**数据处理协议**

1. *定义：*在本《数据处理协议》（DPA）中，以下术语应适用下文规定的含义：

* “充分保护的国家”是指欧盟委员会、信息专员办公室或联邦数据保护和信息专员（视具体情况适用）已确定为其各自职权范围提供保障和充分保护水平的国家。
* “适用的数据保护法”是指适用的数据保护和隐私保护法律，包括（如果适用）美国数据保护法、欧盟数据保护法、英国数据保护法和瑞士数据保护法。
* “控制者”、“处理者”、“数据主体”、“个人数据”、“处理”（和“处理（动词）”）以及“特殊类别的个人数据”应具有适用的数据保护法中规定的含义。
* “EEA”是指欧洲经济区。
* “美国”是指美利坚合众国。
* “EC”是指欧洲委员会。
* “欧盟数据保护法”是指（a）《欧盟通用数据保护条例》（第2016/679号条例）（GDPR）；（ii）《欧盟电子隐私指令》（第002/58/EC号指令）；（iii）依据或根据以上任何法规制定的任何欧盟成员国法律，包括以上各项法律的修订或替代版本。
* “瑞士数据保护法”是指 1992 年颁布至 2022 年 12 月废止的《瑞士联邦数据保护法》（FADP）；从 2023 年 1 月 1 日起，应适用经修订的 2020 年《瑞士联邦数据保护法修订版》（修订版 FADP），包括该法律将来的修订或替代版本。
* “英国数据保护法”是指《数据保护、隐私和电子通信（修订等）（退出欧盟）条例》（第2019/419号条例），并且由根据欧盟相关法规（2018年《退出欧盟法》）颁布的2018年《数据保护法》（英国DPA）和《英国DPA（保留（欧盟）第2016/679号条例》（英国GDPR）进行补充，包括以上法律将来的修订或替代版本。
* “美国数据保护法”是指（a）2018 年《加州消费者隐私法》（CCPA），经 2020 年《加州隐私权法》 (CPRA) 和后续的实施条例修订和整合；（b）2021 年《弗吉尼亚州消费者数据保护法》（VCDPA）；（c）2021 年《科罗拉多州隐私法》（CPA）；（d）2022 年《康涅狄格州数据隐私法》（CTDPA）；（e）2022 年《犹他州消费者隐私法》（UCPA），包括以上法律将来的修订或替代版本。
* “海菲秀" 是指 海菲秀 LLC。
* “设备”是指 海菲秀 Syndeo 设备、系统和软件。
* “消费者”是指获得设备治疗的人士。
* “客户”是指提供设备治疗的诊所或中心。
* “授权用户”是指客户、其关联方以及其各自执行设备治疗的员工、承包商或顾问。

1. *协议双方的关系：*海菲秀（控制者）指定客户（处理者）处理本 DPA 第 14 条所述的个人数据（“数据”），用于本 DPA 第 16 条所述的目的或双方另行书面约定的目的（“许可目的”）。客户不得出于许可目的以外的任何目的保留、使用或披露数据。客户不得买卖数据。各方应遵守适用的数据保护法规定的各自义务。
2. *国际传输和数据本地化法律：*客户及其授权用户通过设备输入和访问的数据在美国托管，并且在[\*链接到 SCCs\*]（“SCC 的网页”）上提供的经批准的适用标准合同条款（“SCC 的”）应视为已纳入本 DPA，以遵守适用的数据保护法。如果客户需要完全签署的标准合同条款版本，其可以在 SCC 的网页上会签适用的预签名版本，并通过电子邮件将副本发送至 dpo@海菲秀.com。在 EEA 以外的国家（“第三国”），如果根据数据本地化法律对数据存储和传输规定了法律限制，数据则不会在当地向境外传输或托管，并且数据将在本地服务器存储。在将数据传输到美国之前，海菲秀l 已采取合理措施确保传输的数据获得与所在国家或来源地提供的基本相同的保护。对于源自英国或瑞士的数据，在第 3 条中提到的：（a）“EEA”应视情况以“英国”或“瑞士”代替；（b）“欧盟数据保护法”应视情况以“英国数据保护法”或“瑞士数据保护法”代替；并且（c）”EC”应视情况以“信息专员办公室”或“联邦数据保护和信息专员”代替。
3. *安全和保密*：考虑到处理的性质，海菲秀 和客户应采取适当的技术和组织措施，以确保与风险相适应的安全级别（参照《欧盟通用数据保护条例》第 32 条规定），以保护数据（i）防止意外或非法破坏，以及（ii）防止丢失、更改、未经授权披露或访问数据（“隐私泄露”）。客户应确保处理数据的任何授权用户已明确同意保密。
4. *分包处理：*考虑到处理的性质，如果授权用户根据适用的数据保护法可能被视为分包处理者，客户则至少应确保仅出于许可目的遵守本 DPA 中规定的要求和条件。
5. *合作与数据主体的权利*：考虑到处理的性质，处理者应在可能的情况下采取适当的技术和组织措施协助控制者，并且在必要时，客户应向 海菲秀 提供合理和及时的协助，使其能够回应：（i）数据主体根据适用的数据保护法行使其权利的任何请求（包括访

问权、更正权、反对权、删除权和数据可移植权，视情况适用）；（ii）从数据主体、监管机构或其他第三方收到的与数据处理有关的任何其他通信、请求或投诉。如果直接向客户提出任何此类请求、通信、查询或投诉，客户应及时通知海菲秀 并提供全部详细信息。

1. *评估、咨询和协助*：考虑到处理的性质，如有需要，客户应配合 海菲秀（a）进行任何数据保护或传输影响评估；以及（b）根据适用的数据保护法的要求，在处理之前咨询主管监管机构。
2. *隐私泄露*：如果客户发现隐私泄露，客户应立即通知 海菲秀l 并向 海菲秀 提供合理的信息和配合，以使 海菲秀l 能够遵守适用的数据保护法规定的任何泄露通知义务。客户还应采取合理必要的措施和行动，以减轻数据泄露造成的影响，并了解与数据泄露相关的所有重大进展情况。分包处理者也应遵守上述相同的要求。
3. *数据的删除或归还*：合同终止时，可能会要求客户向 海菲秀 提供关于客户未保留数据的证明。
4. *合规性检查：*客户应允许 海菲秀（或其指定人）检查或审计其程序和文件，以确保遵守本《数据处理协议》中规定的义务。
5. *透明度报告*：海菲秀 不会向任何政府机构披露或提供任何数据的访问权限，除非法律要求提供。海菲秀 处理公共主管部门关于提供数据请求（“法律请求”）的政策，以及 海菲秀 关于法律请求的透明度报告，在 [\*链接\*] 上提供。海菲秀 将：（a）审查法律请求的合法性，并在合法且适当的情况下对法律请求提出质疑；（b）如果法律请求不符合 GDPR 第 46 条规定或关于个人数据合法传输的任何其他规定，其将通知公共主管部门（在上述每种情况下，在法律请求所适用的数据保护法要求的范围内）。

**附件1 - 信息安全控制措施**

1. *安全控制措施*：
2. 海菲秀 实施以下政策和程序以支持其隐私和安全计划：

* 信息安全政策：根据业务要求以及相关法律和法规，为信息安全提供管理指导和支持。
* 信息安全组织：制定一个框架，用于启动和控制 海菲秀 的信息安全实施和运营。
* 人力资源保障：确保所有员工都适合并理解其各自的职位和职责。确保所有员工了解并履行其信息安全责任和义务。确保组织的利益在整个雇佣过程中（包括从雇佣前到雇佣关系终止时）得到保护。确保所有员工都负有保密义务。
* 数据分类：确定 海菲秀 的信息和数据分类，并定义和分配适当的责任以确保数据受到保护。根据信息和数据的敏感度以及对组织的重要性，确保对信息和数据进行适当的保护。防止未经授权披露、修改、删除或破坏存储在媒体上的信息。
* 访问管理：为用户、系统和应用程序访问控制和管理以及用户职责提供框架。限制对信息和信息处理设施的访问。确保仅授权用户有权访问，并防止未经授权访问系统和服务。确保用户负责保护其身份验证信息。防止未经授权访问系统和应用程序。
* 物理和环境安全：防止未经授权物理访问、损坏和干扰 海菲秀 的信息和信息处理设施。防止 海菲秀 资产发生丢失、损坏、失窃或破坏，以及防止其运营中断。
* 操作安全：确保信息和信息处理设施安全运行，防止恶意软件破坏和数据丢失。确保适当记录安全事件。确保维护操作系统的完整性，避免利用技术漏洞。
* 通信安全：制定网络及其相关设施中信息保护的控制措施。确保在 海菲秀 内部和与外部各方传输的信息的安全性。
* 供应商关系：确保供应商可获取的 海菲秀 资产受到保护。根据供应商协议保持商定的信息安全和服务交付水平。
* 信息安全事件管理：确保采用一致且有效的方法管理信息安全事件，包括事件和弱点。
* 用于远程访问的 VPN（虚拟专用网络）：当用户连接到基于 Web 的服务和站点时，为用户增加安全性和匿名性。VPN 隐藏用户的实际公共 IP 地址，并在用户设备和远程服务器之间“秘密传输”流量。
* 静态数据和传输中的数据（也称为动态数据）加密。静态数据是指不在设备或网络之间移动的非活动数据，一般存储在数据档案中。传输中的数据是指在设备或两个网络点之间移动的数据。
* 备份和恢复能力：是一种流程，用于复制数据并将其存储在安全位置以防丢失或损坏，然后将该数据恢复到某个位置（原始位置或安全替代位置），以便可以在操作中再次使用数据。
* 防火墙：是一种网络安全设备，可根据组织此前制定的安全策略监控和过滤传入和传出的网络流量。从最基本的角度来看，防火墙本质上是位于私有内部网络和公共互联网之间的屏障。
* 杀毒软件：是一种用于防止、扫描、检测和删除计算机病毒的软件。
* 多重身份验证（MFA）：是一种安全技术，需要通过独立类别的凭据进行多种身份验证，以验证用户登录或其他交易的身份。
* 邮件安全过滤：是一种流程，用于阻止不需要的或潜在的恶意代码或将用户重定向到可疑网站。它可以防止电子邮件试图进入系统以访问敏感数据。
* 安全意识培训；是组织成员在保护该组织的有形资产，尤其是信息资产方面所拥有的知识和态度。

1. 客户应根据适用的数据保护法采取适当的技术或组织措施，包括防止未经授权或非法处理以及防止意外丢失、破坏或损坏。

**附件二：关于数据处理的详情**

1. *数据主体的类别：*（i）消费者；（ii）授权用户；（iii）客户。
2. *处理的数据类别：*（i）数据主体的联系方式和账户信息，例如全名、电话号码、电子邮件地址、职位和 IP 地址；（ii）治疗历史和表现。
3. *特殊类别的数据：*设备内不会处理任何特殊类别的数据。
4. *处理操作的目的：*为了提供设备服务，将在必要的情况下处理个人数据。处理的个人数据可能会进行以下基本处理活动：收集、通过沟通和咨询进行披露。具体而言，处理操作包括：（i）如果消费者希望创建一个帐户，客户和授权用户则将其详细信息输入设备系统，以便消费者收到短信/电子邮件并完成注册过程。（ii）消费者可以选择向客户和授权用户提供其治疗历史。同样，在使用设备时，客户和授权用户可以选择将其应用帐户与设备同步，以记录提供者的治疗历史。 客户和授权用户将看到关于其提供的治疗服务的汇总治疗数据，并且消费者和授权用户看到的治疗信息不会关联任何消费者的个人身份信息。
5. *处理的持续时间：*个人数据可能会在 海菲秀l Device 服务相关的合同期限内进行处理。