杏树林自称符合HIPAA的书面说明：

杏树林按照 HIPAA 要求执行的数据安全和患者隐私保护规范

V2.2 更新日期 2015 年 1 月 4 日

美国 1996 年颁布的医疗保险携带和责任法案（HIPAA）目的是保护患者隐私和健康有关的电子数据，并且让数据的交换过程尽可能标准化。HIPAA 中非常重要的一块是“安全原则”，包括了技术保障措施及其应用。技术保障在 HIPAA 里是 445 CFR 164.304 定义的：

技术保障是指为了保护和控制电子健康信息使用所采用的所有技术、政策和操作的总和。

HIPAA 的安全原则所定义的技术保障并不要求使用某一项具体的技术，而是一个可调整的框架，要求机构为了保护数据安全，尽可能多地采用适宜的技术。如下所述，这些安全方案需要达到一些标准。杏树林达到甚至超过了这些要求。我们这样做，才能把创新和安全同时提供给医生用户。

入口控制（Access Control）

在 164.304 节中，“入口”的定义如下：

入口指的是对数据/信息进行读取、增写、修改或交换所需要的前提或路径。

而对于入口控制的标准，在 164.312 节中，是如下要求的：

对于信息系统，机构需要采用合适的技术政策和方案，让受保护的健康信息（PHI）只能被某些人或者软件接触到。能够获得入口权力的人和软件在 164.308（a）（4）中有定义。

入口控制是为了让某些合规的用户能够获取数据、应用和文档。HIPAA 安全原则对于入口控制标准的执行细节是如下定义的：

唯一用户身份证明（Unique User Identification）164.312（a）（2）（i）。为验证和追踪用户身份，需要给用户一个唯一的名字或数字。

杏树林给每个用户唯一的身份编号，以便可以使信息传递并能追踪用户行为。每个医生账号都会通过验证码短信下发的手段，和医生的手机号进行绑定，便于杏树林根据需要进行沟通和身份的详细确认。

自动退出 164.312（a）（2）（iii）。用户不活跃状态持续一段时间后系统会自动终止用户的登陆状态。

杏树林网站会根据用户登陆的设备类型决定自动退出的时间长短。在没有操作的情况下，系统设定的自动退出时间为 30 分钟。

加密和解密 164.312（a）（2）（iv）。对于受保护的健康信息（PHI），系统需要有机制对

其进行加密和解密。

为保护敏感的健康信息，杏树林网络中的所有数据都使用了 SSL 协议（Secure Sockets Layer）进行了加密保护。事实上，杏树林在网站的通讯功能上都执行了 https://标准，在有线和无线端都能防止未授权的登陆。对于移动端，我们还会额外使用了公钥加密算法（RSA）对包括姓名、电话、地址等所有受保护健康信息（PHI）实施端到端加密，。

检查控制（Audit Control）

对于检查控制的标准 164.312（b），HIPAA 要求机构必须：
采用硬件、软件和管理方法，记录并检查所有包括或使用受保护健康信息（PHI）的活动。

为保护用户的 PHI 信息的安全，杏树林会记录和检查网络中相关的活动。登陆 log 信息会无限期存储。病历夹每次被使用或编辑的时候，log 信息都会被记录。而且这些 log 信息都完全加密，在紧急情况下能马上恢复。

信息完整（Integrity）

在 HIPAA 里，信息完整是如下定义的 164.304：

信息完整是指数据或信息在未授权的情况下不会被修改或损坏的特性。

信息完整的标准 164.312（c）（1）要求机构必须：

实施合适的政策和方案，确保受保护的健康信息（PHI）不会被随意地修改或损坏。

为了确保信息完整，杏树林使用端到端的 SSL 协议信息加密和解密技术。为了保护信息免遭损坏，杏树林信息完全实时的进行安全存储和备份。登陆查看历史数据本身也会被分别记录和存储。

数据传输安全

数据传输安全标准 164.312（e）（1）要求机构必须：

采用技术安全措施，确保在电子传输过程中，未得到授权的个人无法访问受保护的健康信息（PHI）。

对于传输安全标准的实施，有两条细则：

控制信息的完整 164.312（e）（2）（i）。需要确保在电子传输过程中，受保护的健康信息（PHI）不会在未被监测的情况下被随意修改，除非该信息已经废弃。

加密 164.312（e）（2）（ii）。在所有合适的情况下，采取措施对受保护的健康信息（PHI）进行加密。

杏树林使用 SSL Handshake 协议，对所有网站数据进行了加密，并通过加 2048 位 RSA 加密系统，对移动端的关键信息进行加密，避免无线和有线网络中的非法侵入。

移动设备

杏树林移动应用（ios 和安卓）对应用内的发送的关键信息设置有安全保护。这些信息在杏树林服务器上会加密保存。如果出现移动设备遗失的情况，用户可以通过设置应用开启 PIN 码的方式阻止他人的使用。

总结

在中国，目前在互联网医疗信息的使用上，还没有严格和规范的技术标准和法律法规。很多应用和产品，都没有采取相应的措施，保护患者有关的信息和隐私安全。很多医生用短信、微信或邮件讨论患者资料，都有很大的风险。

杏树林采用美国 HIPAA 标准要求自己，是希望为医生提供一个既方便又安全的临床数据解决方案。我们期待中国立法机关能够早日出台类似 HIPAA 的行业法规，让互联网医疗行业能够更健康有序地发展。

杏树林所采用安全和合规措施总结

- 唯一用户身份证明
- SSL Handshake 协议与 2048 位 RSA 加密
- 不活跃状态下自动退出登录
- 检查控制，保障用户信息不会受到安全违规
- 备份所有网络内的行为信息
- 移动端设置应用开启 PIN 密码

杏树林是在 iPhone、安卓设备和网站上使用的免费应用。对杏树林平台来说，确保 HIPAA 合规和数据安全是我们的首要任务。如果大家有额外的意见、建议或问题，可以通过邮件 support@xingshulin.com 联系我们。