保密承诺书

1. **数据安全保密事项**

为确保信息安全保密事项的有效落实，我司承诺遵守医院的数据安全、软件安全、服务器安全、网络安全、终端设备安全、介质安全、第三方人员管理等信息安全规范。

* 1. **数据安全的内容和范围**
     1. 凡涉及医院信息系统相关的具体信息，包括但不限于信息系统架构和配置、账号密码管理、医疗数据及接入院内测试设备捕获的生产数据。
     2. 未经授权，获取、披露和使用涉及保密内容的行为均属泄密。
  2. **保密的内容和范围**
     1. 涉及医院技术相关具体的信息，包括但不限于医院信息系统保存在相关服务器、终端设备、开发环境等上的技术信息。
     2. 凡未经授权以直接、间接、口头或书面等形式提供涉及保密内容的行为均属泄密。
  3. **权利与义务**
     1. 我司承诺自觉维护医院的利益，严格遵守医院的保密规定；
     2. 我司承诺不得向任何单位和个人泄露所掌握的医院数据秘密事项；
     3. 我司承诺不得利用所掌握的医院数据秘密牟取私利；
     4. 我司了解并承认，通过医院信息系统医院会将业务数据（保密信息）保存于该系统相关院内服务器上，只有在被医院授权情况下可访问数据；
     5. 我司同意并承诺，对所有保密信息予以严格保密，在未得到医院事先许可的情况下不披露给任何其他人士或机构；
     6. 我司应尽可能采取一切必要措施，保证授权使用期间的账号安全，并对账号访问期间的访问轨迹负责。
  4. **本细则项下的保密义务不适用于如下信息：**
     1. 非由于我司的原因已经为公众所知的；
     2. 由于我司以外其他渠道被他人获知的信息，这些渠道并不受保密义务的限制；
     3. 由于法律的适用、法院或其他国家有权机关的要求而披露的信息。
  5. **网络安全的内容和范围** 
     1. 网络系统的硬件、软件及数据均受到保护，禁止破坏、更改、泄露；
     2. 未经授权和审批，不得私自登录设备进行操作；
     3. 通过授权的安全方式登录和操作，过程需得到有效的监管和审计，系统中所有操作留痕，稽查痕迹可查。
  6. **终端安全的内容和范围**
     1. 项目需要部署院内的终端设备需报备，所装的系统符合医院的安全要求；
     2. 未经授权和审批不得私自联入医院内网；
     3. 严格禁止终端设备内、外网同时连接；
     4. 终端因返修或需取回，需信息科报备，经检查后无储存敏感信息的方可离院；
     5. 不得私自安装远程管理软件或开放远程管理端口。
  7. **人员管理安全的内容和范围**
     1. 项目人员仅限使用自己的帐号登录，不得私自使用非个人帐号登录。

1. **我司将严格遵守本承诺书中的各项承诺事项，如有违反，我司赔偿因此给医院造成的全部损失。**

公司/职务：

承诺人签名：

身份证号码：

日期： 年 月 日