宁夏回族自治区

医疗保障局文件

宁医保办发〔2023〕72号

自治区医疗保障局关于印发《宁夏回族自治区医疗保障信息平台定点医药机构接入管理办法（试行）》的通知

各市、县(区)医疗保障局，宁东管委会社会事务局，各定点医药机构:

为进一步加强医保信息平台网络和数据安全管理，规范定点医药机构网络安全接入工作，保证医疗保障业务的稳定、高效运行，我局制定了《宁夏回族自治区医疗保障信息平台定点医药机构接入管理办法（试行）》，并经2023年第11次局长办公会审议通过，现予以印发，请认真遵照执行。

附件：宁夏回族自治区医疗保障信息平台定点医药机构接入管理办法（试行）

自治区医疗保障局

2023年8月25日

（此件公开发布）

宁夏回族自治区医疗保障局办公室　　2022年8月28日印发

附件

宁夏回族自治区医疗保障信息平台定点医药机构接入管理办法（试行）

第一章 总则

第一条 为保障我区医疗保障信息平台网络和数据安全，规范定点医药机构网络安全工作和管理，保证医疗保障业务正常运行，依据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《医疗机构医疗保障定点管理暂行办法》、《零售药店医疗保障定点管理暂行办法》等相关规定，结合宁夏回族自治区医疗保障局（以下简称“自治区医保局”）实际，制定本办法。

第二条 本办法所称网络安全是指信息网络的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，信息服务不中断。

第三条 本办法适用于自治区医疗保障定点医疗机构、定点零售药店（以下简称“定点医药机构”）。

第二章 组织机构

第四条 自治区医保局成立由局党组书记任组长、分管副局长任副组长、信建办全体工作人员为成员的网络安全应急领导小组，全面负责医疗保障信息平台安全管理工作，主要履行以下职责：

（一）负责规划医疗保障信息平台网络安全顶层设计；

（二）研究网络安全管理重大问题;

（三）决策网络安全管理重大事项;

（四）组织、指导、协调、管理地方医保局及定点医药机构的网络安全管理工作

（五）提供必要的技术支撑。

应急领导小组下设应急处置工作组，由相关处室负责人、信息平台技术服务人员组成，负责具体执行应急领导小组的决策、处置突发网络安全事故、及时汇总报告事件处置情况。

各地医保局要参照自治区医保局同步成立网络安全工作领导小组，负责落实自治区医保局相关工作要求，履行对属地定点医药机构管理职责，及时受理、反馈、协调、跟踪、处理突发网络安全事件。

第三章 信息系统接入管理

第五条 定点医药机构应至少配备一名计算机设备和网络的安全运维人员。

第六条 定点医药机构开通医保专网线路需凭借已签订的医保协议至当地运营商自行申请，并将接入医保专网终端计算机的 IP 地址、MAC 地址报送属地医保局进行登记备案。

第七条 定点医药机构在办理医保线路的申请、变更、撤销等手续时需向属地医保局进行备案，同时保留办理线路联网及运营商提供医保线路缴费的相关凭证，随时接受核查。

第八条 定点医药机构须采用在医疗保障经办机构申请备案的 IP 地址接入医疗保障信息平台直接联网结算，原则上一个

定点医药机构只能申请一个医保专网 IP 地址。未经备案的 IP 地址将无法接入医疗保障信息平台进行医保结算。定点医药机构不得使用除运营商之外的任何单位提供的线路接入医疗保障信息平台。定点医药机构向运营商申请医保专网线路服务时，须提供当年医保定点服务协议，运营商进行备案审核，对符合要求的医药机构开通医保专网线路服务时，必须将接入医保专网的计算机终端 MAC 地址与 IP 地址进行绑定。

第九条 不得擅自延伸终端设备连接医疗保障信息平台，不得擅自将不具备医保定点资质的分支机构或其他机构的费用纳入本单位结算。

第十条 使用医保专网的计算机，严禁通过双网卡同时连接互联网或与互联网交替使用。严格管理使用移动存储介质，严禁交叉互用。

第十一条 不得在接入医保网络的计算机上使用、运行来历不明的计算机软件和信息载体。严禁下载、传播和使用黑客软件。

第十二条 对接入专网的计算机定期进行安全漏洞扫描和病毒查杀，及时更新系统补丁程序，禁止将从互联网未经处理的任何数据资料拷贝到专网终端计算机或在专网终端计算机上进行读取操作，防范信息泄露。

第十三条 应加强计算机密码和业务软件口令管理，使用包含大小写字母、数字和符号，长度在 8 位以上的复杂密码，并以 90 天为周期定期更改以保证系统安全。因密码或口令保管不善造成的问题由定点医药机构自行承担。

第十四条 定点医药机构应当自行负责所使用医保网络计

算机的安全防范工作，发现计算机和网络异常时须第一时间断开网络连接，同时向属地医保局报告。

第十五条 定点医药机构更换新系统进行医保刷卡结算或传输存储数据的，须使用国家医疗保障信息平台标准数据接口与宁夏医疗保障信息平台对接。

第十六条 更换的新系统须采用有效的安全管理措施，配备相应的安全设备，将互联网与医保网络进行物理隔离。

第十七条 定点医药机构应当具备完善的信息系统技术和接口标准，实现与医疗保障信息平台有效对接，为参保人员提供直接联网结算。根据提供医药服务的范围，设立相应医保药品、诊疗项目、医疗服务设施等基础数据库，按规定使用国家统一的医保编码。

第十八条 自治区医保局负责监测定点医药机构运行情况。发现定点医药机构接入设备或网络异常时，第一时间切断网络连接，直至整改完毕并得到医保局确认后方可再次接入医保专网。

第十九条 定点医药机构应当按照自治区医保局公布的接口规范对接机构内部信息管理系统。

第二十条 定点医药机构接入医疗保障信息平台流程：

（一）对于新定点的医药机构或需要更换信息系统的定点医药机构需要将自行选择的系统服务商的信息系统的等保测评（至少满足等保三级）证书、医药机构系统接入医疗保障信息平台网络拓扑图、医药机构系统接入医疗保障信息平台网络安全方案、定点医药机构接入医疗保障信息平台数据安全承诺书（承诺书见附件一）以及接入医疗保障信息平台申请表（申报表见附件二）

一并申报至属地医保局，由属地医保局对申报材料进行核实，确保申报材料真实、完整，无误后上报至自治区医保局。

（二）自治区医保局收到申报材料后，5个工作日内组织网络和信息系统方面的技术人员对需要接入医保网络的信息系统拓扑图以及网络安全方面所采取的方案进行验证评估，评估合格后10个工作日内由自治区医保局指定医疗保障信息平台两定接口联调厂商配合申请医药机构系统接入方进行联调测试。联调测试完成后属地医保局、医疗保障信息平台厂商、定点医药机构系统接入方和定点医药机构对测试报告分别加盖公章并报送至自治区医保局（测试报告模板见附件三）。

（三）自治区医保局对报送的测试报告组织相关技术人员进行验证和评估，验证无误后方可接入医疗保障信息平台生产环境。

（四）各定点医药机构在联调测试期间需要确保测试环境和生产环境进行物理隔离，不允许定点医药机构的测试环境数据误接入到医疗保障信息平台的生产环境，若因医药机构原因导致生产环境数据错误或造成医保基金的损失由此产生后果由医药机构自行承担，同时各地医保局按照协议规定可暂停或终止医保结算。

定点零售药店由于信息化力量薄弱，系统部署大多采用的是单机版或云药店模式，网络环境单一，部署简单，为确保医保基金安全，定点零售药店自申请系统对接之日起，各地医保局需暂停协议结算、停止医保基金的拨付，直至定点零售药店更换的系统联调测试完毕，将盖章后的测试报告上报至自治区医保局，收

到上线反馈单后方可开通医保协议（反馈单见附件四）。

宁夏医疗保障信息平台上线后的新定点医药机构或更换信息系统的医药机构均需按照本办法执行，各地医保局摸排清楚底数后督促符合条件的定点医药机构按照本办法要求尽快完成测试联调工作。

第三章 第三方安全管理

第二十一条 各定点医药机构在采购第三方安全服务或自行维护时，如涉及敏感信息应当严格按照规定与服务提供者签订安全保密协议（保密协议见附件五），明确安全和保密义务与责任。

第二十二条 第三方开发、集成和运维单位应当与定点医药机构与属地医保局签署相关知识产权保护协议和保密协议并严格执行，不得将信息系统采用的关键安全技术措施和核心安全功能设计、拓扑结构对外公开，不得对外泄露、传输公民就医、购药等个人隐私数据。提供服务期间，其工作人员应当严格遵守相关安全规定与操作规程。

第二十三条 定点药店第三方系统开发单位、定点医疗机构应当根据等级保护相关规定每年开展一次等保测评，并将测评报告报送至属地医保局备案。

第二十四条 第三方开发单位必须在软件交付前进行安全检测，以发现交付软件中所存在的风险，且对每一次维护提交详细记录和维护报告，维护报告包括业务流程变更、软硬件情况变更，系统故障原因和处理办法等内容。该报告用于留档统计分析

与查阅。

第二十五条 第三方开发单位对信息系统进行维护更新前必须向自治区医保局提交相关申请，对操作内容、影响范围、恢复策略进行说明，在得到自治区医保局同意后才能进行操作。

第二十六条 第三方开发、集成和运维单位应当及时对自治区医保局发现的问题与漏洞进行排查整改，对于整改不及时或拒不整改的，将暂停系统与医疗保障信息平台的对接。

第四章 网络安全事件应急响应

第二十七条 坚持以预防为主、注重时效、快速反应、综合协调、化零为整、组织配合、资源优化为原则，落实网络安全和数据保护工作职责，提升应急管理水平，切实维护基础信息网络、重要信息系统安全，预防和减少网络安全事件造成的损失和危害。

第二十八条 健全完善上下协同的通报预警机制，对于已发生的安全事件，应第一时间封堵漏洞。并按照流程及时上报，事后做好分析、整改和相关环节的完善。

第二十九条 定点医药机构信息系统出现突发网络安全事件时，应立即上报属地医保局，并积极协调相关技术人员实施先期处置，控制事件进一步发展，并做好相应记录，根据事态的发生情况，及时向自治区医保局领导、应急领导小组进行报告。

第三十条 经应急领导小组商议，判定突发事件的等级，并决定启动相应的应急预案。启动应急处置预案后，由应急处置工作组负责具体应急处置工作，并实时报告应急领导小组处置工作

进展及结果，做好相应记录。按照《国家网络安全事件应急预案》相关规定，重大网络安全事件的处理结果需要即时汇报应急领导小组，由组长负责向上级领导和其他机关沟通；较大网络安全事件的处理结果需要在一小时内汇报给应急领导小组，由组长负责向上级领导沟通；一般网络安全事件的处理结果需要在两小时内汇报应急领导小组。

第三十一条 突发事件处置工作结束后，应将相关文件、资料及时归档管理，形成总结报告，配合有关内部审计工作。编写总结报告时应遵循以下原则：

（一）及时性。报告时间应及时，不拖延汇报；

（二）准确性。报告内容客观真实，不主观臆断；

（三）规范性。格式规范，内容清晰有条理。

第三十二条 黑客攻击时的紧急处置措施

（一）系统维护人员发现网页内容被篡改，或有黑客攻击行为时，应立即向上级通报情况，同时进行必要的攻击防护；

（二）首先应将被攻击的服务器等设备从网络中隔离出来，保护现场，同时向应急领导小组汇报情况；

（三）组织协调系统提供厂商和安全厂家对被破坏系统进行恢复与重建工作；

（四）协同有关单位共同追查非法信息来源；

（五）应急领导小组沟通商议后，如认为情况严重，应向上级领导汇报，若上级领导认为有必要，则向有关上级机关、网信部门和公安部门报告。

第三十三条 病毒安全紧急处置措施

（一）当发现计算机感染有病毒后，应立即将该机从网络中隔离出来；

（二）对该设备的硬盘进行数据备份；

（三）启用反病毒软件对该计算机进行杀毒处理，同时进行病毒检测软件对其他机器进行病毒扫描和清除工作；

（四）如发现反病毒软件无法清除该病毒，应立即寻求第三方技术支持并向上级领导报告；

（五）应急领导小组在接到事件通报后，应在三十分钟内启动响应；

（六）经确认确实无法查杀该病毒后，应作好相关记录，同时立即向应急领导小组报告，并迅速联系有关产品商研究解决方案；

（七）应急领导小组沟通商议后，认为情况极为严重，应向上级领导汇报，若上级领导认为有必要，则向上级机关、网信或公安部门报告；

（八）如果感染病毒的设备是服务器或者主机系统，经应急领导小组同意，应立即告知各相关单位做好相应的清查工作。

第三十四条 软件系统遭受破坏性攻击的紧急处置措施

（一）重要的软件系统平时必须存有备份，与软件系统相对应的数据必须有多日备份，并将其保存于安全处；

（二）一旦软件遭到破坏性攻击，系统维护人员应将系统停止运行；

（三）系统维护人员负责软件系统和数据的恢复；

（四）安全和系统维护人员检查日志等资料，确认攻击来源；

（五）应急领导小组沟通商议后，认为情况极为严重的，应及时向上级领导汇报，若上级领导认为有必要，则应向有关上级机关、网信部门和公安部门报警。

第三十五条 数据库安全紧急处置措施

（一）各数据库系统要至少准备两个以上数据库备份，并确保其完整性；

（二）一旦数据库崩溃，应立即向应急领导小组报告，同时通知各单位暂缓上传上报数据；

（三）系统维护人员应对主机系统进行维修，如遇无法解决的问题，立即向软硬件提供商请求支援；

（四）系统修复启动后，将第一个数据库备份取出，按照要求将其恢复到主机系统中；

（五）如因第一个备份损坏，导致数据库无法恢复，则应取出第二套数据库备份加以恢复；

（六）如果两个备份均无法恢复，应立即向有关厂商请求紧急支援。

第五章 责任和处理

第三十六条 任何定点医药机构与个人均须遵守国家有关法律法规，不得利用医保网络和信息系统从事任何违法违规活动，不得在医保信息系统所包含的终端设备、服务器、存储设备及移动介质中，制作、复制、存储、传输和发布对党、国家、政府和人民有害的各种形式的信息。

第三十七条 定点医药机构与所选择的信息系统提供方发生

的任何有关系统知识产权等问题的纠纷，由定点医药机构自行承担。

第三十八条 对工作中出现问题造成不良后果的定点医药机构及人员要通报批评，造成严重后果的要依纪依法问责处理。

第六章 附则

第三十九条 本办法由自治区医保局负责解释。

第四十条 本办法自印发之日起施行。

附件一

自治区医疗保障信息平台
数据安全承诺书

根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《医疗机构医疗保障定点管理暂行办法》、《零售药店医疗保障定点管理暂行办法》等相关规定要求，为确保医疗保障信息平台网络和数据安全、定点医药机构网络安全工作规范和管理、医疗保障业务正常运行，我单位郑重承诺，在与自治区医疗保障信息平台对接时做到以下几点：

一、更换的新系统采用有效的安全管理措施，配备相应的安全设备，将互联网与医保网络进行物理隔离。

二、具备完善的信息系统技术和接口标准，实现与医保信息系统有效对接，为参保人员提供直接联网结算。根据提供医药服务的范围，设立相应医保药品、诊疗项目、医疗服务设施等基础数据库，按规定使用国家统一的医保编码。

三、明确安全责任人，并将责任人信息提交属地医保局备案，确保责任人联系渠道畅通，责任人变动需及时更新备案信息。

四、按照自治区医保局公布的接口规范对接机构内部信息管理系统。

五、相关操作人员已通过安全培训及考核，具备操作能力。

六、妥善保存信息系统、接入医保专网终端、基础数据库的登录账号，并定期修改登录密码。

七、定期对接入专网的计算机更新系统补丁程序，定期对接

入专网的计算机进行安全漏洞扫描和病毒查杀。不拷贝任何从互联网未经处理的数据资料到专网终端计算机或在专网终端计算机上进行读取操作，防范数据泄露。

八、根据定期进行安全扫描结果及时修补漏洞。

九、不延伸终端设备连接医疗保障信息平台，不擅自将不具备医保定点资质的分支机构或其他机构的费用纳入我单位结算。

十、使用医保专网的计算机，不通过双网卡同时连接互联网或与互联网交替使用。严格管理使用移动存储介质，不交叉互用。

十一、不在接入医保网络的计算机上使用、运行来历不明的计算机软件和信息载体。严禁下载、传播和使用黑客软件。

我单位愿意承担以上各项数据安全管理责任，积极配合相关管理部门做好数据安全管理工作，若违反上述承诺导致网络安全事故，我单位自愿承担相应责任和法律后果。

单位负责人（授权委托人）:

单位名称（签章）:

年　月　日

附件二

定点医药机构接入医疗保障信息平台申报表

定点医药机构接入医疗保障信息平台接入申报/反馈表	
1.医药机构信息	
医药机构名称：XXXXXX（国家编码） （签章）	
医药机构地址：XXXX 市 XXXX 县 XXXXXX（详细地址）	
联系人：	联系电话：
申报类型：□新定点　□更换系统	
2.信息系统接入基本信息	
信息系统名称：	
信息系统承建厂商名称：	
信息系统部署模式：　□单机版　□云药店	
联系人：	联系电话：
测试环境（地址、端口）：	
生产环境（地址、端口）：	
信息系统接入具备条件（有一项不满足不予批准）	
1.信息系统已完成医保提供的统一读卡环境的改造工作	
2.信息系统已完成了 15 项标准编码的贯标工作	

3.信息系统已按照贯标要求完成了15项标准编码涉及的页面展示要求
4.完成了医疗保障部门要求的所有接口的改造工作
信息系统承建厂商承诺信息系统已具备接入条件。 （签章）
3.市、县（区）医疗保障机构信息
联系人： 联系电话：
市、县（区）医疗保障部门意见： （盖章）
4.自治区医疗保障局审批意见
网络安全检查意见：
信息系统自检意见：
医保部门接入意见： （盖章）
5.医保信息系统对接厂商信息
医保信息系统对接厂商名称：
联系人： 联系电话：
医保测试环境（地址、端口）：
医保生产环境（地址、端口）：

附件三

定点医药机构接入医疗保障信息平台测试报告模板

1、 必须测试项

使用医疗保障部门的统一的读卡环境且支持各种就诊凭证
涉及 15 项标准编码要求的贯标要求，涉及界面展示以及数据库存储等
信息系统要有体现定点医药机构涉及 15 项标准编码长期贯标要求的相关功能
定点医药机构所涉及就诊类别范围内的接口全部进行充分测试
定点医药机构所涉及医疗类别的场景全覆盖测试
测试过程中约定的其他测试项

2、 测试报告模板

1.身份鉴别

a）应对登录信息系统的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换；

1)应核查用户在登录信息系统时是否采用了身份鉴别措施；

2)应核查用户列表确认用户身份标识是否具有唯一性；

3)应核查用户配置信息或测试验证是否不存在空口令用户；

4)应核查用户鉴别信息是否具有复杂度要求并定期更换。

结果记录

b） 信息系统应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；

1)应核查信息系统是否配置并启用了登录失败处理功能；

2)应核查信息系统是否配置并启用了限制非法登录功能,非法登录达到一定次数后采取特定动作,如账户锁定等；

3)应核查信息系统是否配置并启用了登录连接超时及自动退出功能。

结果记录

c）当进行远程管理时，信息系统应采取必要措施防止鉴别信息在网络传输过程中被窃听；

1)应核查是否采用加密等安全方式对信息系统进行远程管理，防止鉴别信息在网络传输过程中被窃听。

结果记录

d）应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

1)应核查是否采用动态口令、数字证书、生物技术和设备指纹等两种或两种以上组合的鉴别技术对用户身份进行鉴别；

2)应核查其中一种鉴别技术是否使用密码技术来实现。

结果记录

2.访问控制

a）应对登录的用户分配账户和权限；

1)应核查是否为用户分配了账户和权限及相关设置情况；

2)应核查是否已禁用或限制匿名、默认账户的访问权限。

结果记录

b）应重命名或删除默认账户，修改默认账户的默认口令；

1)应核查是否已经重命名默认账户或默认账户已被删除；

2)应核查是否已修改默认账户的默认口令。

结果记录

c）应及时删除或停用多余的、过期的账户，避免共享账户的存在；

1)应核查是否不存在多余或过期账户，管理员用户与账户之间是否一一对

应；

2)应测试验证多余的、过期的账户是否被删除或停用。

结果记录

d）应授予管理用户所需的最小权限，实现管理用户的权限分离；

1)应核查是否进行角色划分；

2)应核查管理用户的权限是否已进行分离；

3)应核查管理用户权限是否为其工作任务所需的最小权限。

结果记录

e）应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；

1)应核查是否由授权主体(如管理用户)负责配置访问控制策略；

2)应核查授权主体是否依据安全策略配置了主体对客体的访问规则；

3)应测试验证用户是否有可越权访问情形。

结果记录

f）访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级；

1)应核查访问控制策略的控制粒度是否达到主体为用户级或进程级,客体为文件、数据库表、记录或字段级。

结果记录

g）应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。

1)应核查是否对主体、客体设置了安全标记；

2)应测试验证是否依据主体、客体安全标记控制主体对客体访问的强制访问控制策略。

结果记录

3. 安全审计

a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；

1)应核查是否开启了安全审计功能；

2)应核查安全审计范围是否覆盖到每个用户；

3)应核查是否对重要的用户行为和重要安全事件进行审计。

结果记录

b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；

1)应核查审计记录信息是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

结果记录

c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；

1)应核查是否采取了保护措施对审计记录进行保护；

2)应核查是否采取技术措施对审计记录进行定期备份，并核查其备份策略。

结果记录

d）应对审计进程进行保护，防止未经授权的中断。

1)应测试验证通过非审计管理员的其他账户来中断审计进程，验证审计进程是否受到保护。

结果记录

4. 入侵防范

a）应遵循最小安装的原则，仅安装需要的组件和应用程序；

1)应核查是否遵循最小安装原则；

2)应核查是否未安装非必要的组件和应用程序。

结果记录

b）应关闭不需要的系统服务、默认共享和高危端口；

1)应核查是否关闭了非必要的系统服务和默认共享；

2)应核查是否不存在非必要的高危端口。

结果记录

c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制；

1)应核查配置文件或参数是否对终端接入范围进行限制。

结果记录

d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求；

1)应核查系统设计文档的内容是否包括数据有效性检验功能的内容或模块；

2)应测试验证是否对人机接口或通信接口输入的内容进行有效性检验。

结果记录

e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞；

1)应通过漏洞扫描、渗透测试等方式核查是否不存在高风险漏洞；

2)应核查是否在经过充分测试评估后及时修补漏洞。

结果记录

f）应能够检测到对重要节点进行入侵的行为，并在发生严重入侵事件时

提供报警。

1)应访谈并核查是否有入侵检测的措施;

2)应核查在发生严重人侵事件时是否提供报警。

结果记录

5.可信验证

a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证,并在应用程序的关键执行环节进行动态可信验证，在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

1)应核查是否基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证;

2)应核查是否在应用程序的关键执行环节进行动态可信验证;

3)应测试验证当检测到计算设备的可信性受到破坏后是否进行报警;

4)应测试验证结果是否以审计记录的形式送至安全管理中心。

结果记录

6.数据完整性

a）应采用校验技术或密码技术保证重要数据在传输过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等;

1）应核查系统设计文档，鉴别数据.重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等在传输过程中是否采用了校验技术或密码技术保证完整性;

2)应测试验证在传输过程中对鉴别数据、重要业务数据、重要审计数据、重要配置数据.重要视频数据和重要个人信息等进行篡改,是否能够检测

到数据在传输过程中的完整性受到破坏并能够及时恢复。

结果记录

b）应采用校验技术或密码技术保证重要数据在存储过程中的完整性，包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

1)应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性;

2)应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性;

3)应测试验证是否对指定的数据进行加密处理。

结果记录

7.数据保密性

a）应采用密码技术保证重要数据在传输过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等;

1)应核查系统设计文档,鉴别数据、重要业务数据和重要个人信息等在传输过程中是否采用密码技术保证保密性;

2)应通过嗅探等方式抓取传输过程中的数据包,鉴别数据、重要业务数据和重要个人信息等在传输过程中是否进行了加密处理。

结果记录

b）应采用密码技术保证重要数据在存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。

1)应核查是否采用密码技术保证鉴别数据、重要业务数据和重要个人信息等在存储过程中的保密性;

2)应核查是否采用技术措施(如数据安全保护系统等)保证鉴别数据、重要

业务数据和重要个人信息等在存储过程中的保密性;

3)应测试验证是否对指定的数据进行加密处理。

结果记录

8.数据备份恢复

a）应提供重要数据的本地数据备份与恢复功能;

1）应核查是否按照备份策略进行本地备份;

2）应核查备份策略设置是否合理、配置是否正确;

3）应核查备份结果是否与备份策略一致;

4)应核查近期恢复测试记录是否能够进行正常的数据恢复。

结果记录

b）应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地;

1)应核查是否提供异地实时备份功能,并通过网络将重要配置数据、重要业务数据实时备份至备份场地。

结果记录

9.剩余信息保护

a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除;

1)应核查相关配置信息或系统设计文档,用户的鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。

结果记录

b）应保证存有敏感数据的存储空间被释放或重新分配前得到完全清除。

1)应核查相关配置信息或系统设计文档,敏感数据所在的存储空间被释放或重新分配给其他用户前是否得到完全清除。

结果记录

10.个人信息保护

a）应仅采集和保存业务必需的用户个人信息；

1)应核查采集的用户个人信息是否是业务应用必需的；

2)应核查是否制定了有关用户个人信息保护的管理制度和流程。

结果记录

b）应禁止未授权访问和非法使用用户个人信息。

1)应核查是否采用技术措施限制对用户个人信息的访问和使用；

2)应核查是否制定了有关用户个人信息保护的管理制度和流程。

结果记录

附件四

定点医药机构接入医疗保障信息平台联调测试结果反馈表

定点医药机构接入医疗保障信息平台联调测试反馈表	
1. 医药机构信息	
医药机构名称：XXXXXX（国家编码）	
医药机构地址：XXXX 市 XXXX 县 XXXXXX（详细地址）	
联系人：	联系电话：
申报类型：□新定点　□更换系统	
2. 信息系统接入基本信息	
信息系统名称：	
信息系统承建厂商名称：	
信息系统部署模式：　□单机版　　□云药店	
联系人：	联系电话：
测试环境（地址、端口）：	
生产环境（地址、端口）：	
3. 联调测试结果反馈	
测试结果：□同意接入　□不同意接入	

反馈意见：
自治区医疗保障局 （盖章） XXXX 年 XX 月 XX 日

附件五

第三方人员安全保密协议

甲方：

地址：

乙方：

地址：

乙方为甲方提供支持服务时，可能直接或间接接触、掌握公民就医、购药等个人隐私数据等保密信息，经甲乙双方平等协商，就乙方在提供支持服务期间及以后保守甲方保密信息的有关事项，达成下列保密协议：

第一条　保密信息

本协议所称的保密信息是指，乙方为甲方提供技术支持服务期间，获得、接触或以其他方式知悉的，带有公民就医、购药等个人隐私数据，不论此种信息以书面、电子或者通过其他介质形式存在，亦不论是在协议签署之前、当时或之后知悉。保密信息的内容包括但不限于：

（一）依据国家法律法规，乙方应保密的秘密信息；

（二）甲方的信息系统采用的关键安全技术措施和核心安全功能设计、拓扑结构等；

（三）甲方未公开的技术文档；

（四）甲方基础设施情况、系统建设情况、安全防护情况等秘密信息。

（五）乙方采集的宁夏医疗保障信息平台、医疗专网上的隐私信息。

（六）乙方在甲方的工作岗位和服务内容。

（七）乙方的技术服务内容等相关内容。

第二条　保密义务

（一）未经甲方同意，乙方不得查阅、复制、留存甲方保密信息或提供用于对接宁夏医疗保障信息平台的任何信息；

（二）未经甲方同意，乙方不得将其以任何方式获得的保密信息带离甲方为其提供的工作场所；

（三）未经甲方同意，乙方不以任何方式向第三方泄漏甲方保密信息；

（四）当乙方不确定某些信息是否为保密信息时，须请示甲方鉴定其保密性质。

（五）约定服务期满后，乙方应主动无条件地将其持有的保密信息移交给甲方或甲方授权人，不得留存任何保密信息。

第三条　保密期限

本协议的保密期限为自乙方首次获得、接触或者知悉甲方保密信息之日起，至该保密信息解密或被甲方书面宣布解密之日止。

第四条　保密信息的返还

服务期满后，乙方应无条件地将其持有的保密信息移交给甲方或甲方授权人。

如果保存保密信息的载体（包括但不限于硬盘、移动硬盘、光盘、U盘、存储卡）属于乙方所有，则应当将甲方的保密信息

从载体上永久删除。

第五条　其他约定

（一）双方违反有关保密规定的，依照《中华人民共和国保密法》等有关法律法规的规定处理。

（二）双方违反本协议规定或数据保管不当，造成损失或后果，甲方将追究乙方责任并要求赔偿；构成犯罪的，由司法机关追究其刑事责任。

（三）本协议是合同不可分割的组成部分，随合同由双方持有，与合同具有同等法律效力。

甲方签字：

年　月　日

乙方签字：

年　月　日