腾讯医疗健康

医学影像云应用及网络安全能力评估白皮书

构建患者为中心安全链接，助力分级诊疗

腾讯医疗健康 | 腾讯研究院 Tencent Research Institute | 腾讯安全云鼎实验室 | 腾讯标准 Tencent Standard

顾问

司晓、吴文达、董志强、杨鹏

腾讯研究院

刘琼、宋扬、翟尤、吴朋阳、王京婕、李南、
管洪博、肖菲、赵子飞

腾讯医疗健康

钱天翼、伍健荣、王小军、陈飞

腾讯云鼎实验室

李滨、张祖优、李鑫、王青龙、杨枭

腾讯标准

梅述家、代威、黄超、刘震宇、张亚军、徐永太

目录

一、医疗数字化进入新阶段，影像云成为分级诊疗重要抓手

1. 医疗数字化不断加快，数据互联互通助力分级诊疗

医疗数字化进程持续推进，为 “健康中国”战略提供新助力

党的十九大将“实施健康中国战略”纳入国家整体发展战略统筹推进，目前健康中国建设已经进入了全面实施阶段。医学科技创新是全力推进健康中国的重点任务之一，通过云计算、大数据、人工智能等新一代信息技术推进医疗数字化进程，助力医疗卫生行业供给侧改革创新，加快优质医疗资源扩容和区域均衡布局是“健康中国”战略实施的重要抓手。其中云平台的搭建将帮助医院提升服务全流程效率；大数据将助力医院及政府部门的精准管理；人工智能将推动医学影像识别、辅助诊断、智能健康管理等进入新的发展阶段。

在今年 3 月发布的“十四五”规划中，提出要聚焦医疗等领域，推动数字化服务普惠应用；推进医院等公共服务机构资源数字化，加大开放共享和应用力度；同时鼓励社会力量参与“互联网 + 公共服务”，创新提供服务模式和产品等内容。在十四五期间，医疗数字化进程将持续推进，推动我国医疗领域的服务模式和产品发生深刻变化，助力健康中国战略的深入实施。

新冠疫情防控成为新常态，带来远程医疗新机遇

目前，疫情防控已成为一种新常态，远程医疗和互联网医疗可以不断赋能疫情防控管理，分担线下医疗就诊压力，优势凸显。国家也不断释放利好政策，接连出台了《国家卫生健康委办公厅关于在疫情防控中做好互联网诊疗咨询服务工作的通知》和《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》，充分肯定了远程医疗和互联网医疗在此次疫情防控中的重要作用。

通过此次疫情防控，也强化了用户远程医疗服务使用习惯，线上挂号、问诊、复诊和医药电商等持续发挥积极作用，数字技术 +“医、药、险”等新应用、新模式不断涌现，远程医疗和互联网医疗快速从大型城市向中小城市渗透。从政策红利的持续释放到用户习惯的改变，再到创新应用的迅速普及，行业迎来新机遇。

医疗改革进入深水区，数据互通进一步推动落实分级诊疗

根据第七次全国人口普查结果，我国 60 岁及以上人口超过 2.6 亿，人口老龄化程度进一步加深，同时伴随人们健康意识的提升，催生了大量医疗需求，加之当前我国存在优质的医疗资源总量相对不足，分布不均衡等问题，更加难以满足快速增长的医疗需求。目前大部分优质医疗卫生资源集中在城市，尤其集中在大中型医院，而医疗需求集中的基层，大量的农村人口仅占较少的医院资源，这导致大量基层患者无法享受优质的医疗资源，医疗服务体系格局和人民群众看病就医的需求之间出现了不适应和不匹配的情况。

建立合理配置医疗资源的分级诊疗体系，推动实现“基层首诊、双向转诊、急慢分治、上下联动”的分级诊疗和就医模式，是新一轮深化医改的重要目标和方向，也是提高医疗资源利用效率，缓解“看病难、看病贵”的重要举措。利用云计算、大数据、人工智能等数字技术助力实现医院之间的数据互联互通、数据高效利用和智能辅诊，构建“医院 – 医生 – 患者”之间的智能数字链接，是实现分级诊疗的重要抓手，而医疗影像打造此链接的重要一环。

2. 影像是医疗重要诊断依据，传统模式亟待改变

医学影像是医疗重要基础支撑，医院现有的数据存储 85% 到 90% 来自影像，影像已成为医疗大数据的主要来源和医疗信息化中应用频度最高的医疗信息。医疗影像也是医疗诊断的重要依据：对于医生来说，影像就是一幅宝贵的生命高清地图，能够让医疗过程更安全、更合理，让医生与医生的沟通与协作、医生与病人的沟通更有效。

传统影像模式及物理医用胶片作为辅助诊断手段发挥了重要作用，但伴随着“互联网 +”时代的来临，已经不能适应医疗数字化中医生对患者影像应用和处理的要求，也严重制约了医疗信息化的发展：主要表现为：

1）患者无法有效管理影像数据：物理胶片相对笨重不方便携带，特别是患者如转院，异地就诊时此缺点尤为突出；同时传统胶片容易发生自然氧化、霉斑，严重影响结果观察，患者难以有效保存、管理自己的医学影像检查资料。

2）医院存储设备投入大：随着检查设备越来越先进，医生对患者的疾病诊断对医学影像处理的功能越来越高，产生的医学影像数据日益剧增，导致医院每年需要投入巨大的资金来建设物理存储设备。而且如果传统的影像存储设备发生宕机而导致患者数据的丢失，对医院带来的影响几乎是灾难性的。

3）基层医疗资源浪费：来自基层医院的患者在转诊到上级医院的过程中，往往由于影像数据跨院调阅困难、导出的数据存储在光盘不易查阅、打印的胶片不清楚等问题，需要进行二次检查。这不仅会增加医疗负担，产生重复浪费，还会使得基层医疗资源无法得到有效利用。

3. 医疗影像云打破信息孤岛，赋能医院 – 医生 – 患者链接

面对传统影像模式存在问题，在医疗数字化浪潮下，各地医院纷纷建设了 PACS（Picture Archiving and Communication Systems，影像归档和通信系统）系统，替代传统模拟医学影像体系，解决了数字医学影像获取、显示、存储、传送和管理的问题，不过在医院之间数据还不能互联互通，形成了医疗影像的“数据孤岛”。而解决医院之间数据孤岛最好路径是利用影像云技术。

医疗影像云是指利用云计算等数字技术，将患者检查的原始 DICOM（Digital Imaging and Communications in Medicine，医学数字成像和通信）影像数据存储至云端，从而支持在互联网条件下通过

手机、电脑等各类终端不限时间、不限地点的数据查询、下载和分享，满足影像调阅、诊断、教学培训等综合应用需求。

医疗影像云是医院信息化服务的新模式，可以打通目前广泛存在于各个医院之间的“信息孤岛”，促进医疗数据互通互联。医疗影像云技术，极大的推动数字医疗影像数据从院内应用向到区域应用发展、从面向医生诊断到兼顾面向患者的个人影像档案管理、由本地存储向云存储迁移，从而实现远程会诊、远程诊断及智能辅助诊断等基于链接的医疗应用，助力分级诊疗的实现。从业务上，医疗影像云覆盖诊断、治疗、康复等关键环节，从链接主体上看，涉及医生、患者、医院等多个主体：

医生：帮助医生提高诊断效率和精度，降低医患矛盾，提高患者满意度，提供更好的医疗服务。
患者：从“牛皮袋 + 胶片”四处跑，到“备份云盘”，同时通过远程咨询诊疗，患者便捷就医，省时省钱，推动以患者为中心的分级诊疗。
医院：推动医院间数据互通，打破信息孤岛；并助力互联网医院的远程医疗、远程会诊等业务。

二、政策红利不断释放，行业已经驶入快车道

1. 政策持续推动影像数据共享和上云，支持措施不断深入细化

近年来国家卫健委及相关部门不断出台相关政策鼓励医学影像诊断信息共享和数据互认，推动远程影像诊断等服务。通过医学影像数据的互联互通，推动“基层首诊、双向转诊、急慢分治、上下联动”的分级诊疗和就医模式。

时间	部门	政策名称	内容
2015 年 9 月	国务院办公厅	关于推进分级诊疗制度建设的指导意见	鼓励二、三级医院向基层医疗卫生机构提供远程会诊、远程病理诊断、远程影像诊断、远程心电图诊断、远程培训等服务，鼓励有条件的地方探索“基层检查、上级诊断”的有效模式。
2016 年 6 月	国务院办公厅	关于促进和规范健康医疗大数据应用发展的指导意见	实施健康中国云服务计划，建设健康医疗服务集成平台，提供远程会诊、远程影像、远程病理、远程心电诊断服务，健全检查检验结果互认共享机制。推进大医院与基层医疗卫生机构、全科医生与专科医生的数据资源共享和业务协同，健全基于互联网、大数据技术的分级诊疗信息系统，延伸放大医疗卫生机构服务能力，有针对性地促进“重心下移、资源下沉”。
2016 年 8 月	原国家卫生计生委	医学影像诊断中心基本标准和管理规范(试行)	在质控的基础上，逐步推进医疗机构与医学影像诊断中心间检查结果互认。鼓励利用信息化手段促进医疗资源纵向流动，由医学影像诊断中心向基层医疗卫生机构提供远程影像诊断等服务。
2017 年 2 月	原国家卫生计生委、中医药管理局	电子病历管理规范 (试行)	医疗机构可以为患者提供全电子化的病历。云胶片作为电子病历组成部分，开始具有合法性。

2018 年 1 月	原国家卫生计生委	关于印发进一步改善医疗服务行动计划（2018-2020 年）的通知	自 2018 年起，医疗机构要建立预约诊疗制度、远程医疗制度、临床路径管理制度、检查检验结果互认制度、医务社工和志愿者制度。医联体牵头医院向医联体内医疗机构提供远程会诊、影像、超声、心电等服务；医联体内实现医学影像、医学检验、病理检查等资料和信息共享，实行检查检验结果互认。
2018 年 4 月	国务院办公厅	促进“互联网 + 医疗健康”发展的意见	鼓励医疗联合体内上级医疗机构借助人工智能等技术手段，面向基层提供远程会诊、远程心电诊断、远程影像诊断等服务，促进医疗联合体内医疗机构间检查检验结果实时查阅、互认共享。
2019 年 3 月	国家卫健委	2019 年深入落实进一步改善医疗服务行动计划重点工作方案	不断完善远程医疗制度，推动远程医疗服务常态化，大力推动结果互认制度，提升检查检验同质化水平，造福患者。在医联体内率先实现医学检验、医学影像、病理检查等资料和信息共享

在国家鼓励政策的引领下，地方相关机构也纷纷颁布配套政策：2018 年以来，辽宁、浙江、贵州、山西、山东等省份相继出台细化政策，将电子胶片纳入收费目录，并确定收费标准，或出台应用规范推广应用。2020 年 12 月，国家卫健委出台政策，明确鼓励通过“云胶片”形式，推动检查资料共享。

时间	部门	政策名称	内容
2018 年 8 月	浙江省物价局、浙江省卫生和计划生育委员会	关于核定数字影像服务费等有关事项的通知	公立医疗机构提供数字影像服务的，省级公立医院的收费标准为每次检查每人最高不超过 20 元，其他公立医疗机构的收费标准在最高标准范围内由各市核定。
2018 年 9 月	辽宁省物价局、卫生和计划生育委员会	关于明确我省综合数字影像服务价格政策有关问题的通知	医疗机构提供综合数字影像服务（包括患者检查所有图像及诊断报告）时，服务费每人每次最高不超过 20 元。
2018 年 11 月	贵州省发展改革委、省卫生计生委、省人力资源社会保障厅	新增医疗服务价格项目 85 项	“医学影像云存储”进入新增医疗服务价格项目
2020 年 9 月	山东省医学影像质控中心	山东省数字胶片服务（云胶片）应用规范	对数字胶片服务（云胶片）的服务流程进行了规范；
2020 年 12 月	国家卫健委	关于进一步规范医疗行为促进合理医疗检查的指导意见	要求医疗机构通过建立检查资料数据库或“云胶片”等形式，推动检查资料共享。

从鼓励医疗影像数据互联互通互认，到把电子胶片作为电子病历组成部分，再到后各级地方政府相继出台收费标准、应用规范等细化政策，无论是国家卫健委还是地方各级机构都在为医疗影像数据共享及上云释放政策红利，这为电子胶片和影像云服务的落地及普及提供了有力的保障。越来越多的省市医疗机构开始试点电子胶片，在先行试点电子胶片服务的医院，患者检查后无需等待报告和影像便可离开医院，报告完成之后，系统推送通知，患者即可通过在线方式检查报告和影像，管理和保存个人影像资料更加便利。

2. 医疗影像云产业快速发展，云服务商及传统厂商各具优势

我国正处于传统医用胶片和电子胶片共存的状态，传统医用胶片占主导，不过电子胶片因其便利性和互联性，未来替代传统胶片是大势所趋。目前医疗影像云总体仍处在初期阶段，不过发展迅速，已经驶入快车道；格局相对分散，各类厂商各具特点和优势，商业模式渐显，仍需继续探索。

根据相关测算，我国电子胶片市场空间巨大，市场规模超过 200 亿人民币，众多厂商纷纷入局提供医疗影像云产品和服务。业内厂商大致可以分为三类，第一类是头部的大型互联网云计算企业或运营商：此类厂商在云计算技术方面比较成熟，一般具有“政务云”或“医务云”等相关云产品，产品安全性、稳定性及运营服务能力客户认可度相对较高。第二类是传统设备厂商：很多也同时是 PACS 厂商，这些厂商对于医疗业务逻辑了解较深，在和医院的长期合作过程中建立了紧密的联系，但自身也面临云化转型升级以满足医疗机构“互联网 +”和数字化需求的问题。第三类是中小型的医疗软件系统厂商：这类厂商多以区域覆盖为主，并多与云服务商进行合作，产品功能相对集中，在系统稳定性和安全防护性能方面需要提升。

3.AI 医学影像正式步入商业化，将成为影像云发展新引擎

AI 影像技术利用深度学习和大数据技术，完成对医学影像的分类、目标检测、图像分割和检索工作，帮助医生进行病变识别、辅助诊断和疗效评估，极大提高医生影像诊断效率和精度。我国 AI 医学影像行业经历了从快速发展、变缓，到正式商业化的起伏。2017 年，国务院发布《新一代人工智能发展规划》，提出要实现智能影像识别，大量创业团队涌入医学影像 AI 领域，行业迅速发展；但由于商业化较为缓慢，初创企业数量在 2018 年达到顶峰，在 2019 年行业有所放缓；2020 年国家药品监督管理局通过 9 项 AI 影像产品的批准，AI 影像正式步入商业化阶段，行业再次迎来春天。

从技术角度，影像云与 AI 影像关系非常紧密，两种应用的发展和普及相辅相成。目前影像云产品大多有 AI 辅诊功能或模块，两者相结合，在原有数据保存和分享基础上，可以为医生和患者提供辅助诊断、影像报告分析等服务，极大的丰富了服务模式，增加了产品的商业价值。随着 AI 影像正式商业化，未来将成为推动影像云发展的新引擎。

三、腾讯觅影 · 影像云，打造以个人为中心的医学影像服务

腾讯觅影 · 影像云以“互联网 + 医学影像”的方式连接医院、医生和患者三方，从而实现影像全流程、全协作化的互联网应用服务。

腾讯觅影 · 影像云面向患者提供个人的医学影像数据管理存储服务。通过腾讯觅影 · 影像云平台、医联体或医共体实现个人影像数据的互联互通。患者可通过一部手机管理个人医学影像档案，并通过微信将影像资料授权分享，为互联网问诊提供便捷服务。医生依托腾讯觅影 · 影像云平台开展院间的远程医疗业务，例如远程诊断、远程会诊；同时，医生可通过 PC 端和移动端企业微信进行远程办公及诊断，例如远程审核报告、远程浏览影像等。

1. 腾讯觅影 · 影像云平台功能及价值

腾讯觅影 · 影像云平台致力于打通上、下级医疗机构之间医疗影像数据的协同共享信息通路，建立健全患者主导的医疗数据共享方式和模式。为患者提供个人健康档案管理服务，以及医疗影像数据在患者知情状况下的授权分享功能。结合互联网医院建设基础，开展线上问诊、远程会诊等服务，创造更好的医疗健康体系，提高检查影像数据使用效率，实现检查影像随身带的效果。主要功能如下：

1）院内设备 /PACS 将影像上传至影像云平台；
2）医生在院内通过前置服务器接入影像云平台，通过 PC 端 / 移动端查看影像，审核、打印报告；
3）医生通过 PC、移动设备（企业微信）查看影像、报告；
4）互联网医院医生通过企业微信接入影像云档案提供在线会诊等服务；
5）患者移动端通过微信小程序方式，能够对接现有互联网医院，方便患者查看影像档案，管理个人医学影像档案；
6）与互联网医院平台集成，实现线上线下一体化管理，有利于医院患者端及医生端医疗健康档案的建立、查阅、存储和在线门诊的融合，方便患者在线就诊及医生在线接诊的需求。

影像云平台通过云端方式打通了医生和患者之间、医院与医院之间、医院与患者之间的信息通路，进一步促进了基于影像数据互联互通的医疗业务发展，主要价值如下：

1）建立互联网医联体影像云平台服务，实现区域间影像检查结果共享、远程诊断、远程会诊、远程教学
通过搭建影像云平台服务，与院内放射影像 PACS/RIS 系统完成对接，实现医疗影像数据的互通上传，并上线患者个人影像档案管理小程序，通过医院互联网医院平台提供患者云胶片调阅及互联网医院在线问诊、会诊等服务，提高居民健康服务获得感。

2）集成云胶片与互联网医院，助力在线问诊业务
通过将患者的个人医学影像档案上传至云端存储，使患者通过手机移动端管理自己的医学影像档案。同时，患者影像档案与互联网医院业务集成，当患者对自己的检查报告有疑问时，患者可直接通过影像云平台向互联网医生发起在线报告咨询服务，并直接授权将自己的影像分享给互联网医院医生，助力互联网在线问诊业务，促进互联网医院的发展。

3）医学影像数据上云安全存储
实现从云基础设施、存储安全、影像云应用的全流程服务，保障医疗数据在云端长期的安全可靠存储、在线调阅。在不影响院内 PACS 系统的前提下，将院内影像数据备份至云端存储，借助影像云灵活扩容、存储安全的特色，避免设备故障导致的数据丢失，降低医院每年在影像存储、重复打印等胶片耗材的投入。

2. 腾讯觅影 · 影像云产品主要应用与存储服务

云 PACS 应用

云 PACS 应用为医院提供云 PACS 功能：帮助医生在云端实现完成院内的影像业务，包括检查管理、查看诊断报告、影像浏览等。具体功能包括登录、检查管理、诊断报告、知识库管理、mini 检查列表、影像浏览等模块。

远程诊断应用

为医联体、不同院间提供远程诊断服务：实现医院之间数据互联互通，以便医院开展远程诊断业务，助力分级诊疗，具体功能包括检查管理、诊断报告、影像浏览、报告知识库、mini 检查列表等模块。

图 1：远程诊断应用

远程会诊应用

提供远程会诊管理服务，包括申请会诊、会议管理等，具体功能包括申请会诊、会诊管理、音视频交流。

图 2：远程会诊应用

基于企业微信的移动影像应用

为医生提供基于企业微信的移动影像应用，包括通过企业微信进行移动诊断和远程会诊，即使医生不在院内，也能通过一部手机完成远程移动诊断业务。具体功能包括移动诊断、远程会诊。

图 3：基于企业微信的移动影像应用

管理中心应用

为每家机构独立提供影像云平台管理中心，供每家机构的管理员访问。管理员在管理中心可以维护本院信息、功能限制、用户权限、数据日志等等。具体功能包括机构管理、科室管理、医生管理、设备管理、部位管理、日志审核等。

患者影像档案应用

为患者提供的面向个人的医学影像档案管理服务，为患者实现一部手机管影像。患者不仅可以查看到自己在觅影影像云的影像和检查结果，也可将其分享给自己的微信好友。此外，患者线下就医时，也可通过面对面展示检查二维码使医生在影像云查看自己的医学影像检查。具体功能包括登录、检查管理、查看报告、影像浏览、分享检查、个人信息管理、家庭成员管理。

图 4：患者影像档案应用

储存服务

在储存服务方面，觅影还提供影像数据的中长期归档、管理、EB 级存储服务，为医疗机构提供高可靠性、高安全性、高可用性的影像大数据即时存储及中长期容灾备份服务。

觅影构建具有医疗可信云认证的 PB 及 EB 级数据存储管理能力的影像云存储服务，并提供 99.9% 的高可靠性数据服务。存储数据格式上，支持国际标准的 DICOM3.0 图像格式，包括标准 DICOM 图像压缩格式、DICOM JPEG2000 图像压缩格式。针对 CT、MR、X 光、乳腺等影像数据特点，以 DICOM 全兼容的无损压缩技术，实现影像大数据的高效编码、压缩，提升数据通信的效率，并采用断点续传技术和云端分布式通信能力，提供高可用影像数据的传输通信能力，并具备 DICOM 网段和图像处理终端物理隔离设计。此外，系统采用分布式存储方案，具有强大的横向扩展能力，可实现多资源池之间数据异地冗余，满足医疗影像信息按照影像数据的生命周期长期存储和备份的需求。

影像云存储后台采用腾讯云的对象存储 COS，对象存储是一种海量、弹性、高可靠、高性价比的对象存储产品，是继云硬盘、文件系统之后的第三种存储形态，是专门针对云计算、大数据和非结构化数据的海量存储形态，通过标准的服务接口，提供非结构化数据（图片、音视频、文本等格式文件）的无限存储服务。COS 同时提供数据安全保障，对象存储通过多层安全防护体系，包括对象存储可用性级别不低于 99.95%；对象持久性级别不低于 99.999999999%；支持不同地域的存储桶进行增量数据拷贝，满足异地容灾、就近访问等需求，保证用户的数据万无。COS 对象存储在技术功能和性能方面，可满足以下需求：

技术名称	指标项	功能要求
对象存储	接口协议	全面兼容标准S3接口，提供基于RESTFul的API操作接口;
	SLA	1、对象存储可用性级别不低于 99.95%； 2、对象持久性级别不低于 99.999999999%（11 个 9）；
	可扩展性	存储规模可自动扩展，不影响对外服务，对用户透明；
	安全管理	1、支持主子账号权限设置、URL 鉴权、白名单、防盗链、临时密钥访问等功能； 2、ACL 至少支持存储桶、对象粒度的访问控制； 3、支持对象数据的客户端加密（SSE-C）和服务端加密（SSE-COS）两种加密方式，保障数据隐私性； 4、支持对象锁定，保障对象不被篡改； 5、访问日志管理：支持记录存储桶的用户访问日志。
	生命周期管理	支持数据生命周期管理，可根据需求自定义到期数据的处理方式：进行批量删除或者转入到低成本存储；
	对象操作	1、每个存储桶下的对象数量不少于 50 亿； 2、对象支持分块上传，单个对象容量上限不小于 1TB； 3、支持对象多副本（不小于 3 副本）； 4、清单功能：支持周期性导出存储桶内的对象列表和详情。
	IO 性能	1、每个存储桶 QPS 不低于 30000 次 / 秒； 2、单次请求读取速率不低于 100Mb/ 秒； 3、首字节延时毫秒级；
	CDN 集成	支持对象存储作为源站，对接 CDN 进行加速分发，支持多家 CDN 厂商回源，不受厂商绑定。
	版本控制	支持保留同名文件的多个历史版本，防止文件误删或者误覆盖。
	跨地域复制	支持不同地域的存储桶进行增量数据拷贝，满足异地容灾、就近访问等需求。

四、腾讯安全助力医疗影像安全能力评估

1. 医疗数据较为敏感，安全成为医疗行业聚焦

目前，传统医疗服务加速向互联网医疗、智慧医疗的新业态转化，医疗行业数字化转型提速医疗数字化的迅猛发展在给人们的就医等带来便利的同时，安全风险也在增加。

医疗数据具有真实性、敏感性、数据覆盖范围广等特点。医疗信息包含了个人的真实姓名、证件号码、就医记录、用药信息等个人高度隐私信息，这使得医疗数据价值极高，一旦泄露会对个人生活、工作等造成较大负面后果。但与医疗信息高价值相对的，却是医疗系统安全防护相对较薄弱的现状。根据中国医院协会信息管理专业委员会（CHIMA）的《2019-2020 年度中国医院

信息化状况调研》，大多数医疗信息系统的信息数据保护措施不够完善。中国信息通信研究院发布的《2020 健康医疗行业网络安全观测报告》也显示，安全漏洞，僵木蠕毒、网站篡改等层出不穷且花样百出的渗透攻击，是医疗行业安全方面面临的主要威胁。

互联网医院较之非互联网医院，一般安全意识更强，在资产脆弱性防护方面相对更好，然而互联网医院在公共互联网上有更多应用服务和数据接口，安全暴露面更大，僵木蠕毒、漏洞风险等很高。总体上，行业面临的安全形势依旧十分严峻，医疗机构须不断升级自己的网络信息安全防护，加固防护系统，保障医疗信息安全。

2. 医疗信息安全法规政策及相关标准不断完善

网络安全方面，2017 年 6 月 1 日，我国正式施行《中华人民共和国网络安全法》，该法律同样适用于医疗健康领域。无论是服务机构的信息拥有者，还是网络运营者，都需要不断加强和完善信息服务体系，重视物理边界或重视具体服务体验，不断增加对运行安全和信息安全、通报机制等投入，不断进行规范化建设。数据安全方面，2021 年 9 月 1 日，我国正式施行《中华人民共和国数据安全法》。《数据安全法》明确了数据管理者和运营者的数据保护责任，指明了数据保护的工作方向，对整个信息安全产业都带来了积极的影响，将为数据管理者和运营者在数据安全建设中提供重要的参考依据，这对促进经济社会信息化健康发展，保护公民、组织的合法权益具有非常大的价值。相关内容和要求也将在医疗健康领域产生积极的影响。个人信息保护方面，我国将于 2021 年 11 月 1 日正式施行《中华人民共和国个人信息保护法》，作为个人信息保护方面的专门立法，《个保法》包含了个人信息保护的基本原则、要求及相关制度。其中，医疗健康信息明确作为敏感个人信息受到法律的严格保护。

面对医院信息安全的风险，医疗领域主管部门也不断颁布相关政策，推动行业安全水平提升。2018 年 4 月，国家卫健委发布《关于印发全国医院信息化建设标准与规范（试行）的通知》，针对网络信息安全，从身份认证、桌面终端安全、移动终端安全、计算安全、通信安全、数据防泄露、可信组网、数据备份与恢复、应用容灾、安全运维等方面提出建设要求。

在远程医疗及互联网诊疗安全方面，2017 年原国家卫计委发布的《远程医疗信息系统技术规范》，从网络结构、网络隔离、网络接入、入侵检测与防御、网络传输、网络安全审计等角度对网络安全做出了规范，同时还从数据采集安全保障、数据存储、数据传输、数据的删除、数据的备份与恢复安全等

角度对数据安全做出了规范。《互联网诊疗管理办法（试行）》的第十三条、《互联网医院管理办法（试行）》的第十五条和《互联网医院基本标准（试行）》的第 4 章节第 5 条，均要求相关的系统需要实施三级网络安全等级保护。今年 6 月国家卫健委发布《互联网医疗健康信息安全管理规范（征求意见稿）》，其中要求互联网医疗健康服务过程中数据存储、传输数据、应用数据和销毁数据应符合 GB/T 35273—2020《信息安全技术个人信息安全规范》、GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》三级网络安全等级保护要求。

针对数据安全，全国信息安全标准化技术委员会发布了 GB/T 39725-2020《信息安全技术 健康医疗数据安全指南》，从分类体系、使用披露、安全措施、安全管理、安全技术等多个维度进行规范。同时，还从八个典型应用场景进行了详细说明，其中包括医生调阅、患者查询和医疗器械等典型场景。

3. 腾讯云鼎实验室制定安全测评规范，助力医疗影像云安全评估

医疗影像云涉及的远程医疗安全相关政策和标准相继发布，有助于行业整体安全建设水平进一步提升。不过行业内各类厂商较多，产品和应用也有差异。如何参考国家相关标准规范，科学的对医疗影像云的应用安全进行评估，成为当下迫切需要解决的问题。因此构建医疗影像云的应用安全测试规范，对于推动树立医疗影像行业标杆，帮助医院选择合适的产品，推定医疗影像领域技术变革具有重要意义。

腾讯安全云鼎实验室专注云安全技术研究和云安全产品创新工作；负责腾讯云安全架构设计、腾讯云安全防护和运营工作；通过攻防对抗、合规审计搭建管控体系，提升腾讯云整体安全能力。同时，基于前沿领域的研究和探索，发现前沿技术中可能存在的安全问题，守护政府及企业的数据、系统、业务安全，运用前沿技术解决安全问题，以紧贴业务安全的最佳实践为产业数字化升级保驾护航。结合安全技术经验和医疗行业对安全的需求，云鼎实验室完成了《远程医疗线上应用服务系统安全测评规范　第 1 部分：渗透测试》，给出了远程医疗线上应用服务安全评测目标及流程、安全测试技术、安全测试基本测试方法等，可以帮助和指导远程医疗线上应用服务相关机构进行信息系统安全测试（评测方法具体见附件一）。

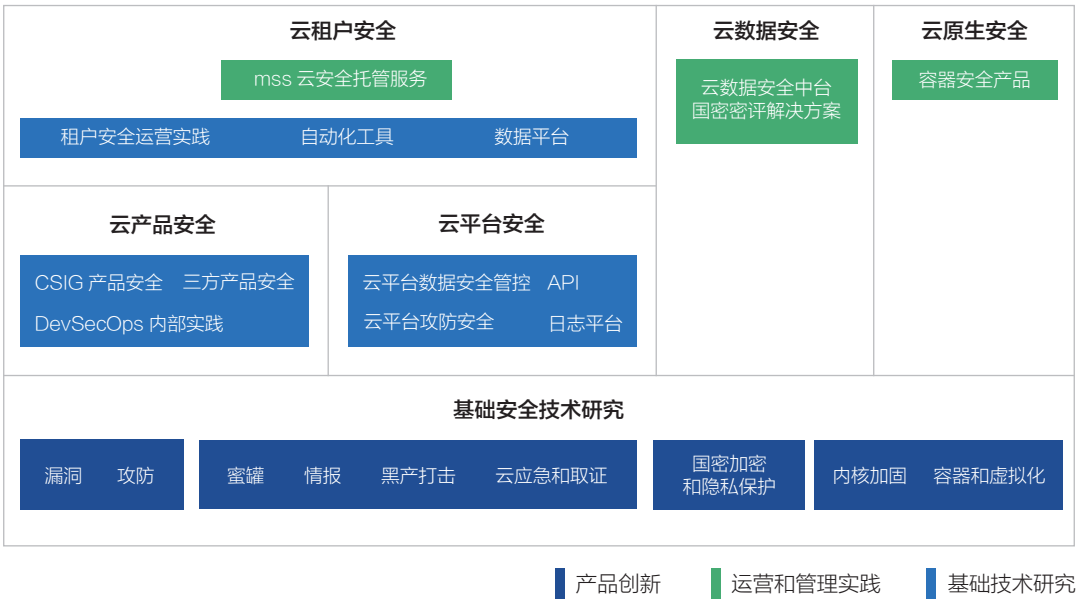

图 5：云鼎实验室能力全景图

安全测试评估原理和方法

远程医疗应用服务安全测试评估，针对三级等保中应用安全部分，采用渗透测试方法，模拟黑客使用的攻击技术和漏洞发现技术，对目标系统进行深入非破坏性质的攻击测试，全面发现系统存在的问题，使管理人员能够直观的通过渗透测试了解系统存在的安全问题。在安全渗透测试中，云鼎实验室利用网络专用安全测试工具，结合工程师丰富的渗透经验，对测试对象进行模拟攻击，将侵入系统、获取敏感信息等等过程和细节进行记录。

远程医疗线上应用服务系统参考架构

远程医疗线上应用服务系统参考架构采用分层架构，主要由数据采集、应用层、服务层、数据层四部分组成。远程医疗线上应用服务系统参考架构的主要层级的相应功能如下：

1）数据采集：对接影像设备及 PACS、RIS 系统；

2）应用层：即最终用于提供基于 Web 方式访问的产品功能；

3）服务层：软件中相对独立的服务模块；

4）数据层：为整个软件提供数据存储和访问服务。

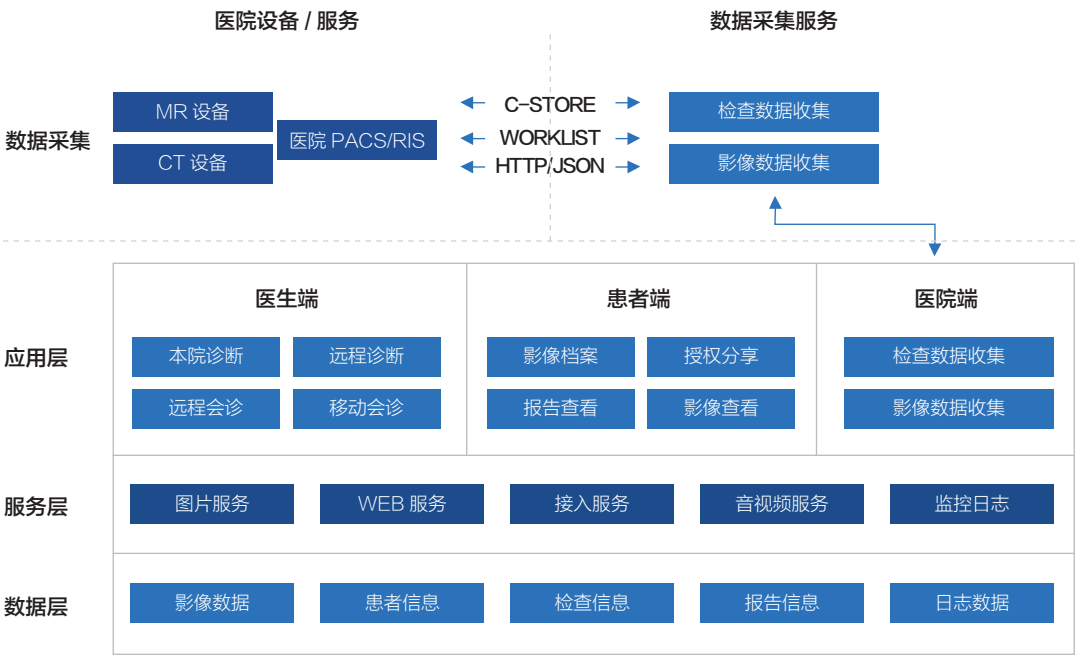

图 6：远程医疗线上应用服务系统参考架构

测试项目

腾讯觅影 · 影像云的测试项涵盖了 14 大类安全风险，共包含 83 个测试项。所涉及的风险面包括：客户端（浏览器）浏览安全、数据传输层、后端服务安全、数据库安全等层面。具体测试项如下表所示：

序号	安全风险	测试项目
1	敏感信息发现测试	使用搜索引擎不应搜索到程序源代码、配置信息、凭据信息等敏感信息
		服务器不应返回版本和类型等指纹信息
		服务器不应存在 robots.txt 文件
		服务器不应存在非标准端口、DNS 域传送
		网页源代码不应存在注释的敏感信息和元数据
		不应存在暴露程序框架 /CMS 类型相关的 HTTP 头信息、Cookie 信息、源代码等
		不应存在暴露其类型和版本相关的信息
		不应返回架构、数据库等相关的信息
2	配置和部署管理测试	网络或基础配置信息不应存在安全漏洞
		平台配置不应存在安全漏洞
		文件扩展处理信息不应存在安全漏洞
		不应存在敏感信息的备份和未引用文件
		基础架构和管理员界面不应存在安全漏洞
		HTTP 请求方法不应存在头部访问控制绕过和 XST 漏洞
		不应存在 HTTP 传输安全漏
		不应存在 RIA 跨域策略安全漏洞
3	报告查询越权测试	不应存在垂直越权漏洞
		不应存在平行越权漏
		应确定指定用户查询的回显内容中不包括当前用户权限所无法查看的内容

4	就诊信息脱敏测试	不应返回未脱敏手机号
		不应返回未脱敏身份证
		不应返回未脱敏地址信息
5	身份鉴别测试	角色定义不应存在安全漏洞
		用户注册的身份要求应符合业务和安全需求;
		账户发放流程不应存在安全漏洞;
		不应存在账户枚举和可猜测的用户账户安全漏洞
		用户名不应猜测
		访问策略和客户 / 培训账户访问权限的应一致性;
		用户注册的身份要求应与业务 / 安全要求一致。
6	身份认证测试	应采用加密通道进行传输
		不应存在默认凭据（默认密码）安全漏洞
		应存在账户锁定机制
		身份验证模式不应存在安全漏洞
		Cookie 不应明文存储密码
		浏览器缓存不应存在安全漏洞;
		不应存在暴力破解密码的安全漏洞
		不应存在弱安全问题 / 答案安全漏洞
		不应存在测试密码更改或重置安全漏洞、CSRF 漏洞等
		不应存在较弱的身份验证安全漏洞

7	访问授权测试	不应存在目录遍历漏洞
		不应存在未授权访问漏洞
		不应存在越权漏洞
		不应存在不安全的直接对象引用
		不应存在文件包含漏洞
8	会话管理测试	不应存在暴力破解会话漏洞
		Cookie 属性中应存在会话过期设置，HttpOnly 属性
		在用户身份验证成功后，不应存在 Cookie 更新安全漏洞
		不应存在重用会话令牌漏洞
		不应存在跨站请求伪造漏洞
		在服务器端和 SSO 注销后不应可以重用会话
		在超时后，所有会话令牌应被销毁或不可用
		会话信息不应该通过 GET 方式传输
9	数据验证测试	不应存在 XSS 漏洞
		HTTP 请求应用具备防篡改能力
		不应存在 HTTP 参数污染漏洞
		不应存在 SQL 注入漏洞
		不应存在 ORM 注入漏洞
		不应存在 XML 注入漏洞
		不应存在 SSI 注入漏洞

		不应存在 XPath 注入漏洞
		不应存在 IMAP/SMTP 注入漏洞
		不应存在代码注入漏洞
		不应存在本地文件包含漏洞
		不应存在远程文件包含漏洞
		不应存在缓冲区溢出漏洞
		不应存在字符串格式化漏洞;
		不应存在拆分 / 走私漏洞
		不应上传意外的文件类型
		不应上传恶意代码
10	异常信息处理不当	在执行出错时，不应回显程序报错信息
		在 HTTP 请求出现异常时，不应回显服务器、中间件报错信息
11	密码安全测试	不应出现在身份验证过程中没有使用 SSL/TLS 或者使用 SSL/TLS 不正确的情况
		不应具备密码填充提示功能
		不应允许通过未加密通道发送敏感信息
12	业务逻辑测试	无效的数据插入后，远程医疗线上应用服务系统能够识别
		应具备伪造请求识别能力
		功能使用次数限制、等待时长限制不应被绕过
		流程步骤应遵循正确顺序，不应被跳过

		应具备针对滥用的防御措施，如账号锁定策略、图形验证码、短信验证码等
13	第三方组件安全测试	第三方组件的使用应符合基础安全配置要求
		第三方组件不应该存在重要未更新补丁
		第三方组件应进行源代码安全分析，确认不存在后门
		第三方组件应使用最新版本或无漏洞版本
		第三方组件更新源应与官方保持一致
14	客户端安全测试	客户端 URL 重定向功能正常
		不应存在 CSS 注入漏洞
		客户端资源操作功能正常
		跨源资源共享功能正常
		不应存在 WebSockets 安全漏洞
		不应存在 Web 消息传递安全漏洞
		不应存在本地存储安全漏洞

渗透测试流程概述

腾讯觅影 · 影像云的渗透测试流程包含：方案制定、信息收集、测试实施、报告输出和安全复查，共 5 个主要流程，对每个流程具体要求如下：

方案制定

确定项目测试事项后，测试方根据系统架构及部署模式等文档，制定合适的渗透测试方案，准备测试工具，并按照该测试方案开展后续工作。

信息收集

收集目标系统的相关信息，包括但不限于：系统域名、系统登录地址、测试账号、开放端口、接口文档等信息。

测试实施

按照已沟通确定的渗透测试方案对目标系统进行渗透测试，在测试过程中及时沟通发生的异常情况，详细记录发现的安全问题，直至渗透测试完成。

报告输出

根据在渗透测试过程中记录的安全问题编写、输出完整的渗透测试报告，并提供对应安全问题的修复建议，将完成的报告发给业务方进行修复。

安全复查

在获知业务方对问题已修复完成的反馈后，测试方需及时进行安全问题的复测，对修复结果进行确认，直至确保所有问题均已修复为止，出具复测报告。

下图是详细的渗透测试流程拆示分解图：

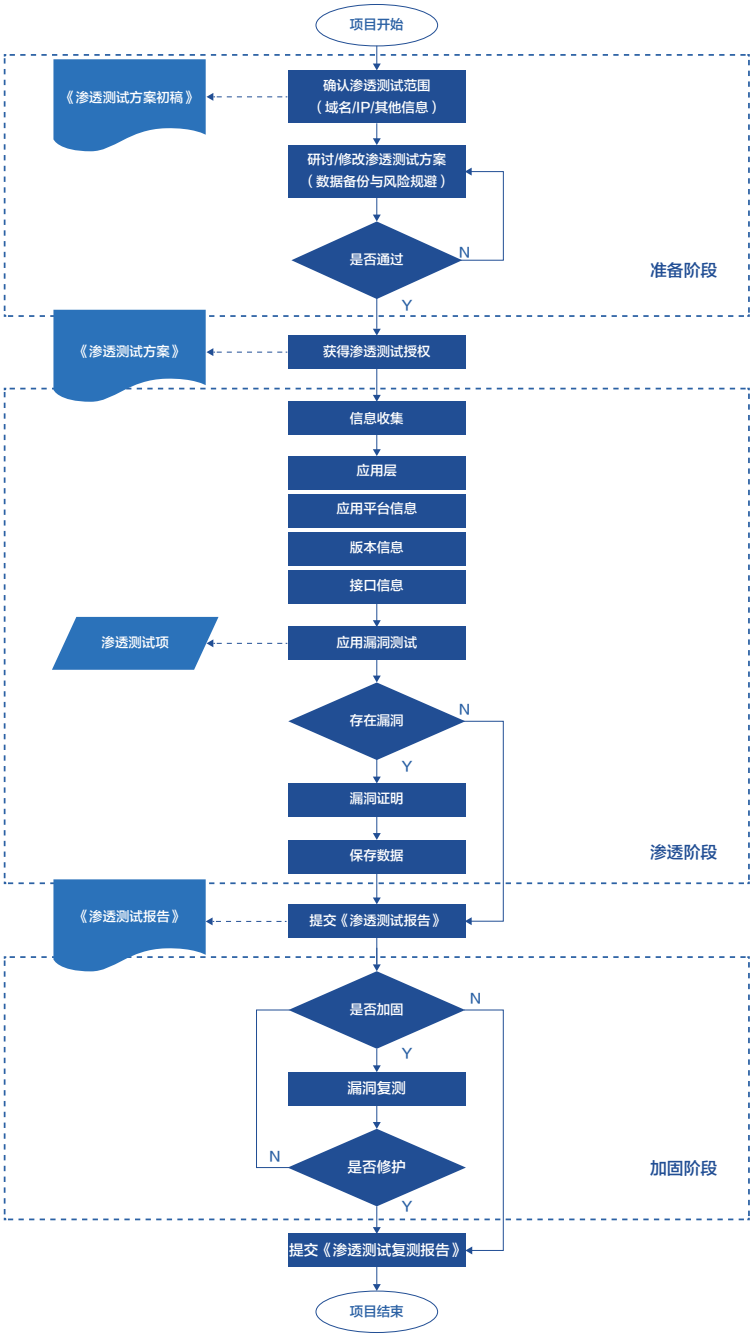

图 6：测试流程图

4. 腾讯觅影 · 影像云渗透测试结果

根据评估标准和方法，对腾讯觅影 · 影像云系统进行渗透测试，本测试主要包括主动模式和被动模式两种。在被动模式中，测试人员尽可能的了解应用逻辑：比如用工具分析所有的 HTTP 请求及响应，以便测试人员掌握应用程序所有的接入点（包括 HTTP 头，参数，cookie 等）；在主动模式中，测试人员试图以黑客的身份来对应用及其系统、后台等进行渗透测试，其可能造成的影响主要是数据破坏、拒绝服务等。测试人员需要先熟悉目标系统，即被动模式下的测试，然后再开展进一步的分析，即主动模式下的测试。主动测试会与被测目标进行直接的数据交互，而被动测试不需要。

本次测试觅影模块如下：

序号	模块名称
1	患者影像档案
2	影像云平台
3	医生移动端
4	影像云管理平台
5	运营平台
6	网关访问的影像云接口
7	DICOM 影像上传工具客户端

本次测试使用系统账号角色如下：

序号	账号角色
1	一般医生
2	主任医师
3	医院管理员
4	医院管理员、运营人员

应用系统风险评级标准：

系统风险评级	漏洞评级说明
严重不安全系统	存在 1 个及以上严重漏洞，或 2 个以上高危漏洞的系统
高危不安全系统	存在 1 个及以上高危漏洞，或 2 个以上中危漏洞的系统
中危不安全系统	存在 1 个及以上中危漏洞，或 2 个以上低危漏洞的系统
安全系统	存在 5 个及内低危漏洞，或不存在漏洞的系统

本次测试发现觅影系统无严重、高危、中危或低危漏洞，因此对腾讯觅影 · 影像云整体安全风险评级为：安全系统，后期需要定期安全检查。

序号	安全风险	测试项目	是否有漏洞
1	敏感信息发现测试	使用搜索引擎不应搜索到程序源代码、配置信息、凭据信息等敏感信息	不涉及
		服务器不应返回版本和类型等指纹信息	不涉及
		服务器不应存在 robots.txt 文件	不涉及
		服务器不应存在非标准端口、DNS 域传送	不涉及
		网页源代码不应存在注释的敏感信息和元数据	不涉及
		不应存在暴露程序框架 /CMS 类型相关的 HTTP 头信息、Cookie 信息、源代码等	不涉及
		不应存在暴露其类型和版本相关的信息	不涉及
		不应返回架构、数据库等相关的信息	不涉及
2	配置和部署管理测试	网络或基础配置信息不应存在安全漏洞	不存在漏洞
		平台配置不应存在安全漏洞	不存在漏洞

		文件扩展处理信息不应存在安全漏洞	不存在漏洞
		不应存在敏感信息的备份和未引用文件	不存在漏洞
		基础架构和管理员界面不应存在安全漏洞	不存在漏洞
		HTTP 请求方法不应存在头部访问控制绕过和 XST 漏洞	不存在漏洞
		不应存在 HTTP 传输安全漏	不存在漏洞
		不应存在 RIA 跨域策略安全漏洞	不存在漏洞
3	报告查询越权测试	不应存在垂直越权漏洞	不存在漏洞
		不应存在平行越权漏	不存在漏洞
		应确定指定用户查询的回显内容中不包括当前用户权限所无法查看的内容	不存在漏洞
4	就诊信息脱敏测试	不应返回未脱敏手机号	不存在漏洞
		不应返回未脱敏身份证	不存在漏洞
		不应返回未脱敏地址信息	不存在漏洞
5	身份鉴别测试	角色定义不应存在安全漏洞	不存在漏洞
		用户注册的身份要求应符合业务和安全需求；	不存在漏洞
		账户发放流程不应存在安全漏洞；	不存在漏洞
		不应存在账户枚举和可猜测的用户账户安全漏洞	不存在漏洞
		用户名不应猜测	不存在漏洞
		访问策略和客户 / 培训账户访问权限的应一致性；	不存在漏洞
		用户注册的身份要求应与业务 / 安全要求一致。	不存在漏洞

6	身份认证测试	应采用加密通道进行传输	不存在漏洞
		不应存在默认凭据（默认密码）安全漏洞	不存在漏洞
		应存在账户锁定机制	不存在漏洞
		身份验证模式不应存在安全漏洞	不存在漏洞
		Cookie 不应明文存储密码	不存在漏洞
		浏览器缓存不应存在安全漏洞；	不存在漏洞
		不应存在暴力破解密码的安全漏洞	不存在漏洞
		不应存在弱安全问题 / 答案安全漏洞	不存在漏洞
		不应存在测试密码更改或重置安全漏洞、CSRF 漏洞等	不存在漏洞
		不应存在较弱的身份验证安全漏洞	不存在漏洞
7	访问授权测试	不应存在目录遍历漏洞	不存在漏洞
		不应存在未授权访问漏洞	不存在漏洞
		不应存在越权漏洞	不存在漏洞
		不应存在不安全的直接对象引用	不存在漏洞
		不应存在文件包含漏洞	不存在漏洞
8	会话管理测试	不应存在暴力破解会话漏洞	不存在漏洞
		Cookie 属性中应存在会话过期设置，HttpOnly 属性	不存在漏洞
		在用户身份验证成功后，不应存在 Cookie 更新安全漏洞	不存在漏洞
		不应存在重用会话令牌漏洞	不存在漏洞
		不应存在跨站请求伪造漏洞	不存在漏洞
		在服务器端和 SSO 注销后不应可以重用会话	不存在漏洞

		在超时后，所有会话令牌应被销毁或不可用	不存在漏洞
		会话信息不应该通过 GET 方式传输	不存在漏洞
9	数据验证测试	不应存在 XSS 漏洞	不存在漏洞
		HTTP 请求应用具备防篡改能力	不存在漏洞
		不应存在 HTTP 参数污染漏洞	不存在漏洞
		不应存在 SQL 注入漏洞	不存在漏洞
		不应存在 ORM 注入漏洞	不存在漏洞
		不应存在 XML 注入漏洞	不存在漏洞
		不应存在 SSI 注入漏洞	不存在漏洞
		不应存在 XPath 注入漏洞	不存在漏洞
		不应存在 IMAP/SMTP 注入漏洞	不存在漏洞
		不应存在代码注入漏洞	不存在漏洞
		不应存在本地文件包含漏洞	不存在漏洞
		不应存在远程文件包含漏洞	不存在漏洞
		不应存在缓冲区溢出漏洞	不存在漏洞
		不应存在字符串格式化漏洞；	不存在漏洞
		不应存在拆分 / 走私漏洞	不存在漏洞
		不应上传意外的文件类型	不存在漏洞
		不应上传恶意代码	不存在漏洞
10	异常信息处理不当	在执行出错时，不应回显程序报错信息	不存在漏洞
		在 HTTP 请求出现异常时，不应回显服务器、中间件报错信息	不存在漏洞

11	密码安全测试	不应出现在身份验证过程中没有使用 SSL/TLS 或者使用 SSL/TLS 不正确的情况	不存在漏洞
		不应具备密码填充提示功能	不存在漏洞
		不应允许通过未加密通道发送敏感信息	不存在漏洞
12	业务逻辑测试	无效的数据插入后，远程医疗线上应用服务系统能够识别	不存在漏洞
		应具备伪造请求识别能力	不存在漏洞
		功能使用次数限制、等待时长限制不应被绕过	不存在漏洞
		流程步骤应遵循正确顺序，不应被跳过	不存在漏洞
		应具备针对滥用的防御措施，如账号锁定策略、图形验证码、短信验证码等	不存在漏洞
13	第三方组件安全测试	第三方组件的使用应符合基础安全配置要求	不存在漏洞
		第三方组件不应该存在重要未更新补丁	不存在漏洞
		第三方组件应进行源代码安全分析，确认不存在后门	不存在漏洞
		第三方组件应使用最新版本或无漏洞版本	不存在漏洞
		第三方组件更新源应与官方保持一致	不存在漏洞
14	客户端安全测试	客户端 URL 重定向功能正常	不存在漏洞
		不应存在 CSS 注入漏洞	不存在漏洞
		客户端资源操作功能正常	不存在漏洞
		跨源资源共享功能正常	不存在漏洞
		不应存在 WebSockets 安全漏洞	不存在漏洞
		不应存在 Web 消息传递安全漏洞	不存在漏洞
		不应存在本地存储安全漏洞	不存在漏洞

五、产业发展建议

1. 鼓励医疗影像上云，助力患者为中心分级诊疗

医疗影像上云可以降低医院耗材成本，推动医院间数据互通互认和数据共享；对于患者可以减少重复检查，节约医疗费用。伴随技术逐渐的成熟和政策的不断推动，目前医疗影像上云时机较为成熟，并已成为行业重要发展趋势。各地应继续落实细化政策，鼓励影像上云，如设立电子胶片设定相关收费标准、将电子胶片纳入医保等。同时相关部门应协同各级医疗机构，共同打造区域医学影像云平台，实现区域医疗影像数据互联互通，构建互认机制，实现共享应用。通过打通医院－患者－医生的链接，推动以患者为中心的 “基层首诊、双向转诊、急慢分治、上下联动”的分级诊疗，提高医疗资源利用效率。

2. 拓展新型应用，孵化建设运营新模式

在新冠疫情防控过程中，数字技术持续赋能，互联网诊疗、远程医疗等医疗数字化应用得到了大规模的检验，新模式、新业态应用得到快速认可和普及。医疗行业应抓住此发展良机，继续推动医疗影像云与 AI、互联网等新一代数字技术融合，拓展产品新形式：如将深度学习技术应用于医学影像的分析，为医生提供智能分析和辅助诊断服务，帮助医生更高效、更准确的发现早期的病灶，提升阅片效率；利用小程序、App 等互联网技术推动以个人为中心的医疗影像数据保存、分享和分析机制，助力个体化的精准治疗。同时应探索“政府 – 企业 – 医院”共同参与的建设运营新形态和商业新模式，保障医疗影像云建设水平及质量，提高医疗影像云服务能力及效率，实现行业良性、可持续发展。

3. 搭建产业联盟，构建合作共赢生态圈

联盟或产业组织等平台对行业的规范、健康有序发展起到重要的引领作用。应积极推动建立医疗影像云产业联盟，通过产业联盟汇聚医疗机构及相关企业、科研单位等，打造合作研发、技术创新、标准制定等领域交流平台，完善产业链协作、促进产业资源有效利用和互惠互利，构建“产、研、学、医”合作共赢的生态圈。

4. 制定安全评估标准和准入门槛，规范行业行为

由于承载大量个人信息，加之医疗影像云使用场景多在互联网环境下，环境复杂且受到多方面安全威胁，安全更应细致完备。建议业内相关组织或机构结合安全政策及标准，推动建立影像云安全测试和评估标准，并积极开展安全检测评估认证工作，进而推动相关企业和厂商加强产品设计研发和运维中的安全意识，落地 DevSecOps 安全流程，实现产品全周期安全。此外，影像数据存档时间周期要求较长，其中门诊病历要求 15 年，住院病历要求 30 年，对企业的技术能力、运营情况、数据保存能力等有一定的要求，需要设置准入门槛，对企业的资质和能力进行规范管理。

附件 1：远程医疗线上应用服务系统安全测评方法

1. 敏感信息发现

测试目的：通过分析远程医疗线上应用服务系统的结构，识别并发现其对外暴露的敏感信息、指纹信息等。

敏感信息发现的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 使用搜索引擎不应搜索到程序源代码、配置信息、凭据信息等敏感信息；

· 服务器不应返回版本和类型等指纹信息；

· 服务器不应存在 robots.txt 文件；

· 服务器不应存在非标准端口、DNS 域传送；

· 网页源代码不应存在注释的敏感信息和元数据；

· 不应存在暴露程序框架 /CMS 类型相关的 HTTP 头信息、Cookie 信息、源代码等；

· 不应存在暴露其类型和版本相关的信息；

· 不应返回架构、数据库等相关的信息

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

2. 配置和部署管理

测试目的：检查远程医疗线上应用服务系统业务在部署、运维、迁移、变更过程中出现的非代码层的安全风险。

配置和部署管理的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 网络或基础配置信息不应存在安全漏洞；

· 平台配置不应存在安全漏洞；

· 文件扩展处理信息不应存在安全漏洞；

· 不应存在敏感信息的备份和未引用文件；

· 基础架构和管理员界面不应存在安全漏洞；

· HTTP 请求方法不应存在头部访问控制绕过和 XST 漏洞；

· 不应存在 HTTP 传输安全漏洞；

· 不应存在 RIA 跨域策略安全漏洞。

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

3. 报告查询越权

测试目的：检查远程医疗线上应用服务系统是否未根据会话上下文对身份权限进行校验。

报告查询越权测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 不应存在垂直越权漏洞；

· 不应存在平行越权漏洞；

· 应确定指定用户查询的回显内容中不包括当前用户权限所无法查看的内容；

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

4. 就诊信息脱敏

测试目的：检查远程医疗线上应用服务系统是否未对就诊信息就行脱敏处理。

就诊信息脱敏测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 不应返回未脱敏手机号；

· 不应返回未脱敏身份证号；

· 不应返回未脱敏地址信息；

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

5. 身份鉴别

测试目的：检查远程医疗线上应用服务系统是否对用户访问身份进行鉴别，是否合理划分角色，鉴别过程是否存在纰漏。

身份管理的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 角色定义不应存在安全漏洞；

· 用户注册的身份要求应符合业务和安全需求；

· 账户发放流程不应存在安全漏洞；

· 不应存在账户枚举和可猜测的用户账户安全漏洞；

· 用户名不应猜测；

· 访问策略和客户 / 培训账户访问权限的应一致性；

· 用户注册的身份要求应与业务 / 安全要求一致。

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

6. 身份认证

测试目的：检查远程医疗线上应用服务系统是否具备身份认证机制，认证过程及会话管理方式是否存在纰漏。

身份认证的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 应采用加密通道进行传输；

· 不应存在默认凭据（默认密码）安全漏洞；

· 应存在账户锁定机制；

· 身份验证模式不应存在安全漏洞；

· Cookie 不应明文存储密码；

· 浏览器缓存不应存在安全漏洞；

· 不应存在暴力破解密码的安全漏洞；

· 不应存在弱安全问题 / 答案安全漏洞；

· 不应存在测试密码更改或重置安全漏洞、CSRF 漏洞等；

· 不应存在较弱的身份验证安全漏洞。

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

7. 访问授权

测试目的：检查远程医疗线上应用服务系统对程序目录、文件的访问，是否进行授权验证。

访问授权的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 不应存在目录遍历漏洞；

· 不应存在未授权访问漏洞；

· 不应存在越权漏洞；

· 不应存在不安全的直接对象引用；

· 不应存在文件包含漏洞；

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

8. 会话管理

测试目的：检查远程医疗线上应用服务系统在用户的整个计算机交互的过程中，是否全程保护好用户会话。

会话管理的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 不应存在暴力破解会话漏洞；

· Cookie 属性中应存在会话过期设置，HttpOnly 属性；

· 在用户身份验证成功后，不应存在 Cookie 更新安全漏洞；

· 不应存在重用会话令牌漏洞；

· 不应存在跨站请求伪造漏洞；

· 在服务器端和 SSO 注销后不应可以重用会话；

· 在超时后，所有会话令牌应被销毁或不可用；

· 会话信息不应该通过 GET 方式传输。

2）预期结果：

远程医疗线上应用服务系统务应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

9. 输入验证

测试目的：检查远程医疗线上应用服务系统表单对于用户输入内容是否做合法性判断，是否可以通过输入非法注入语句获得超预期内容。数据验证的测试评价方法如下：

1）测试步骤：

数据验证的测试评价方法如下：

· 不应存在 XSS 漏洞；

· HTTP 请求应用具备防篡改能力；

· 不应存在 HTTP 参数污染漏洞；

· 不应存在 SQL 注入漏洞；

· 不应存在 ORM 注入漏洞；

· 不应存在 XML 注入漏洞；

· 不应存在 SSI 注入漏洞；

· 不应存在 XPath 注入漏洞；

· 不应存在 IMAP/SMTP 注入漏洞；

· 不应存在代码注入漏洞；

· 不应存在本地文件包含漏洞；

· 不应存在远程文件包含漏洞；

· 不应存在缓冲区溢出漏洞；

· 不应存在字符串格式化漏洞；

· 不应存在拆分 / 走私漏洞；

· 不应上传意外的文件类型；

· 不应上传恶意代码。

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

10. 异常信息处理不当

测试目的：检查远程医疗线上应用服务系统是否合理处置程序异常信息，是否存在直接将错误代码、调试信息、后台数据输出到到前端的情况。

异常信息处理不当的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 在执行出错时，不应回显程序报错信息；

· 在 HTTP 请求出现异常时，不应回显服务器、中间件报错信息。

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

11. 密码安全

测试目的：检查远程医疗线上应用服务系统在密码的使用过程中是否遵循保密原则。

密码安全的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 不应出现在身份验证过程中没有使用 SSL/TLS 或者使用 SSL/TLS 不正确的情况；

· 不应具备密码填充提示功能；

· 不应允许通过未加密通道发送敏感信息。

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

12. 业务逻辑

测试目的：检查远程医疗线上应用服务系统在业务功能执行顺序、活动策略、执行次数等方面是否严格依照业务原有逻辑来执行。

业务逻辑的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 无效的数据插入后，远程医疗线上应用服务系统能够识别；

· 应具备伪造请求识别能力；

· 功能使用次数限制、等待时长限制不应被绕过；

· 流程步骤应遵循正确顺序，不应被跳过；

· 应具备针对滥用的防御措施，如账号锁定策略、图形验证码、短信验证码等；

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

13. 第三方组件安全

测试目的：检查远程医疗线上应用服务系统是否使用了第三方组件，如使用了必须严格审查组件安全性，避免第三方组件带来安全风险。

第三方组件安全测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 第三方组件的使用应符合基础安全配置要求；

· 第三方组件不应该存在重要未更新补丁；

· 第三方组件应进行源代码安全分析，确认不存在后门；

· 第三方组件应使用最新版本或无漏洞版本；

· 第三方组件更新源应与官方保持一致。

2）预期结果：

第三方组件应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

14. 客户端安全

测试目的：检查远程医疗线上应用服务系统在用户浏览器端的安全性，避免应用前端漏洞导致的钓鱼、凭证窃取、敏感信息泄漏等问题。

浏览器安全的测试评价方法如下：

1）测试步骤：

依次测试远程医疗线上应用服务系统是否满足如下要求：

· 客户端 URL 重定向功能正常；

· 不应存在 CSS 注入漏洞；

· 客户端资源操作功能正常；

· 跨源资源共享功能正常；

· 不应存在 WebSockets 安全漏洞；

· 不应存在 Web 消息传递安全漏洞；

· 不应存在本地存储安全漏洞。

2）预期结果：

远程医疗线上应用服务系统应满足上述要求。

3）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

腾讯医疗健康

医学影像云应用及网络安全能力评估白皮书
P/N：THMY-20210930-50P
官网邮箱：miying@tencent.com