者のすべての行為および不作為に関して単独責任を負うものとします。プロバイダは要求に応じてデルに下請契約書のコピーを提供するものとします。

10.4. 下請け業者の監査。プロバイダはデルのデータを処理するそれぞれの下請け業者を12ヶ月に1回以上監査し、また、データ漏えいが発生した場合はより頻繁に監査するものとします。監査によって下請け業者によるコンプライアンスの不備、違反、または不履行、あるいはそれらすべてが判明した場合は、プロバイダは下請け業者と協力し、それを速やかに修正すべく合理的な努力を払うものとします。デルの公正な裁量の範囲において合理的な期間内に満足のいく修正を行うことができない場合、プロバイダはその下請け業者を使用してソリューションをデルに提供することを許可してはならないものとします。この場合、プロバイダはデルの指示に従い、デルのデータを速やかに返却または削除するよう求められるものとします。

11. **通話録音**。プロバイダが通話の録音を処理する場合、プロバイダは機密性が非常に高いデータまたは個人データが含まれている通話の録音の処理に強力な管理体制を確立するものとします。通話録音へのアクセスおよび通話録音の処理は、ソリューションを提供するために必要な代表者のみに限定するものとし、適用法に準拠するものとします。プロバイダは通話録音に対して行われたすべてのアクセスの記録ログを取るものとします。プロバイダは、録音が目的を果たした後、デルのプライバシーオフィスによる書面による承認がない限り、合理的にできる限り早急に、かつプライバシー保護法および適用されるセキュリティ基準に定められているとおりの期間内であり、いずれの場合も90日（EMEAでは21日）以内に個人データが含まれているすべての通話記録を削除するものとします。プロバイダは通話件数からごく少数のみをプライバシー保護法が求める期間内に録音するものとします。ペイメントカードまたはその他の機密扱いのデータが含まれる録音については、録音の時点ですべてのペイメントカードのデータが録音から削除されるか、判読不能/不可聴な状態にされていない限り、プロバイダはそれらの通話録音を音声ストリーム（かつデータファイルではない）形式で保管するものとします。

12. **カナダのデータ**。プロバイダがソリューションを提供する過程でカナダに所在する個人に関する個人データを処理する場合は、プロバイダおよびデルは本第12節の追加義務と要件に合意します。プロバイダは、適宜修正または補足される個人情報保護および電子文書法（カナダ）あるいはその他の個人データの処理に関するカナダの連邦法または州法にデルが抵触することになる何らかの行動を起こしたり、または何らかの不作為を行わないものとします。プロバイダは、ソリューションに関連して処理した個人データが含まれているすべてのデータ、データベース、またはその他の記録を、プロバイダが自己または第三者のために処理したあらゆる情報、データ、データベース、または記録から論理的に分離し、切り離した状態を維持するものとします。プロバイダは個人データの管理を担当する個人を指名し、デルにその身元を明らかにするものとします。デルは、ソリューションに関連するあらゆる調査、監査、または照会に関連し、事前の通知または同意なく、プロバイダの機密情報を当局に開示するよう求められることがあります。プロバイダは、デルの明示的な同意なく、かつ送信中の個人データを保護するための適切な安全な技術を使用することなく、プロバイダの施設から個人データを移動、削除、または伝送しないものとします。プロバイダがソリューションに関連して個人データに関する要求、照会、または苦情の連絡を個人から受けた場合、プロバイダはかかる個人を速やかにデルに照会するものとします。

13. **DPAの補足契約。**

    13.1. EU標準契約条項。ソリューションを提供する過程で欧州連合に所在する個人に関する個人データをプロバイダが処理する場合、プロバイダおよびデルは本契約によって、本契約書に添付する付属書1および2を含めたEU標準契約条項に合意し、プロバイダはそれらを順守するものとします。

    13.2. HIPAAコンプライアンス。プロバイダがソリューションを提供する過程でDell Inc.の包括的福利厚生制度の加盟者の45 C.F.R. § 164.501に定義されている「保護すべき健康情報」にアクセスする、保持する、開示された状態で表示する、または知り得るようになる場合、プロバイダおよびデルは本契約によって、HIPPA米国下請契約およびHIPAA提携事業者契約に合意し、プロバイダはそれらを順守するものとします。

    13.3. 権限。**プロバイダはデルに対し、プロバイダの代わりとして本DPAを承認するプロバイダのすべての代表者を含め、プロバイダは付属書1および付属書2を含めたEU標準契約条項、HIPAA下請契約、および提携事業者契約にプロバイダが拘束される権限が与えられることを表明し、誓約します。**

14. **デルの副次的権利**。本DPAのいかなる内容も本DPAの当事者以外の個人または事業体のいかなる利益も権利も授与しないものとします。ソリューションにデルの直接子会社および間接子会社の代理としてプロバイダの職員によるデルのデータの処理が含まれている場合、デルのデータに関してかかるデルの直接子会社または間接子会社はそれぞれ本DPAまたはプロバイダ契約がある場合はその契約、あるいはそれらのすべての当事者であるかのように、本DPAの条件を第三受益者としてプロバイダに対して適用することができます。

15. **監査**。プロバイダはデルまたはその被指名人が（a）本DPAをプロバイダが順守しているかを監査すること、（b）プロバイダが保管しているまたは保持している個人データを検査すること、および（c）個人データのプロバイダによる取り扱いに関するデルからのすべての問い合わせに速やかに対応することを許可するものとします。

16. **免責。**プロバイダは、デルならびにデルの取締役、役員、従業員、代表者、および代理人を（a）プロバイダによる本DPAへの違反、（b）プロバイダによるPCI DSSの不履行、または（c）プロバイダによる何らかのプライバシー保護法に対する違反に起因または関連して生じたすべての請求、訴訟、要求、法的手続きおよび責任、損害賠償、損害、判決、和解、費用、罰金、違約金、ならびに妥当な弁護士報酬を含む費用に対して弁護し、補償し、損害を与えないものとします。

17. **その他。**本DPAに基づくプロバイダの義務は、DPA、NDA、およびプロバイダ契約の終了または満了しても効力を有するものとします。法的通知は、プロバイダ契約書に記載されている通知先住所宛に書面にて行うものとします。ファクシミリ、翌日配達便、書留郵便または配達証明付き郵便によって行われ、デルの通知先住所またはプロバイダの通知先住所（あるいは他方の当事者に速やかに通知されている後継者および住所）に送信された書面による通知は、送付した時点で効力が生じるものと見なされます。本DPAで求められているかまたは許可されている、あるいは本DPAにかかわるプロバイダとデル間でのその他すべての書面による通信、配信、または業務上の通知は、受け取った時点で効力が生じるものとします。プロバイダは、本DPAの全部または一部を、デルの事前の書面による同意なく、自発的か、あるいは契約または合併（当該当事者が存続会社か消滅会社かにかかわらず）、株式または資産の売却、整理統合、解散、政府の措置または命令、あるいはその他の理由によるかにかかわらず、譲渡または移転することはできません。本節に準拠せずに本DPAを譲渡または移転しようとする試みはすべて無効となります。デルはプロバイダの合意なく本DPAを譲渡することができます。条件の放棄は、両当事者の権限を有する代表者によって署名された書面でない限り有効とはならず、さらに、その対象となる個別の状況に限定されるものとします。本DPAに対する修正または変更は、本DPAを具体的に参照する書面に記載され、両当事者の権限を有する代表者が署名しない限り有効とはならないものとします。その他すべての行為または不作為はすべての権利の放棄となるものとします。本DPAは契約全体および本契約の対象に関連する両当事者の理解を表明するものであり、口頭および書面にかかわらず、これよりも前または同時に行ったすべての討議および合意に取って代わります。本DPAに準じたプロバイダによる責務の履行においては、プロバイダは常に独立請負人として行動し、プロバイダはパートナー、ジョイントベンチャー、またはデルの従業員でないことを理解し、同意します。プロバイダは、いかなる目的についても、デルの代理人、表見代理人または見掛けの代理人、あるいは従業員とは見なされないことに明示的に合意し、両当事者はデルが合理的に求めるように、プロフェッショナルサービスを利用して一般およびその他にかかる事実を通知するためのすべての措置を講じることに合意します。それぞれの当事者はここに、相手側当事者から適宜求められる文書を作成し、本DPA、プライバシー保護法、または適用法に従ってかかる当事者の義務を実行または履行することに同意します。両当事者は、プライバシー保護法および適用法を順守するためにデルが必要とする本DPAの適宜の修正に

必要とされる合理的な措置を講じることに合意します。解釈。本DPAの曖昧性は、プライバシー保護法および適用法をデルが順守できる意味となるように解釈されます。

EU標準契約条項

これらの条項は、デルとプロバイダ間のデータ保護契約（「**DPA**」）に付属し、その一部となります。

EU標準契約条項を目的とした場合、データエクスポート組織の名称はアイルランドの法律に基づいて組織された登録番号191034の無限責任会社であるDell Productsであり、その他すべてのデルグループの事業体（下記に定義）とともに70 Sir John Rogerson’s Quay, Dublin 2, Irelandに事務所が登記されています。デルのかかる各事業体には、デルのかかる事業体が独自に別途一連の標準契約条項をデータインポータと締結したかのように、かかるデルの事業体が管理者として処理する個人データに関しデータインポータに対する第三受益者として、これらの標準契約条項を施行する権利を有します。

デルグループ事業体とは常時管理する、またはDell Productsによって管理される、あるいはDell Productsとの共同管理の下に管理されている当事者またはあらゆる事業体を意味します。「**管理**」とは、企業に関しては、直接的または間接的にその企業の業務が当該者の希望または指示に従って実行されることを保証する当該者の権能のことを意味します。「管理する」、「により管理される」、または「共通管理の下」は、相応に解釈されるものとします。

1) ***第1条*定義。**本条項の目的については以下のとおりとします。

   a) **「個人データ」、「データの特殊カテゴリ」、「処理」、「管理者」、「処理者」、「データ主体」、および「監督当局」**は、個人データの処理に関する個人の保護およびかかるデータの自由移動に関する1995年10月24日の欧州議会および理事会の指令95/46/ECと同一の意味を有するものとします。

   b) **「データエクスポータ」**とは、個人データを転送する管理者を意味するものとします。

   c) **「データインポータ」**とは、データエクスポータからその代理として、データエクスポータの指示およびこれらの条項に従って転送後に処理を行うための個人データを受け取ることに合意し、指令95/46/ECの25（1）条の意味の範囲内で十分な保護を確保する第三国のシステムの対象ではない処理者を意味するものとします。

   d) **「下請け処理業者」**とは、データインポータまたはデータインポータのその他のすべての下請け処理業に従事し、データエクスポータの指示、本条項の条件、および書面による下請けの条件に準拠してデータインポータからまたはデータインポータのその他の下請け処理業者から、データエクスポータの代理として処理活動を専門的に行うことに合意した処理業者を意味します。

   e) **「適用されるデータ保護法」**とは、個人の基本的権利および自由、特に、データエクスポータが設立されている加盟国においてデータ収集者に適用される個人データの処理に関するプライバシーへの権利を保護する法律を意味します。

   f) **「技術的および組織的なセキュリティ対策」**とは、個人データを、特にネットワークを介したデータの伝送が処理に含まれる場合に偶発的なまたは違法な破壊、あるいは偶発的な損失、変更、不正な開示またはアクセス、ならびにその他の違法な処理形態から保護することを目的とした対策を意味します。

2) ***第2条*移転の詳細。**移転の詳細、ならびに該当する場合は特に個人データの特殊カテゴリは、本諸条項の不可欠な部分を形成する付属書1に定められています。

3) ***第3条*第三受益者条項**

   1. データ主体はデータエクスポータに対して本条、第4条（b）～（i）、第5条（a）～（e）および（g）～（j）、第6条（1）および（2）、第7条、第8条（2）、第9～12条を第三受益者として適用できます。

   2. データ主体は、データエクスポータが事実上行方不明となっている、または法律上消滅している場合、後継の事業体が契約または法の作用によりデータエクスポータの法的義務全体を負い、その結果、データエクスポータの権利と義務を引き受け、データ主体がそれらの権利および義務をかかる事業体に適用できない場合を除き、データインポータに本条、第5条（a）～（e）および（g）、第6条、第7条、第8条（2）、および第9～12条を適用することができます。

   3. データ主体は、データエクスポータおよびデータインポータの両方が事実上行方不明となっている、または法律上消滅している、あるいは破産している場合、後継の事業体が契約または法の作用によりデータエクスポータの法的義務全体を負い、その結果データエクスポータの権利と義務を引き受け、データ主体がそれらの権利および義務をかかる事業体に適用できない限り、下請け処理業者に本条、第5条（a）～（e）および（g）、第6条、第7条、第8条（2）、および第9～12条を適用できます。下請け処理業者のかかる第三者賠償責任は、本諸条項に基づく自己の処理作業に限定されるものとします。

   4. データ主体がその旨を明示的に希望し、かつ国内法令によって許可されている場合、両当事者は業務提携者またはその他の団体によって代表されているデータ主体に意義を唱えません。

4) ***第4条*データエクスポータの義務。**データエクスポータは以下に合意し、保証します。

   a) 個人データ自体の移転を含む処理が関連する（該当する場合は、データエクスポータが設立されている加盟国の関連当局に通知されている場所の）適用可能なデータ保護法の関連規定に準拠して実行されており、今後も実行され、以下に記載する関連規定に違反していないこと。

b) データエクスポータの代理としてのみ、さらに適用されるデータ保護法および本書条項を順守してのみ、転送される個人データを処理するようにデータインポータに指示しており、個人データの処理サービスの機関全体を通じて指示すること。

c) データインポータはこれらの条項の付属書2に定められている技術的および組織的なセキュリティ対策に関する十分な保証を提供すること。

d) 適用されるデータ保護法の要件の評価後、セキュリティ対策が、特に、処理にネットワークを介したデータの伝送が含まれている場合は偶発的または違法な破壊または偶発的な損失、変更、不正な開示またはアクセスから、ならびにその他の違法なすべての処理形態から個人データを保護するために適切であること、さらに、それらの対策の実施の最先端性とコストを考慮し、処理によって生じるリスクおよび保護されるデータの特性に適切なセキュリティのレベルがそれらの対策によって確保されること。

e) セキュリティ対策を順守することを保証すること。

f) 移転に特殊なカテゴリのデータが含まれている場合、そのデータが指令95/46/ECの意味の範囲内の十分な保護を提供しない第三国に伝送される可能性があることをデータ主体にその移動の前に通知されているか、または移動後のできる限り早い時点で通知されること。

g) データエクスポータが移転を継続するまたは活動の一時停止を解除することを決定した場合、第5条（b）および第8条（3）に従ってデータインポータまたは下請け処理業者から受け取った通知をデータ保護監督当局に転送すること。

h) 本諸条項または契約に商用情報が含まれておらず、かかる商用情報を削除できない限り、付属書2を除き本諸条項のコピーおよびセキュリティ対策の概要説明とともに本諸条項に従って実行する必要がある再処理委託サービスの契約のコピーを、要求に応じて、データ主体が利用できるようにすること。

i) 処理再委託が発生した場合、処理活動は第11条に従い、個人データに対して最低でも本諸条項に基づくデータインポータと同レベルの保護とデータ主体の権利を提供する下請け処理業者によって処理活動が実行されること。

j) 第4条（a）～（i）を順守することを保証すること。

5) ***第5条データインポータの義務。***データインポータは以下に合意し、保証します。

a) データエクスポータの代理としてのみ、さらにデータエクスポータの指示および本諸条項を順守してのみ、個人データを処理します。いかなる理由によってもかかるコンプライアンスを実現できない場合は、データエクスポータに順守できないことを速やかに通知し、その場合にはデータの移転を停止させること、または契約を終了すること、あるいはその両方を行う権利がデータエクスポータにあることに合意します。

b) データインポータに適用される法律がデータエクスポータから受ける指示や本契約による義務の遂行を妨げていると信じるに足る根拠なく、法令に変更が生じ、本諸条項によって定めた保証および義務に大幅な悪影響が及ぶ可能性がある場合はそれを認識した時点で、できる限り早急にその変更をデータエクスポータに通知します。この場合、データの転送を停止させることまたは契約を終了すること、あるいはその両方を行う権利はデータエクスポータが有します。

c) 移転された個人データを処理する前に付属書2に定めた技術的および組織的なセキュリティ対策を実施します。

d) 以下に関してデータエクスポータに速やかに通知します。

i) 警察当局による調査の機密性を保持するために刑法で禁止されているなど別途に禁止されている場合を除き、警察当局による個人データの法的拘束力のあるすべての開示要求。

ii) 偶発的または不正なアクセス。ならびに

iii) 要求に対応せずに受け取ることを許可されていない場合を除き、要求に対応せずにデータ主体から直接受け取った要求。

e) 移転対象の個人データの処理に関連し、移転されたデータの処理に関する監督当局の助言に従い、データエクスポータからのすべての問い合わせに迅速かつ正確に対応すること。

f) 監督当局との合意により、該当する場合は、データエクスポータの要求に応じてデータエクスポータまたは独立したメンバーで構成され、守秘義務に拘束され、必要な専門的資格を有し、データエクスポータによって選択された検査団体が実行すべき本条項の対象となっている処理活動の監査を行うデータ処理設備を提示すること。

g) 要求に応じて、本条項または契約に商業情報が含まれている場合を除き、本条項のコピー、または下請け処理に関する既存の契約のコピーをデータ主体が利用できるようにすること。本条項または契約に商業情報が含まれている場合は、データ主体がデータエクスポータからコピーを取得できない場合のセキュリティ対策に関する概要説明で置き換える付属書2の例外により、かかる商業情報を削除することができます。

h) 下請け処理の場合は、その旨をデータエクスポータに通知しており、書面による事前合意を取得していること。

i) 下請け処理業者による処理サービスが第11条（下請け処理）に従って行われること。

j) 本諸条項に基づいて締結したすべての下請け処理契約書のコピーをデータエクスポータに速やかに送付すること。

6) ***第6条*責任**

1. 両当事者は、第3条または第11条で言及する義務に違反した結果として、いずれかの当事者または下請け処理業者により損害を被ったデータ主体には、被った損害に対する損害賠償をデータエクスポータから受ける権利があることに合意します。

2. データエクスポータが事実上行方不明となっているまたは法的に消滅している、あるいは破産しているためにデータ主体がデータエクスポータに対して第1項に従いデータインポータまたはその下請け処理業者による第3条または第11条に言及されているいずれかの義務の違反から生じた補償に関する訴訟を起こすことができない場合、データインポータは、後継の事業体が契約または法の作用によりデータエクスポータの法的義務全体を負い、データ主体がその権利をかかる事業体に適用できる場合を除き、データ主体がデータエクスポータであるかのようにデータインポータに対して申し立てを行うことができます。

   データインポータは、自己の責任を回避するために下請け処理業者によるその義務違反に依存することはできません。

3. データ主体が第1項および第2項で言及されているデータエクスポータまたはデータインポータに対して、データエクスポータおよびデータインポータの両方が事実上行方不明になっているか、または法的に消滅している、あるいは破産しているために第3条または第11条で言及されているそれらのいずれかの義務の下請け処理業者による不履行に起因する訴訟を起こすことができない場合、下請け処理業者は、本条項に基づく自身の処理作業に関連する訴訟をデータ主体がデータエクスポータまたはデータインポータであるかのようにデータ主体がデータ下請け処理業者に対して起こせることに合意します。ただし、後継事業体がデータエクスポータまたはデータインポータの法的義務全体を契約または法の作用により負う場合を除きます。その場合、データ主体はその権利をかかる事業体に対して適用できます。下請け処理業者の責任は、本諸条項に基づく自己の処理作業に限定されるものとします。

7) ***第7条*救済および管轄区**

1. データインポータは、データ主体が本諸条項による第三受益者の権利を行使した、または損害賠償を要求した、あるいはその両方を行った場合はデータインポータがデータ主体の以下の意思決定を受け入れることに合意します。

   a. 独立性を持った人物、または該当する場合は監督当局による救済に紛争を付すこと。

   b. データエクスポータが設立されている加盟国の裁判所に紛争を付すこと。

2. 両当事者は、データ主体が行った選択を国内法令または国際法令のその他の規定に準拠して救済を求めるための実質的権利または手続き上の権利を害することがないことに合意します。

8) ***第8条*監督当局との協力**

1. 本契約のコピーを預けるように監督当局に求められた場合、あるいは適用されるデータ保護法の下でかかる預け入れが求められている場合、データエクスポータは本契約のコピーを監督当局に預けることに合意します。

2. 両当事者は、適用されるデータ保護法によるデータエクスポータの監査に適用されるものと同じ条件の範囲で、対象となるデータインポータおよび下請け処理業者の監査を行う権利が監督当局にあることに合意します。

3. データインポータは、データインポータまたはすべての下請け処理業者に適用される、第2項によるデータインポータまたはすべての下請け処理業者の監査の実施を阻害する法律の存在についてデータエクスポータに速やかに通知するものとします。かかる場合においては、第5（b）条において予見される対策を取る権利はデータエクスポータにあるものとします。

9) ***第9条*準拠法。**本諸条項は、データエクスポータが設立されている加盟国の法律に準拠するものとします。

10) ***第10条*契約の変更。**両当事者は本諸条項を変更または修正しません。これは、本諸条項に反していない限り、業務関連の問題に関する条項を両当事者が必要に応じて追加することを妨げるものではありません。

11) ***第11条*下請け処理**

1. データインポータは、データエクスポータの書面による事前の合意なく、本諸条項に基づいたデータエクスポータの代理として行ういずれの処理作業も下請けに出すことはできないものとします。データインポータが本諸条項による義務をデータエクスポータの同意を得て下請けに出す場合、そのデータインポータは本諸条項によりデータインポータに課せられるものと同じ下請け処理業者の義務を課す下請け処理業者との書面による合意によってのみ行うものとします。下請け処理業者がかかる書面による合意に基づくデータ保護の義務の履行を怠った場合、データインポータはかかる合意に基づく下請け処理業者の義務の履行についてデータエクスポータに対して責任を負い続けるものとします。

2. データ主体が第6条の第1項に言及されている補償に関する訴訟をデータエクスポータまたはデータインポータが事実上行方不明になっているか法的に消滅している、あるいは破産しており、契約または法の作用によって課せられるデータエクスポータまたはデータインポータの法的義務全体を負う後継の事業体が存在しないため、データエクスポータまたはデータインポータに対して訴訟を起こすことができない場合、データインポータと下請け処理業者間の事前の書面による契約は第3条に定める第三受益者条項も規定するものとします。下請け処理業者のかかる第三者賠償責任は、本諸条項に基づく自己の処理作業に限定されるものとします。

3. 第1項で言及した契約の下請け処理業者のデータ保護の見地に関連する規定は、データエクスポータが設立されている加盟国の法律に準拠するものとします。

4. データエクスポータは本諸条項に基づいて締結され、第5（j）条に従ってデータインポータにより通知された下請け処理契約のリストを保管するものとし、少なくとも年に1回は更新するものとします。このリストは、データエクスポータのデータ保護監督当局が利用できるようにするものとします。

12) ***第12条*個人データ処理サービス終了後の義務**

1. 両当事者は、データ処理サービスの提供の終了をもって、データインポータおよび下請け処理者は、データエクスポータの選択により、データエクスポータに移転されたすべての個人データまたはそれらのコピーを返却する、あるいは、すべての個人データを破壊するものとし、移転された個人データの全部または一部をデータインポータに課せられた法律により返却または破壊できない場合を除いて、そのようにしたことをデータエクスポータに証明するものとします。その場合、データインポータは移転された個人データの機密性を保証し、移転された個人データをその後は積極的に処理しないこと保証します。

2. データインポータおよび下請け処理業者は、データエクスポータまたは監督当局あるいはその両方の要求に応じて、第1項に言及されている対策の監査のためにデータ処理設備を提示することを保証します。

標準契約条項付属書類1

これらの条項は、デルとプロバイダ間のデータ保護契約（「**DPA**」）に付属し、その一部となります。本付属書類は本諸条項の一部となります。加盟国は、それらの国の手続きに従って必要な追加情報を本付属書に記入または指定することができます。

データエクスポータ。データエクスポータは本諸条項の先頭で特定され、IT製品およびサービスのプロバイダです。データエクスポータはプロバイダ契約に指定されている特定の製品またはサービスあるいはその両方を提供するデータインポータを指名しています。これらの製品およびサービスの提供を促進するため、データエクスポータはデータインポータに下記に説明する個人データへのアクセスを提供することができます。

データインポータ。データインポータは本諸条項の署名者であり、製品またはサービスあるいはその両方のプロバイダです。データインポータは、下記に説明するように、データインポータに対してデータエクスポータがエクスポートした個人データの受領者となります。

データ主体。移転された個人データは次のカテゴリのデータ主体に関連することがあります。

- 過去および現在の従業員、採用候補者、ならびにパートナー、
- 過去および現在のクライアントならびに見込み客、
- 過去および現在、ならびに候補となっている顧問、コンサルタント、サプライヤ、請負業者、下請け業者、および代理人、
- 苦情申し立て者、投書者、および照会者
- 受益者、親、保護者

データのカテゴリ。データ主体の移転済みの個人データは以下のデータのカテゴリに関する場合があります。

1. 契約の詳細（名前、住所、Eメールアドレス、電話およびファックス連絡先の詳細、関連する地域のタイムゾーン情報などが含まれる場合があります）、
2. 雇用の詳細（会社名、役職、評価、人口統計学上および場所のデータが含まれる場合があります）、
3. ITシステム情報（ユーザーIDおよびパスワード、コンピュータ名、ドメイン名、IPアドレス、ならびにソフトウェア使用パターン追跡情報（cookie）が含まれる場合があります）、
4. 情報テクノロジーのコンサルティング、サポート、およびサービスの提供の際に偶発的に取得可能なデータ主体のEメールの内容および送信日（偶発的なアクセスには、Eメールの送信、ルーティングおよび配信に関連するEメール通信およびデータの内容へのアクセスが含まれる場合があります）、
5. データ主体に対して、またはデータ主体のために提供された物品またはサービスの詳細、
6. 財務上の詳細（貸方、支払い、および銀行に関する詳細情報など）。

データの特殊なカテゴリ（該当する場合）。人種または民族、政治的見解、宗教的または哲学的な信念、労働組合に関する見解、メンバーシップおよび活動、社会保障の記録、健康に関するデータ（身体または精神上の健康および状態を含む）、性生活および犯罪行為または申し立てられている犯罪および関連する訴訟手続きに関する情報を開示し、指令95/46/ECの第8条項に定義されている特殊なカテゴリのデータが含まれる個人データ。

処理作業。移転された個人データは、使用された手段および手順にかかわりなく、特に、データの取得、収集、記録、体系化、保管、保持、使用、修正、改作、変更、開示、流布、あるいは取得可能にすること、調整、結合、検索、コンサルティング、アーカイビング、伝送、ブロッキング、消去または破壊、システムの運用およびメンテナンス、管理および管理報告、財務報告、リスク管理、コンプライアンス、法律上および監査の機能、個人情報に関するすべての操作の処理活動の対象となる場合があり、指令の当該条件に定められた意味を有する「処理」を含むものとします。

標準契約条項付属書2
データインポータの情報セキュリティに関する概要

これらの条項は、デルとプロバイダ間のデータ保護契約（「**DPA**」）に付属し、その一部となります。本付属書2では、第4条（d）および第5条（c）に準拠してデータインポータが実施する技術的および組織的な対策を詳しく説明します。データインポータは情報セキュリティを真摯に受け止め、個人データの処理および移動においてこのアプローチに従います。この情報セキュリティの概要は、データインポータのグループ各社間で処理および移転される個人データを保護するためのデータインポータの企業管理体制に適用されます。データインポータの情報セキュリティプログラムにより全従業員が自分たちの責務を理解できるようになります。顧客のソリューションによっては、それぞれの顧客が合意した適用可能な作業範囲記述書に代替の保障措置が概説されている場合があります。

セキュリティ対策。データインポータは、データインポータの企業環境を保護し、（1）情報セキュリティ、（2）システムおよび資産管理、（3）開発、ならびに（4）ガバナンスのすべての分野にわたり事業目標に取り組むように設計された企業情報のセキュリティ対策および基準を実施しています。これらの対策および基準はデータインポータの経営管理者によって承認されており、定期的な見直しおよび必要に応じた更新が行われます。データインポータは、物理的および論理的なアクセス制限、データ分類、アクセス権、資格認定プログラム、記録の保持、データプライバシー、情報セキュリティ、ならびに個人データおよび機密扱いの個人データのライフサイクルにわたる処理に関するポリシーおよび手順を含む適切なデータプライバシーおよび情報セキュリティのプログラムを保守するものとします。重要なポリシーについては少なくとも年に1回は見直す必要があります。

組織的セキュリティ。これらの対策および基準の順守は、データインポータの組織全体にわたり個人の責任です。これらの対策および基準への企業としての順守を促進するために、データインポータの情報セキュリティ（「**IS**」）機能が以下の活動の責任を担います。

1. **セキュリティ戦略** - IS機能がデータインポータのセキュリティの方向付けを行います。IS機能は、セキュリティ関連のポリシー、基準、および規則の順守を保証し、認識を高め、ユーザーに教育を提供するよう取り組みます。また、IS機能はリスク評価とリスク管理の活動を実行し、契約のセキュリティ要件を管理します。
2. **セキュリティエンジニアリング** - IS機能は、セキュリティソリューションのテスト、設計、および実施を管理し、環境全体にわたってセキュリティ体制を採用できるようにします。
3. **セキュリティ活動** - IS機能は、実装したセキュリティソリューションのサポートを管理し、環境と資産を監視およびスキャンし、インシデント対応を管理します。
4. **科学調査** - IS機能はセキュリティ活動、法務、グローバル・プライバシー・オフィス、および人事部門と協力し、eDiscoveryおよびeForensicsを含めて調査を実施します。
5. **セキュリティコンサルティングおよびテスト** - IS機能はセキュリティのベストプラクティスの開発においてソフトウェア開発者と協力し、ソフトウェアプロジェクトのためのアプリケーション開発およびアーキテクチャについてのコンサルティングを行い、確認テストを実施します。

資産の分類および管理。データインポータの対策は、重要な情報ならびに物的資産、ソフトウェア資産、および論理的資産を追跡および管理することです。データインポータが追跡する可能性のある資産の例には以下が含まれます。

- 特定済みのデータベース、災害対策計画、ビジネス継続性計画、データ分類、アーカイブ済みの情報などの情報資産
- 特定済みのアプリケーションおよびシステムソフトウェアなどのソフトウェア資産
- 特定済みのサーバ、デスクトップ/ノートパソコン、バックアップ/アーカイバルテープ、プリンタ、および通信機器などの物的資産

これらの資産は機密性の要件を決定するビジネス重大度に基づいて分類されます。個人データの処理に関する業界のガイドラインは、技術的、組織的、および物理的な保障措置を規定します。これらの保障措置には、アクセス管理、暗号化、ロギングおよびモニタリング、ならびにデータの破壊などの管理体制が含まれる場合があります。

従業員のスクリーニング、トレーニング、およびセキュリティ

1. **スクリーニング/経歴調査:** 実行性および適切性が合理的である場合、従業員がデータインポータのネットワーク、システムまたは設備へのアクセス権を有するようになる場合には、雇用/採用過程の一部として、データインポータは従業員に関するスクリーニング/経歴調査（現地法および規則に基づいて国によって異なる）を実行するものします。
2. **身元確認:** データインポータはすべての従業員に身元を確認するための証拠、ならびに雇用した国により必要とされる可能性があるかあるいは従業員がサービスを提供する他のデータインポータまたは顧客が求める場合は追加の書類を提供するよう求めるものとします。

3. **トレーニング:** データインポータの年次コンプライアンス・トレーニング・プログラムには、データ保護および情報セキュリティを認識させるためのコースを修了し、コースの最後に行う評価に合格することを従業員に求めることを含めます。また、セキュリティを認識させるためのコースでは、特定の職務権限に固有の教材を提供することもできます。

4. **機密性:** データインポータは標準的な合意に準拠してその従業員が処理する個人データの機密性を保護し、保守することにその従業員が法律的に拘束されることを保証するものとします。

物理的なアクセス制御および環境セキュリティ

1. **物理的なセキュリティプログラム:** データインポータは物理的なセキュリティプログラムに多くの技術的および組織的なアプローチを利用して、合理的に実行可能な範囲においてセキュリティリスクを軽減するものとします。データインポータのセキュリティチームは各現場と密接に協力し、個人データが処理されるシステムへのアクセス権を未承認の人物が取得することを防止する適切な対策が取られているかどうかを判断し、物理インフラストラクチャ、ビジネスへのすべての変更および既知の脅威を継続的に監視します。また、業界他社が使用しているベストプラクティスの対策を監視し、データインポータのビジネスプラクティスの独自性と期待の両方に見合うアプローチを慎重に選択します。データインポータは、アーキテクチャ、運用、およびシステムを含む管理要素を考慮することによってセキュリティに対するアプローチのバランスを取ります。

2. **物理的アクセスの管理体制:** データインポータの設備/施設での物理的なアクセス制御/セキュリティの対策は、次の要件を満たすように考案されます。

   (a) データインポータの建物、設備、その他の物理的な施設へのアクセスは、ビジネスの必要性、資産の機密性、ならびに個人の役割およびデータインポータに対する関係に基づいて管理されるものとします。データインポータと関係のある職員のみに、データインポータの設備および物的資源へのアクセスを組織内のその役割および責任に合致する方法で提供します。

   (b) 関連するデータインポータの設備はアクセス制御システムによって保護されます。かかる設備へのアクセス権はアクティブ化されたカードのみで付与されます。

   (c) 設備または資源あるいはその両方へのアクセスが必要なすべての人物にはIS機能によって適切かつ固有の物理的アクセスクレデンシャル（その個人に割り当てられたバッジまたはキーカードなど）が支給されます。固有の物理的なアクセスクレデンシャルが支給された個人は、他の個人の個人固有のクレデンシャルを使用したデータインポータの設備または資源へのアクセスは許可されない、またはできないことが指示されます。（i）特定の設備へアクセスするため、および（ii）正当なビジネスニーズのために必要な場合、アクティブなIDを持たない個人に一時的（最大14日）なクレデンシャルを支給することができます。固有のクレデンシャルは譲渡不能であるため、要求に応じて個人が自分のクレデンシャルを提示できない場合、それらの個人はデータインポータの設備に立ち入ることを拒否されるか、または構内から連れ出される場合があります。人員が配置されている入り口で、個人は有効な写真付きのIDか、または有効なクレデンシャルを入館時にセキュリティ担当者に提示する必要があります。自分のクレデンシャルまたはその他のIDを紛失したかまたは置き忘れた個人は、職員が配置されている入り口から入館し、セキュリティ担当者から一時的なバッチを支給してもらう必要があります。

   (d) 従業員は定期的にトレーニングを受け、常にクレデンシャルを携帯し、ノートパソコン、ポータブルデバイス、および（特に移動中は）書類を安全な場所に保管し、デスクを離れる際にはコンピュータからログアウトするかまたはコンピュータをシャットダウンするように注意喚起されます。

   (e) データインポータの設備への出入りが必要な訪問者は職員が配置されているか、または設備の正面玄関から入館する必要があります。訪問者は建物への到着日時、退出時刻、および訪問する人物の氏名を登録する必要があります。訪問者は現行の政府が発行した形式のIDを提示し、自分の身元の正当性を立証する必要があります。企業固有の情報へのアクセスまたは開示を防ぐため、訪問者は立ち入り禁止区域または管理区域に付き添いなしに立ち入ることはできません。

   (f) 限定されたデータインポータの設備はCCTVモニタリング、セキュリティガード、およびその他の物理的な対策を適切かつ法的に認められている場合は利用します。

   (g) ほとんどの現場には鍵付きのシュレッダーが備わっており、秘密情報/個人データを安全に破壊することができます。

   (h) データインポータの主要なデータセンターでは、セキュリティガード、UPSおよび発電機、ならびに変更管理の基準を利用できます。

   (i) ソフトウェア開発およびインフラストラクチャ配備プロジェクトの場合、IS機能はリスク評価プロセスおよびデータ分類プログラムを使用してかかる活動から生じるリスクを管理します。

変更管理。IT組織は、企業のインフラストラクチャ、システム、およびアプリケーションを集中管理された変更管理システムを通じて管理します。これには、必要に応じてテスト、ビジネスインパクト分析、経営管理者による承認が含まれる場合があります。すべての関連するアプリケーションおよびシステムの開発は、承認された変更管理プロセスを順守します。

セキュリティインシデントおよび対応計画

1. **セキュリティインシデントおよび対応計画:** データインポータは個人データの制御不能、窃盗、不正開示、不正アクセス、または不正取得が発生した場合にデータインポータが講じる対策に取り組むセキュリティインシデント対応ポリシーならびに関連する計画および手順を保守します。これらの対策にはインシデント分析、抑制、報告、および通常運用への復帰を含めることができます。

2. **対応管理体制:** 資産を悪意のある利用および悪意のあるソフトウェアから保護し、それらの検出をサポートし、適切な措置を取れるよう、データインポータのIS機能またはサービスデスクに潜在的なインシデントを報告するために管理体制を整えます。管理体制には、情報セキュリティポリシーおよび基準、アクセスの制限、開発環境およびテスト環境の指定、サーバ、デスクトップ、およびノートパソコン上でのウイルス検出、ウイルスが添付されたEメールのスキャン、システム・コンプライアンス・スキャン、侵入防御モニタリングおよび対応、ファイアウォールルール、重大イベントのログおよびアラート、データタイプに基づく情報処理手順、Eコマースアプリケーションおよびネットワークのセキュリティ、システムおよびアプリケーションの脆弱性スキャンが含まれる場合がありますが、これらに限定されません。その他の管理体制もリスクに基づいて実施することができます。

データの伝送制御および暗号化。データインポータは、個人データの電子的伝送または移転に対するその管理が及ぶ範囲において、個人データの伝送または移転の間に適切な権限なくかかる伝送または移転の読み取り、コピー、改変、または削除ができないことを保証するためのあらゆる合理的な処置を講じるものとします。特に、データインポータは以下を行うものとします。

1. 個人データの伝送に業界基準の暗号化プラクティスの実施。データインポータが使用する業界基準の暗号化方式には、Secure Sockets Layer（SSL）、Transport Layer Security（TLS）、SSHなどのセキュア・シェル・プログラム、またはInternet Protocol Security（IPSec）などがあります。

2. 技術的に実現可能な場合、すべての個人データ、特に、すべての機密扱いの個人データまたは機密情報を公衆ネットワーク、あるいはデータインポータが所有または保守していないあらゆるネットワークを通じて伝送または転送する際の当該すべてのデータの暗号化。データインポータのポリシーで、承認されていない個人が暗号化キーにアクセスできない場合を除けば暗号化は無効であることを認め、暗号化された文書と同じチャネルを通じて暗号化キーを提供することがないよう指示します。

3. 機密扱いの個人データを処理する、またはかかる情報が含まれているネットワーク上（データインポータのコアネットワークを含む）のシステムとのリアルタイム統合を実行する可能性があるインターネットに接続するアプリケーションの場合は、Web Application Firewall（WAF）を使用して入力チェックおよび攻撃軽減の追加レイヤを提供することができます。WAFは、インジェクション攻撃、バッファーオーバーフロー、Cookie操作、およびその他の一般的な攻撃方法など、潜在的な脆弱性を軽減するように設定されます。

システムのアクセス制御。データインポータのシステムに対するアクセスは承認されているユーザーに限定します。承認されていない個人からのアクセスを防止するように適切な承認が付与されることを保証するように考案された正式な手順に基づいてアクセス権が付与されます。かかる手順には以下が含まれます。

1. **受付制御**（つまり、承認されていない個人によるデータ処理システムの使用を防止する対策）。
   （a） アクセス権は、誤用、故意、またはその他のリスクを削減するための職務分掌および最小権限に基づいて提供されます。
   （b） ITシステムに対するアクセス権は、ユーザーが有効なユーザー名およびパスワードにより登録されている場合に付与されます。
   （c） データインポータには、支給されたノートパソコンへのユーザーログインに強力なパスワードを要求し、仕事以外の機能にも使用されるパスワードの使用を禁止し、パスワードまたはその他のログインクレデンシャルを忘れた、盗まれた、または侵害された場合にすべきことをユーザーにアドバイスするパスワードポリシーが設けられています。
   （d） 必須パスワードは定期的に変更します。
   （e） 有効なユーザー名およびパスワードでの新規登録後にのみ、自動的にコンピュータをロックし、PCへのアクセスが更新されます。
   （f） データおよびユーザーの分類によって、各システムが使用する必要がある認証の種類を決定します。
   （g） リモートアクセスおよびワイヤレスコンピューティングの機能が制限され、ユーザーおよびシステムの両方の保障措置とともにユーザー認証が実施されていることが求められます。

2. **アクセス制御**（つまり、システムに対する不正アクセスを防止するための対策）。
   （a） アクセス承認は、個人が割り当てられている作業（仕事場の役割）の特定分野ついて発行されます。
   （b） 作業領域に変更があった場合、または従業員の雇用が何らかの理由で終了した場合のアクセス承認の調整。
   （c） 適切な制御を追加し、問題のシステムをサポートする必要がある場合に限定した管理者特権の付与、解除、および見直し。

（d） 重要デバイスおよびシステムからのイベントログは集中的に収集され、例外ベースで報告されて、インシデント対応および科学調査を可能にします。

データのアクセス制御。データインポータは個人データのアクセスおよび使用に関して下記に示す管理を行います。

1. 職員は、データインポータに関連する業務目的を達成するために必要な最小限の個人データのみを使用するように指示されます。
2. 職員は、自身の職務を遂行するために必要である場合を除き、個人データの読み取り、コピー、変更、または削除を行わないように指示されます。
3. 第三者の個人データの使用に制限を課す第三者とデータインポータ間の契約諸条件を通じて個人情報の第三者による使用が管理され、かかる使用はサービスの提供に第三者が必要とするものに限定します。

分離制御法的に求められている場合、データインポータは異なる目的のために収集された個人データを別途に処理できることを保証します。また、データインポータはテストシステムと生産システムとを区別することを保証するものとします。

可用性制御。データインポータは偶発的破壊または損失から以下の管理を行うことで個人データを保護します。

1. 個人データは、顧客契約、あるいはそれがない場合はデータインポータの記録管理ポリシーおよびプラクティスとともに、法的な保存要件に従って保持します。
2. ハードコピーの個人データは安全なごみ箱内か、または情報が容易に解読されないようにシュレッダーでクロスカットして処分します。
3. 電子的な個人データは適切に処分されるよう、データインポータのIT資産管理チームに渡します。
4. ウイルス対策ソフトウェアがすべてのシステムにインストールされており、ファイアウォールを使用してネットワークが保護されています。ネットワーク分離、コンテンツフィルター/プロキシの使用、無停電電源、定期的なバックアップの生成、必要に応じたハードディスクのミラーリング、耐火性システム、必要に応じた防水システム、緊急対策、空調管理されたサーバ室を含め（これらに限定されることなく）適切な技術的な対策が取られています。

データ入力制御。データインポータに、必要に応じて、個人データがデータ処理システムに入力されているかどうかおよび誰によって入力されたか、あるいはかかるデータが変更または削除されているかどうかを確認するように設計された対策があります。関連するアプリケーションへのアクセスが記録されます。

システムの開発およびメンテナンス。データインポータ環境における適用性について公に公開された第三者脆弱性を確認します。データインポータのビジネスおよび顧客へのリスクに基づき、修正のための時間枠が事前に決められています。さらに、新規および重要なアプリケーションならびにインフラストラクチャにリスクに応じた脆弱性スキャンおよび評価を実行します。実稼働前に開発環境でコードレビューおよびスキャナーを使用し、リスク基づいてコーディングの脆弱性を積極的に検出します。これらの手順によって脆弱性とともにコンプライアンスも積極的に特定できます。

コンプライアンス。情報セキュリティ、法務、プライバシー、およびコンプライアンスの各部門は、データインポータに適用される可能性のある地域の法律および規則を特定するよう取り組んでいます。これらの要件は、データインポータおよびその顧客の知的所有権、ソフトウェアライセンス、従業員および顧客の個人情報の保護、データ保護およびデータ処理の手順、国境を越えるデータ伝送、財務および運営上の手順、テクノロジーに関連する行政による輸出規制、ならびに科学調査要件などの分野が対象となります。情報セキュリティプログラム、プライバシーに関する運営委員会、社内外の監査/評価、社内外の弁護士によるコンサルティング、内部統制評価、内部侵入テストおよび脆弱性評価、契約管理、セキュリティに関する認識、セキュリティコンサルティング、ポリシーの例外レビュー、ならびにリスク管理などのメカニズムを組み合わせてこれらの要件の順守を促進します。

米国HIPAA下請け契約

Dell Inc.ならびに世界の直接子会社および間接子会社（「**デル**」または「**業務提携者**」）とプロバイダ、その親会社、ならびにその世界の直接子会社および間接子会社（「**下請け業者**」）は、デルがプロバイダから製品を購入し、プロバイダがデルの代理としてサービスを提供するために従う契約（「**プロバイダ契約**」）を締結しました。本HIPAA下請契約（「**HIPAA契約**」）はデルと下請け業者間のデータ保護契約（「**DPA**」）に付属し、その一部となります。

1. **目的の表明。**デルはその顧客への特定のサービスの提供に従事しています。これらの業務に関連し、デルは1996年の医療保険携行可能性/執行責任法（「**HIPAA**」）のプライバシーおよびセキュリティの規則で求められているとおり、その信頼できる顧客と業務提携契約を締結しています。デルは、プロバイダ契約に従い、デルがかかるサービスの履行の全部または一部を下請け業者に請け負わせることに関連し、下請け業者と本HIPAA契約を締結します。両当事者は、下請け業者がPHIを保管または収容する設備またはシステムに責任を負う場合があること、または、デルと下請け業者間のプロバイダ契約に基づくサービスの履行においてPHIに触れる、作成する、受領する、保守する、送信するまたは知り得る、あるいはそれらすべてが行われる場合があることを認めます。本HIPAA契約は、本HIPAA契約およびプロバイダ契約に基づく下請け業者の活動に関連し、HIPAAの規則で求められている書面による保証に相当します。
2. **優先順位。**本HIPAA契約の規定がプロバイダ契約の規定に反している場合、本HIPAA契約の規定が効力を持つものとします。本HIPAA契約の条件におけるいかなる曖昧性も、デルおよびデルの顧客がHIPAAを順守できるように解釈されます。本HIPAA契約のいかなる条件も、下請け業者がデル向けのサービスの履行に役立てるために下請け業者または代理人を雇っておくことを禁止するプロバイダ契約のいかなる条件も変更または修正するものではありません。
3. **定義**。本HIPAA契約に特に定義されていない大文字の用語は、DPA、NDA、または適用されるプロバイダ契約に記載されている意味を有します。
   3.1. 「**違反**」は45 C.F.R. § 164.402に記載された意味を有します。
   3.2. 「**対象事業体**」は45 C.F.R. § 160.103に記載された意味を有します。
   3.3. 「**顧客**」とは、HIPAAに基づく対象事業体であるデルの顧客を意味します。
   3.4. 「**データ集約**」は45 C.F.R. § 164.501に記載された意味を有します。
   3.5. 「**指定されたレコードセット**」は45 C.F.R. § 164.501に記載された意味を有します。
   3.6. 「**発見**」は45 C.F.R. § 164.410（a）（2）で説明されている「発見」を意味します。
   3.7. 「**ePHI**」は、プロバイダ契約に基づいてデルまたはデルの顧客から、またはその代理として下請け業者によって作成、受領、保守、または伝送される、45 C.F.R. § 160.103で定義されている「電子的に保護すべき健康情報」を意味します。
   3.8. 「**HIPAA違反通知規則**」とは、45 C.F.R.第164編の副編Dに示されている「セキュリティで保護されていない保護すべき健康情報に違反した場合の通知」を意味します。
   3.9. 「**HIPAAプライバシー規則**」とは、HIPAAに基づいて公布された45 C.F.R. § 160の副編Aおよび副編Eで公布された基準、要件、および仕様を意味します。
   3.10. 「**HIPAAセキュリティ規則**」とは、HIPAAに基づいて公布された45 C.F.R. § 164の副編Cで長官により公布された基準、要件、および仕様を意味します。
   3.11. 「**HIPAA規則**」は、適宜修正されることがあるHIPAAプライバシー規則、HIPAAセキュリティ規則、違反通知規則と同じ意味を有します。
   3.12. 「**個人**」は、45 C.F.R. § 160.103に記載された意味を有します。
   3.13. 「**PHI**」は、プロバイダ契約に基づいてデルまたはデルの顧客から、またはその代理として下請け業者によって作成、受領、保守、または伝送される、45 C.F.R. § 164.501で定義されている「保護すべき健康情報」を意味します。
   3.14. 「**法律で求められている**」は、45 C.F.R. § 164.103に記載された意味を有します。
   3.15. 「**長官**」とは、45 C.F.R. § 160.103に記載された意味を有します。
   3.16. 「**セキュリティインシデント**」は、45 C.F.R. § 164.304に記載された意味を有します。
   3.17. 「**売却**」または「**販売**」とは、下請け業者によるPHIの開示であり、下請け業者が直接的または間接的にかかるPHIの受領者から、またはその代理としてかかるPHIと交換に報酬を受領することを意味します。ただし、45 C.F.R. § 164.502（a）（5）（ii）（B）（2）に説明されているPHIのいかなる開示も含みません。
   3.18. 「**セキュリティで保護されていない保護すべき健康情報**」とは、45 C.F.R. § 164.402に示された意味を有するものとします。
4. **下請け業者の義務。**下請け業者は以下に合意します。
   4.1. プロバイダ契約に基づきデルに対してその義務を遂行するように求められており、本HIPAA契約で明示的に許可されているまたは求められている、あるいは法律によって求められている場合を除き、PHIを使用しない、またはそれ以上は開示しないこと。PHIのかかる使用、開示、または要求は、実行可能である場合は限定されたデータセットを、それ以外の場合はその使用、開示、または要求の本来の目的を達成するために必要最小限のPHIを利用するものとします。

4.2. 合理的かつ適切な保障措置を使用して本HIPAA契約で許可されており、HIPAA規則に示されている適用可能な原則および義務に一致している場合を除き、いかなる方法によってもPHIを使用または開示しないこと。

4.3. 本HIPAA契約に規定されていないPHIの使用または開示は、かかる使用または開示が認識されてから24時間以内に書面にてデルに報告すること。さらに、下請け業者は、セキュリティで保護されていない保護すべき健康情報の取得、アクセス、使用、または開示が45 C.F.R. § 164.402（1）の違反の定義から除外されていない限り、かかる事象を発見後24時間以内に書面にてデルに報告します。そのようなすべての報告には、セキュリティで保護されていない保護すべき健康情報がアクセス、取得、または開示された、あるいは事業提携者によってそのように合理的に確信されている各個人の身元（わかっている場合）、および45 C.F.R. § 164.410（c）で求められているその他すべての情報、ならびにデルまたは該当する顧客が合理的に求めるその他のいかなる情報も含めるものとします。かかる報告を受領した時点で、デルはリスク評価を実施するか、またはデルの指示の下に下請け業者に実施させ、かかる取得、アクセス、使用、または開示がかかるセキュリティで保護されていない保護すべき健康情報のセキュリティまたはプライバシーが侵害されているかどうかを45 C.F.R. § 164.402（2）の違反の定義に定められている要素に基づいて判断します。下請け業者が、かかるリスク評価に基づいて、かかる取得、アクセス、使用、または開示によってセキュリティで保護されていない保護すべき健康情報が侵害された可能性が低いと確信している場合、下請け業者はかかる結論を裏付けるすべての情報をデルに提供するものとします。

4.4. 164.502（e）（1）（ii）および164.504（e）（2）（ii）（D）に準拠して、PHIを作成、受領、保守、または送信する代理人または下請け業者は、かかる代理人または下請け業者がかかる情報に関して下請け業者に適用されるものと実質的に同じ制限と条件を順守することを書面による契約で証明した合理的な言質を提供することに合意することを保証すること。

4.5. 下請け業者が指定されたレコードセットを維持している範囲において（ある場合）、指定されたレコードセットにおいて下請け業者によって保守されているPHIを、45 C.F.R. § 164.524に記載されたPHIのコピーを検査および取得するためにアクセスする権利を個人に与えるための義務を順守するためのデルの顧客の必要に応じてデルに利用できるようにすること。デルまたは該当する顧客によって明確に求められた場合、下請け業者は以下を行います。

(a) 電子コピー。PHIのコピーを電子的な形式で個人が指定する人物に直接送信します。

(b) 紙のコピー。PHIのコピーを紙で作成し、かかるコピーを個人が指定する人物に直接提供します。

4.6. 下請け業者が指定されたレコードセットを保守している範囲において（ある場合）、指定されたレコードセットに下請け業者によって保守されているPHIを、45 C.F.R. 164.526に記載されたPHIを修正する義務に準拠するためのデルの顧客の必要に応じてデルに利用できるようにすること。

4.7. デルの顧客が自身の要件を満たし、45 C.F.R. 164.528に準拠して個人に対して開示の根拠を提供できるように、45 C.F.R. § 164.528により根拠が必要な下請け業者によるPHIの開示に関する情報をデルが利用できるようにすること。

4.8. 本HIPAA契約による義務の順守、ならびに下請け業者によるPHIの使用または開示に関連する内部慣行、規則、および記録を、デルまたはデルの顧客がHIPAA規則を順守しているかどうかを決定するために長官が利用できるようにし。

4.9. 45 C.F.R. § 164.502（a）（4）（i）に従って、かかる資料を要求に応じてデルまたはデルの顧客に提供すること。

4.10. 本HIPAA契約が何らかの理由によって終了した時点で、可能である場合は、下請け業者がその時点で保守しているすべてのPHIをいかなる形式のものであれすべて返却するか、またはデルの選択により電子的に破壊してかかる情報のコピーを一切保持しないようにします。あるいはこのような返却または破壊が可能でない場合は、下請け業者は（i）デルに対し返却または破壊を不可能としている条件を通知し、（ii）本HIPAA契約による保護をPHIまで拡大し、（iii）PHIの返却または破壊を不可能にしている目的へのそれ以降の使用および開示を制限するものとします。デルがかかるPHIの破壊を選択した場合、かかる破壊が行われたことをデルに書面で証明します。

4.11. ePHIについては、

(a) 本HIPAA契約に規定されている以外のePHIの使用または開示を防止するため、ePHIについては、45 C.F.R. § § 164.308、164.310, 164.312、164.314、および45 C.F.R. § 164.316で説明されている適用される管理上、物理的および技術的な保障措置を含め、セキュリティ規則で求めているePHIの機密性、整合性、および可用性を合理的かつ適切に保護するための管理上、物理的、および技術的な保障措置を実施します。ただし、下請け業者は、（A）下請け業者が（1）適用されるHIPAAの規定に準拠して下請け業者が実施し、文書化したリスク評価を通じてかかる暗号化が合理的でなく適切でないと判断し、（B）かかる文書のコピーをデルに提供し、（C）デルが下請け業者に対してかかる非暗号化の承認を書面で提供した場合を除き、DPAの第3節（f）に従って送信時および保管時にePHIを暗号化するものとします。

(b) 45 C.F.R. § 164.504（e）（2）（ii）（D）、§ 164.308（b）（2）および（3）ならびに § 164.314（a）（2）（iii）に従って、本第3節（j）の第（i）項に説明されている要件のとおりに、かかるePHIを保護するための合理的かつ適切な保障措置を実施することに、ePHIを作成、受領、保守、または伝送するすべての代理人は、下請け業者を含めて合意し、これを書面による契約により証明することを保証します。さらに、

(c) 認識されているePHIに影響するセキュリティインシデントをデルに報告します。

4.12. PHIを売却しないこと。

4.13. 本HIPAA契約に違反した下請け業者によるPHIの使用または開示について下請け業者が認識している悪影響を可能な範囲まで軽減します。

4.14. デルによる書面にての具体的な要求がない限り、データ集約活動およびPHIの匿名化は実行しないこと。

4.15. セキュリティで保護されていない保護すべき健康情報の違反により生じた損害の対応（通知および与信モニタリングサービスを含む）、修正、または軽減、あるいは下請け業者による本HIPAA契約、DPA、NDA、またはプロバイダ契約に基づく義務の不履行または本契約に定めのないPHIの開示の使用によって生じたセキュリティインシデントにより発生した費用および前述に関連して個人または規制者による苦情への対応でデルが負った費用をデルに弁済すること。さらに、

4.16. （i）PHIの使用または開示に関連するいかなる同意、承認、または許可の有効性に対する変更、制限、瑕疵、あるいは取り消しまたは終了、（ii）デルまたは該当する顧客が締結した合意、あるいは、（A）45 C.F.R. § 164.522（a）または45 C.F.R. § 164.520に従ったPHIの使用または開示を制限するか、（B）45 C.F.R. § 164.522（b）に従ったPHIに関する機密情報を求めるかの該当する顧客のプライバシー慣行における制限に準拠すること。制限において下請け業者による順守が必要であることをデルまたは該当する顧客が下請け業者に通知している場合、第（i）項または第（ii）項に基づき、いずれの場合も、かかる修正、瑕疵、取り消し、終了、制限、秘密情報に関する義務または制限は、本HIPAA契約に定められた下請け業者の許可されたまたは必要なPHIの使用または開示に影響を与えます（総称して**「制限」**）。

5. **契約期間と終了。**各プロバイダ契約に関し、本HIPAA契約の条件はかかるプロバイダ契約の条件と同じであるものとします。下請け業者による本HIPAA契約の重大な違反をデルが認識したか、またはかかる違反を下請け業者が認識した時点で、これらは速やかにデルに開示するものであり、デルは、デルの裁量により、かかる通知から30営業日以内にその違反を解決するか、または違反を終結する機会を下請け業者に与えることができます。下請け業者がデルが満足する期間内に不履行を是正または違反行為を終結させることができない場合、あるいはデルがその自由裁量でかかる機会を提供しない場合、デルは本HIPAA契約およびかかる不履行の対象である契約を下請け業者に対する書面による通知をもって直ちに終了する権利を有するものとします。デルの裁量においてかかる契約の終了が実行できない場合、下請け業者はその不履行を長官に報告する権利をデルが有するものであることを本契約により認めます。

6. **下請け業者。**下請け業者はHIPAAが求める範囲において（45 C.F.R. § § 160.102（b）、160.300、164.104（b）、164.302および164.500（c）など）HIPAAプライバシー規則、HIPAAセキュリティ規則、およびHIPAA違反通知規則の基準および要件が下請け業者に適用されることを認めます。

7. **免責。**下請け業者は、デルおよびデルの取締役、役員、従業員、代表者および代理人を、本HIPAA契約に基づく下請け業者の代行、職務および義務に関する下請け業者の作為または不作為に起因または関係し、あるいはその結果によりまたはその結果に関連して生じたすべての申し立て、訴訟、請求および法的手続きならびにすべての債務、損害賠償、損失、判決、正当な委譲、費用、罰金、違約金、ならびに合理的な弁護士報酬を含めた費用について補償し、無害に保ち、保護するものとします。

業務提携契約

Dell Inc.と世界中のその直接子会社または間接子会社は、Dell Inc.の包括的福利厚生制度（「**制度**」）の制度提供者（「**制度提供者**」）の立場で、契約（「**プロバイダ契約**」）に従い、特定のプロフェッショナル、コンサルティング、またはその他のサービス（「**サービス**」）を制度に提供するプロバイダを雇用します。本業務提携契約（「**BAA契約**」）はデルとプロバイダ間のデータ保護契約（「**DPA**」）に付属し、その一部になります。

1. **目的の表明。**プロバイダはサービスの履行において制度加入者の秘密健康情報に対してアクセス、保持し、開示された状態で表示するか、または知り得ることができるため、適宜修正されるとおりの（a）45 C.F.R.第164編の副編Aおよび副編Eにて長官により公布された基準、要件、および仕様（「**プライバシー規則**」）、（b）連邦規制8334以下（45 C.F.R.第160編、第162編、および第164編）で2003年2月20に公開されたセキュリティ基準（「**HIPAAセキュリティ規則**」）、（c）最終総括規則（「**HIPAA総括規則**」）の一部としてHITEC法の副編Dおよびその施行規則で長官によって公布された規則により 制定された違反通知の基準、要件、および仕様（総称して「違反通知規則」）、（d）45 C.F.R.第164編の副編C、副編D、および副編Eで長官によって公布された施行基準（「施行規則」）を含めて、1996年の医療保険の携行可能性/執行責任法（「**HIPAA**」）、経済的および臨床的健全性のための医療情報技術に関する法律（「HITECH法）」、およびそれらに関連して公布された規則（「**HIPAA規則**」）により保護された情報を含み、それらに限定されることなく、連邦法および州法に準拠して、かかる情報の 機密性を保護することに両当事者は合意します。
2. **定義。**本BAA契約に特に定義されていない大文字の用語は、DPA、NDA、適用されるプロバイダ契約またはHIPAA規則に記載されている意味を有します。
   2.1. 「**違反**」とは、45 C.F.R. § 164.402に定義され、その例外の対象となる、プライバシー規則で許可されていない、PHIのセキュリティまたはプライバシーを侵害する方法でのPHIの取得、アクセス、使用、または開示を意味します。
   2.2. 違反の発見に関連する「**発見**」には、HITECH法または45 C.F.R. § 164.410（a）（2）を含む適用法に記載されている意味を有します。
   2.3. 「**ePHI**」とは、制度により、またはその代理として作成、受領、保守、または伝送される、HIPAAセキュリティ規則に定義された「電子的に保護すべき健康情報」を意味します。
   2.4. 「**HIPAAセキュリティ規則**」とは、45 C.F.R.第160編、第162編、および第164編で発表され、適宜修正されるとおりのセキュリティ基準を意味します。
   2.5. 「**HITECH法**」とは、2009年2月17日に施行された経済的および臨床的健全性のための医療情報技術に関する法律の第1款以下および74連邦法42740以下にて公開され、適宜修正されるとおりの「セキュリティで保護されていない保護すべき健康情報」に関する規則を含め、それらに限定されることなく、それらの施行規則を意味します。
   2.6. 「**個人**」とは、45 C.F.R. § 160.103の用語の「個人」と同じ意味を有し、45 C.F.R. § 164.502（g）に従って人格代表者と認める者を含みます。
   2.7. 「**法律**」とは、適用可能なすべての連邦および州の制定法およびその下のすべての関連規則を意味します。
   2.8. 「**PHI**」は45 C.F.R. § 160.103の用語「保護すべき健康情報」と同じ意味を有し、制度からまたはその代理としてプロバイダにより作成、受領、保守、または伝送される情報に限定されます。
   2.9. 「**長官**」とは、保健社会福祉省長官またはその被指名人を意味します。
   2.10. 「**下請け業者**」とは、プロバイダがプロバイダの従業員の能力以外などの面において機能、活動、またはサービスを委託する人物または事業体を意味します。
3. **機密保持。**プロバイダは、PHIの機密性および秘密保持を認め、（a）かかるPHIは、本契約書に添付されている別紙Bに概ね一覧表示されたサービスの履行に固有の使用および開示を含めて、本BAA契約の下で、法律に従いまたは法律で求められているように使用または開示され、（b）プロバイダは、HIPAA規則を含め、法律に従ってかかるPHIのプロバイダによる伝送、処理、保管、および仕様はPHIの機密性が保持されることを保証するように設計された合理的な保障措置を使用するものとすることに合意します。
4. **プロバイダの責務**
   4.1. 記録。プロバイダは本BAAに関連して行ったすべてのトランザクションの正確な記録を保守します。プロバイダは、HIPAA規則およびその他すべての法律に基づいて、業務提携者としての義務に準拠することを承認し、合意します。
   4.2. 根拠。制度は、プライバシー規則に基づく対象事業体として45 C.F.R. 164.528に従い、個人に対しての開示の根拠を示す義務を認めます。本BAA契約に従い、PHIに関してのみ、プロバイダは（i）プライバシー規則およびHITEC法に基づく根拠に従いPHIのすべての開示を文書化し、要求に応じて制度が利用できるようにし、（ii）個人からの根拠に関する要求を受け取って処理し、（iii）個人に対して根拠を提供し、（iv）該当する場合は、根拠の提供を保留することに合意します。プロバイダは、HITECH法およびHIPAA規則で求められていない限り、根拠の提供に必要な情報を開示の日から6年間保守します。
   4.3. 開示。プロバイダは、プロバイダが知り得た、または知るべき本BAA契約で許可されている以外の情報の使用または開示を発見後、合理的な時間枠内に制度に報告することに号します。プロバイダは保護すべきPHIへの違反に関する本BAA契約の第5節にある開示の要件に適用される範囲まで従うものとします。

4.4. 下請け業者。プロバイダは、プロバイダの代理としてすべてのPHIを作成、受領、保守、または伝送する下請け業者を含めたすべての代理人が本BAAで求めているPHIの使用または開示に関連するものと同じ制限、条件、および要件に書面にて合意することを保証するものとし、プライバシー規則またはその他の適用可能な法律のすべての規定に違反するいかなる方法でも、本BAAに掲げる場合以外にPHIを使用または開示しないものとします。プロバイダはさらに、EPHIを提供する下請け業者を含めたすべての代理人が本BAA契約の第4（t）節に従ってかかる情報を保護するための合理的かつ適切な保障措置の実施に合意することを保証することに合意します。プロバイダが、45 C.F.R. § 164.504（e）（1）（iii）および総括規則に従い、プロバイダ契約に基づく下請け業者の義務の重大な不履行または違反となる下請け業者の行動または履行パターンを発見した場合、プロバイダは不履行を是正するかまたは違反行為を終結するための合理的な措置を取らなければならず、かかる措置が失敗に終わった場合、実現可能であれば、下請け業者との契約を終了します。

4.5. 制限事項。プロバイダは、HITECH法およびそれらに従って公布された規則またはガイダンスに準拠し、PHIのいかなる要求、使用、および開示も実際的な範囲まで限定されたデータセットに制限するか、あるいは、必要な場合は、その要求、使用、または開示の目的の達成に必要最小限のPHIに限定することに合意します。両当事者が「必要最小限」という語句をプライバシー規則、HITECH法、および長官が発行したすべてのガイダンスに準拠して解釈されるものであることを認めます。

4.6. 修正。制度は、45 C.F.R.164.526に準拠して個人のPHIを修正する、プライバシー規則に基づく対象事業体としての義務を認めます。本BAA契約に従い、保護すべき健康情報に関して、プロバイダは、該当する場合は保護すべき健康情報の修正およびそれに対して修正を加えることについての要求を承認または拒否することを含め、それらに限定されることなく、45 C.F.R. § 164.526を順守することに合意します。

4.7. 副編Eコンプライアンス。プロバイダが45 C.F.R.第164編の副編Eに基づく1つ以上の制度を実行する範囲において、かかる義務の履行にて制度に適用される副編Eの要件を順守します。

4.8. 慣行および記録。プロバイダは、制度の代理としてプロバイダから受領またはプロバイダによって作成または受領する保護すべき健康情報に関連するポリシーおよび手順を含め、保護すべき健康情報の使用および開示に関連する内部慣行、規則および記録を、HIPAA規則に準拠してコンプライアンスを判断する目的のためのみに制度および長官が利用できるようにすることに合意します。

4.9. 機密保持。プロバイダおよび制度は、本BAA契約のすべての機密保護規定が本BAA契約終了後も存続するものとすることに合意します。

4.10. データ集約。プロバイダは制度の健康管理業務に関連するデータ集約サービスを提供することができます。

4.11. PHIの使用。本BAA契約により適切な管理を行うため、または法的責任が存在する場合はその責任を実行するためにプロバイダがPHIを使用することは禁止されていません。さらに、プロバイダ、その適切な管理のため、または法律によって開示が求められている場合、プロバイダは情報が開示された人物からその情報を機密に保ち、法律によって求められている場合にのみ、またはその人物に開示された目的のために使用またはさらに開示するという合理的な保証を得ている場合に法的責任を実行する目的でPHIを開示することは禁止されていません。プロバイダはさらに、情報が公開される人物は当該情報についての守秘義務の不履行またはHIPAA規則に対する違反があった場合はそれをプロバイダに通知することを求めます。このような場合、プロバイダは情報の守秘義務の不履行、またはプライバシー規則の違反において自身が知り得たすべての出来事を制度に通知します。

4.12. 報告。プロバイダは、法律違反をプライバシー規則に準拠して該当する連邦当局および州当局に報告するためにPHIを使用することは禁止されていません。

4.13. アクセス。制度は、45 C.F.R.164.524に基づき、個人のPHIへのアクセスを当該個人に提供するためのプライバシー規則に基づく対象事業体としてのその義務を認めます。本BAA契約に従い、保護すべき健康情報に関して、プロバイダはアクセスに関する要求を承認または拒否し、45 C.F.R. § 164.524に基づいて求められている場合は、アクセスの拒否に関する見直しを行い、個人にアクセスを提供することに合意します。プロバイダが個人のPHIに関する電子的健康記録を使用または保守する場合、プロバイダは要求に応じて、個人かまたは個人が指名した第三者に直接、HITECH法およびそれに基づいて発行されたすべてのガイダンスに規定されているとおりのコンプライアンスの日付に従ってPHIの電子的コピーを提供するものとします。

4.14. 軽減。プロバイダは、実行できる範囲において、プロバイダ、またはその下請け業者の本BAA契約または適用法の要件に違反したPHIの使用または開示の結果生じ、プロバイダが認識しているすべての悪影響を緩和することに合意します。

4.15. 制度の可用性。プロバイダは、開示がプロバイダ契約の条件の対象となっており、それらに準拠している場合は、要求受領後3営業日以内に、45 C.F.R. § 164.504（f）に基づく健康制度機能を実行するための制度に関連するPHIを制度、または制度の要求に応じて制度提供者が利用できるようにすることに合意します。

4.16. 許可。プロバイダが制度の代理として作成、受領、保守、伝送するPHIに関し、プロバイダは45 C.F.R. § 164.506または164.508に準拠して個人の保護すべき健康情報を使用または開示するために必要な承認をその個人から取得する責任を負います。ただし、制度提供者は適用される連邦または州の法律ならびに規則に基づいて必要となる同意または許可を制度提供者がプロバイダからプライベート健康情報を受領する前に取得するものとします。開示前に必要な

許可の取得を怠った場合、プロバイダは本BAA契約に違反することになることを認め、本BAA契約の第4節（c）に基づいて制度に報告する必要があります。

4.17. 制限要求。制度の代理としてプロバイダが作成、受領、保守、または伝送するPHIに関し、プロバイダは45 C.F.R. § 164.522に準拠して個人からの制限に関する要求を受け取り、かかる要求に従って拒否または合意するために拒否または合意する責任を負います。プロバイダが制限に合意した場合、プロバイダは当該制限と一致するPHIの使用および開示に責任を負うものとします。合意された制限に従わない場合は本BAAの違反となり、本BAAの第4（c）節に準拠し、制度にその旨を報告する必要があります。制限の要求が直接制度に対して行われた場合、本款に準拠して制度はかかる要求の処置についてプロバイダに照会します。

4.18. 機密情報。プロバイダが制度の代理として作成、受領、保守、または伝送するPHIに関し、プロバイダは要求に応じて45 C.F.R. § 164.522に準拠して個人から機密情報を受領し、行動する責任を負います。プロバイダが機密情報に対する要求の収容に合意した場合、プロバイダはその収容を順守する責任を負います。付与されている収容に従わない場合は本BAA契約の違反になり、本BAA契約の第4（c）切に準拠して制度に報告する必要があります。機密情報の要求が制度に対して直接行われた場合、制度はカスタマーサービスを通じて個人をプロバイダに照会します。

4.19. 匿名化。プロバイダがHIPAAに準拠して情報を匿名化しなければならない場合、プロバイダはすべてのPHIを匿名化することができます。匿名化された情報は保護すべき健康情報とはならず、プロバイダまたは関連の事業体が比較データベースの作成、統計分析、またはその他の調査を行うために使用することができます。

4.20. 保障措置。本BAA契約の他の規定を制限することなく、プロバイダは（i）管理上、物理的および技術的な保障措置を実施し、制度の代理として作成、受領、保守、または伝送するEPHIの機密性、整合性、および可用性をHIPAAセキュリティが求めるとおりに合理的かつ適切に保護し、（ii）EPHIを提供する下請け業者がかかる情報を保護するための合理的かつ適切な保障措置を実施することに書面にて合意することを保証することに合意します。プロバイダは、制度が適宜要求した場合にこれらの保障措置に関するいかなる情報も制度に提供するものとします。

4.21. セキュリティインシデント。プロバイダは、認識したすべてのセキュリティインシデントを速やかに制度に報告することに合意します。

5. **セキュリティで保護されていないPHIに関するプロバイダの責務**

5.1. PHIの保護。現状では可能でない場合を除き、事業提携者は制度の代理としてプロバイダが作成、受領、保守、または伝送するPHIを承認されていない個人が使用不能、判読不能、または解読不能な状態にし、それによってPHIを安全に保つため、HITECH法、長官、またはその他の法律が定めるテクノロジーおよび方法を合理的かつ適切な方法で実装することに合意します。さらに、現状では可能でない場合を除き、プロバイダは、制度のPHIを提供する下請け業者またはベンダーを含め、それらに限定されることなく、代理人が制度のPHIを承認されていない個人が使用不能、判読不能、または解読不能な状態にすることに関し、HITECH法、長官、またはその他の法律で定めるテクノロジーおよび方法を実装することを保証するものとします。

5.2. 違反通知。セキュリティで保護されていないPHIに関し、プロバイダはプロバイダまたはプロバイダの下請け業者のいずれかが発見した不履行を発見後24時間以内に制度に報告するものとします。

(a) 報告には、（i）セキュリティで保護されていないPHIに違反した、または違反したと見られるすべての個人のID、（ii）違反の種類（窃盗、損失、不適切な処分、ハッキングなど）、違反の場所（ノートパソコン、デスクトップ、紙）、その違反がどのように発生したか、違反が発生した日付、違反が発見された日付を含めた違反の簡単な説明、（iii）メディアの種類を含め、関連するセキュリティで保護されていないPHIの種類の説明。ただし、制度によって求められている場合を除き、違反のあったPHI自体は除きます。（iv）違反の前に実施されていた保障措置の説明（ファイアウォール、パケットフィルタリング、セキュアなブラウザセッション、強力な認証など）、（v）違反に対して講じられた措置の説明（保障措置の追加、軽減、制裁、ポリシー、および手順など）、（vi）違反通知規則に準拠しリスク評価を制度が実施し、文書化できるようにするため、制度が合理的に要求したその他すべての情報、（vii）個人、長官、またはメディア、あるいはそれらすべに通知するために合理的に必要なその他のすべての情報を含める（または情報が入手可能になった時点で継続的に補充する）必要があります。

(b) 制度の単独の判断で、制度は、違反通知規則で規定されているように侵害の可能性が低いかどうかのリスク評価を行う要件を含めて、当該インシデントが違反ではないことを決定する（および制度に証拠を提供する）責任をプロバイダに委譲することができます。制度がこの義務を不合理な遅延なく、いずれの場合も発見後30暦日前までにプロバイダに委譲した場合、プロバイダは制度に対して違反の書面による通知および侵害の発生が低いかどうかを評価したリスク評価のコピーを提供するものとします。

(c) 制度の単独の判断で、個人、長官、またはメディア、あるいはそれらすべてへの通知を含め、違反通知規則によって求められている制度が決定した通知を提供する責任をプロバイダに委譲することができます。かかる通知を送付する前に、プロバイダは制度による承認を受けるために通知書の定型書式のコピーを提供します。すべての通知は違反通知規則で定められた要素に適合するものであるものとし、違反通知規則に定められた時間枠内に送付するものとします。制度が不合理な遅延なく、いずれの場合も発見後60暦日よりも前にこれらの義務をプロバイダに委譲した場合、プロバイダはメディアまたは長官の通知を含めて必要なすべての通知を行ったことを示す証拠を制度に提供するものとします。

(d) プロバイダは、プロバイダが通知するか、制度が通知するかにかかわらず、制度または該当するプロバイダが違反通知規則に基づいて必要と判断した通知の提供に関連する費用を含め、またそれに限定されることなく、違反または潜在的な違反の発生に関連して生じた合理的なすべての費用を支払うものとします。

6. **制度の責務。**制度は、制度の文書を修正し、PHIの使用および開示を制限して、プライバシー規則に準拠し、かかる使用または開示に対する手続き上の十分な保障措置および根拠提供機構を確保するための特定の規定を含めることに合意します。

7. **契約期間と終了。**

7.1. 契約期間。本BAA契約の期間はプロバイダ契約の終了まで、あるいは本BAA契約に従って終了されるまで継続するものとします。

7.2. 法の作用による終了および修正。本BAA契約は、その時点で最新の法律に基づいてHIPAA業務提携契約が適用されなくなったかまたは必要とされなくなった場合は直ちに終了するものとします。弁護士の助言により、本BAAの期間が適用法に違反するかまたは適用法を順守していないと解釈される可能性があると制度が合理的に判断した場合、両当事者は誠意をもって交渉し、かかる法律を順守するように本BAA契約を修正するものとします。両当事者がかかる修正について合理的に合意できない場合は、本BAA契約およびプロバイダの場合はプロバイダ契約を終了するものとします。

7.3. 制度による終了。プロバイダが本BAA契約、HIPAA規則、またはその他の何らかの適用法の重要な条件に違反したと制度が合理的に判断した場合、制度と協力して違反を是正するか、またはその違反を終結するためにプロバイダに与えた30日が経過した後、制度は本BAA契約を終了することができます。ただし、本BAA契約の当該終了が制度の単独裁量では実現不能である場合、プロバイダは本BAA契約の他の規定がこれと異なっているとしても制度が本BAA契約、および存在する場合はプロバイダ契約を速やかに終了させ、その違反を長官に報告する権利を有するものであることをここに認めます。

7.4. 是正の権利。プロバイダが本BAA契約またはプライバシー規則の規定に違反し、その違反を30日以内に是正できない場合、制度はかかる違反を是正する権限を保有しています。プロバイダは制度が行うかかるすべての取り組みに協力します。不履行の是正によって本BAA契約および存在する場合はプロバイダ契約を速やかに終了する制度の能力は制限されません。

7.5. 差し止めによる救済。プロバイダは、本BAA契約およびHIPAA規則の諸条件が必然的に特殊であり、独自性があり、特異なものであること、およびそれに起因する違反から生じる損失は金銭的な損害賠償では合理的かつ十分に補償されず、かかる違反により制度が回復不能な損害を被ることになることを認め、合意します。したがって、プロバイダによるプロバイダ契約、HIPAA規則、またはその他の適用法に対する不準拠により、本契約に別途規定されている場合を除き、制度またはその後継人または譲渡人には、差し止めまたはその他の臨時的な救済を受ける資格があり、また、かかる差し止めまたはその他の臨時的な救済は、制度、その後継人または譲渡人が利用できるその他すべての救済策に重複され、かかる救済は保証金を差し入れる必要はありません。

7.6. 終了の効果。本BAA契約の終了または満了をもって、プロバイダはプロバイダが制度の代理として作成、受領、保守、または伝送し、プロバイダが何らかの形式で保守しているすべてのPHIを返却または破壊するものとし、かかる情報のコピーを保持しないことが実現可能であり、その他の適用法で禁止されていない範囲において、かかる情報のコピーは一切保持しないものとします。この規定は、プロバイダまたは制度あるいはその両者の代理としてPHIを処理できるプロバイダのすべての下請け業者または代理人に適用されます。制度は、かかる情報の返却または破壊が実行不能であるまたは許可されないことを制度が確認している場合、プロバイダはプロバイダがかかるPHIを保守している限り、かかるPHIの使用、保管、および開示に関しては本BAA契約のすべての規定を順守し続けることに合意します。

7.7. 一般的に許可されている使用および開示。本BAA契約で別途に制限されている場合を除き、制度自体によって履行される場合、機能、活動、またはサービスを、プロバイダ契約に定められているとおりに制度のため、または制度の代理として履行するためのPHIの使用または開示がHIPAAの規則またはその他の法律に違反しないのであれば、プロバイダはPHIのかかる使用または開示を行うことができます。

8. **免責。**各当事者は、相手方当事者によるPHIの使用、開示、または保管、あるいは当該当事者による本BAA契約の違反における免責当事者の怠慢または故意の違法行為により生じたすべての請求、損害賠償、損失、判決、原価および費用（弁護士報酬を含む）を相手方当事者に補償し、それらから保護し、免責するものとします。