“先收集后解密”正在威胁医疗数据安全，如何应对量子威胁？

2026 年 4 月 22 日

第 30 届中国医院信息网络大会（CHIMA 2026）将于 2026 年 4 月 23 日至 26 日在珠海国际会展中心举办。本届大会以“传承、创新、发展”为主题，汇聚全国医疗信息化精英，聚焦 AI 应用、智慧医院、数据安全、数字化转型等核心议题。在数据安全议题中，有一个正在加速逼近、但尚未被行业广泛重视的风险是“先收集后解密”攻击对医疗数据的量子时代安全威胁。本文将结合现行政策法规，论述医疗数据保护的唯一正确技术路径：国密 TLS 1.3 + 国密混合后量子密码（PQC）HTTPS 加密。

一、现状与问题：一个被忽视的医疗数据“时间炸弹”

1. HTTPS 加密普及严重不足

我国医院网站和医疗管理系统 HTTPS 加密普及率长期偏低。许多医院官网和业务系统仍以明文 HTTP 方式提供服务，患者问诊记录、检验报告、远程会诊视频流等敏感医疗数据在公网传输中“裸奔”。部分已完成 HTTPS 加密的系统，其 SSL 证书管理仍依赖人工操作，包括人工采购证书、手动安装、定期续期，面对已经到来的证书有效期大幅缩短，人工证书管理已不可持续。这在根本上阻碍了 HTTPS 加密在医疗行业的大规模普及应用。

2. “先收集后解密”攻击已经开始

量子威胁并非遥远的科幻情节。权威预测显示，2030 年代初，量子计算机或将具备全面破解传统密码算法的能力。更值得警惕的是，“先收集后解密”已成为现实安全威胁：攻击者已开始提前收集保存加密流量和数据，待量子计算机足够强大时再行破解。医疗数据，尤其是患者的病历、诊断记录、基因信息等，因其极高的隐私价值和终身敏感性（病历保存 30 年以上，基因数据跨越代际），一旦在当前被窃取，将对患者未来造成不可估量的长期风险。这正是国际密码学界持续警告的“Q-Day”威胁，当量子计算机成熟之日，就是所有传统密码算法加密的数据失效之时。

3. 数字签名的量子安全缺口

除了 HTTPS 加密通道，医疗报告数字签名的量子安全风险更为隐蔽但影响深远。电子病历、诊断报告等医疗文书依赖数字签名保障其法律效力、完整性和不可否认性。然而，包括 SM2 在内的所有公钥密码算法，在未来的量子计算机面前都将被攻破。今天签发的电子病历，20 年后仍需验证其真实性，但如果当前的数字签名届时被攻破，这些医疗文书的法律效力将荡然无存。医疗机构必须在量子计算机成熟之前，确保历史签名仍能被可信验证，这就要求迁移到抗量子签名算法。

二、政策法规解读：医疗数据加密保护的“合规密码”

1. 法律层级的刚性要求

《密码法》明确要求关键信息基础设施必须使用商用密码进行保护并定期开展商用密码应用安全性评估（密评）。《数据安全法》《个人信息保护法》进一步规定了数据处理活动的安全保障义务。这三部法律构成了医疗数据安全保护的顶层法律框架。国家卫健委等三部门联合印发的《医疗卫生机构网络安全管理办法》（国卫规划发〔2022〕29 号）则将法律要求落实到了行业层面，要求医疗卫生机构在网络建设过程中“同步规划、同步建设、同步运行”网络安全保护措施，充分落实《密码法》等有关法律法规和密码应用相关标准规范的要求。

2. 数据安全新规强化加密要求

2026 年 2 月 14 日，国家卫生健康委会同公安部、国家网信办等部门联合印发《医疗卫生机构数据安全和个人信息保护管理办法（试行）》（国卫规划发〔2026〕6 号），标志着医疗数据安全进入“严监管、强处罚”新纪元。该《办法》要求医疗卫生机构在数据全生命周期中“针对不同场景综合运用加密、鉴权、认证、脱敏、去标识化、数字水印、校验、审计等技术手段进行安全保护”。这实质上是将加密保护从“建议性”上升为“强制性”要求，而数据传输加密，是所有医疗数据处理活动的前提保障措施。

3. 密评：将密码应用要求变为“通行证”

法律法规的顶层设计最终要通过国家标准落地。GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》是医疗系统开展密评的核心依据，从物理和环境、网络和通信、设备和计算、应用和数据安全四个层面规定了密码应用要求。其中，“网络和通信安全”层面明确要求信息系统在通信过程中必须采用密码技术对数据进行机密性和完整性保护。

更为关键的是，密评结果已与医院资质直接挂钩。**《三级医院评审标准（2025 版）》已将密**

评结果设为信息化的“前置否决项”，未通过密评的系统无法参与评审数据采集，直接影响三甲资质申报。这意味着，密评不再是“做不做都行”的软性要求，而是医疗机构信息化的“通行证”。没有通过密评，医院信息系统就无法投入使用，直接影响医疗服务正常运行。

三、政策解读的核心结论：为什么必须是国密 TLS 1.3？

1. “要求加密”不等于“加密就是安全的”

上述政策法规明确要求数据传输必须加密、必须使用国密算法、必须通过密评。然而，从技术要求到真正保障数据安全，中间存在一个关键的认知断层：

“要求加密”只是对安全结果的形式约束，并不等于“选择了哪种加密方案就能保障数据安全”。

换言之，医疗机构为了通过密评，可以在技术上选择多种实现方案，但不同方案所能达到的安全保障效果天差地别。政策法规不会也不可能指定具体协议版本或技术细节，这是行业标准和技术创新共同解决的问题。因此，各家医院在开展密改工作时，必须自行判断什么才是真正能保障医疗数据安全的正确技术路径。

2. 传统密改方案的根本缺陷：TLCP 不支持前向安全

当前市场上广泛使用的传统国密 HTTPS 加密方案，基于 TLCP 协议（国密 TLS 1.2，对应国家标准 GB/T 38636-2020《信息安全技术 传输层密码协议》）。TLCP 在密钥交换阶段主要采用静态密钥交换方式，服务器的加密证书私钥被直接用于加密会话密钥。这意味着：

(1) 如果攻击者记录了某段加密会话的全部流量

(2) 后来（可能是任何时候）获取了 SSL 证书的私钥

(3) 攻击者就可以用这个私钥解密过去记录的所有会话数据

这恰恰是 TLCP 的核心安全缺陷，**不支持前向安全**。前向安全机制的核心价值在于：每一段会话都使用临时生成的一次性密钥，会话结束后立即销毁，即使未来私钥泄露，过去的所有加密会话数据也无法被解密。

对于病历保存 30 年以上的医疗数据而言，TLCP 的这一缺陷是根本性的，服务器上的证书私钥极有可能保管不善而被泄露，特别是现在常用的通配证书从证书申请到部署经过了多人多途径的流转，泄露风险极高。一旦泄露，过去所有加密的患者数据将全部暴露。

3. 为什么通过密评不等于数据安全得到保障？

这里需要澄清一个容易被误解的关系：**通过密评，只是证明信息系统在测评时点满足了 GB/T 39786-2021 的形式要求，并不等同于数据在长达数十年的生命周期中得到了真正的安全保障。**

密评关注的是合规性，是否采用了国密算法？是否部署了国密 SSL 证书？是否具备加密通信能力？这些问题都能得到“是/否”的答案。但密评并不测试“如果服务器私钥泄露，过去的数据能否被解密”，这不是密评的测评范围，而是密码协议设计层面的安全属性。因此，一个基于 TLCP 的国密改造方案完全有可能通过密评三级评估，但其医疗数据在未来长达 30 年的保存周期中，始终面临着私钥泄露导致历史数据被批量解密的安全风险。

这就是为什么医疗机构在开展密改工作时，不能仅仅以“通过密评”为唯一目标，而必须深入理解不同技术方案的内在安全属性差异，真正从保护自己医院的医疗数据长期安全出发，认真评估密改方案。

4. 国密 TLS 1.3：强制前向安全的唯一选择

2021 年 3 月，国际标准组织 IETF 正式发布 **RFC 8998：ShangMi (SM) Cipher Suites for TLS 1.3**，将国密算法正式纳入 TLS 1.3 协议的国际标准体系。与 TLCP 不同，TLS 1.3 协议从设计之初就强制所有密钥交换算法都必须支持前向安全。在 RFC 8998 定义的国密 TLS 1.3 中：

(1) 每一段会话都使用临时生成的密钥对进行密钥交换

(2) 会话密钥不与服务器上的加密证书私钥绑定

(3) 会话结束后临时密钥立即销毁

(4) **即使未来私钥泄露，过去的所有加密会话数据也无法被解密**

基于国密 TLS 1.3 的 HTTPS 加密，是当前满足密评合规要求的同时，真正保障医疗数据长期安全的唯一正确技术路线。任何基于 TLCP 的改造方案，无论是否通过密评，都无法提供同等水平的医疗数据长期安全保障。

四、量子安全：国密合规之后的下一道必答题

1. 国密算法同样不抗量子攻击

当前医疗行业正在推进的国密改造，主要基于 SM2/SM3/SM4 算法体系。但国际密码学界

已达成共识：**包括 SM2 在内的所有公钥密码算法，在量子计算机面前都同样脆弱**。与 RSA、ECC 一样，SM2 的安全性也依赖椭圆曲线离散对数问题的计算复杂性，而量子计算机的 Shor 算法可以在多项式时间内破解这些问题。

这意味着：即使医院今天按照 GB/T 39786-2021 要求完成了国密改造并顺利通过密评，其核心医疗数据在未来量子计算机面前将是**明文**状态，攻击者现在就正在收集当前的加密流量，待量子计算机成熟后一次性破解所有历史医疗数据。

2. 国际进展：全球医疗行业已加速 PQC 迁移

国际后量子密码迁移已进入实质性部署阶段。2024 年 8 月，NIST 发布了首批三项 PQC 标准：FIPS 203（ML-KEM 密钥封装）、FIPS 204（ML-DSA 数字签名）和 FIPS 205（SLH-DSA 数字签名）。2025 年 9 月，NIST 进一步发布 PQC 迁移路线图白皮书草案，明确警告：迁移到后量子密码将需要数年时间，必须立即开始行动。全球超过 68%的互联网流量已启用后量子密码 HTTPS 加密，标志着 PQC 的大规模部署已经进入快车道。

在医疗行业，相关美国公司正在开发基于 PQC 的电子健康记录和电子病历系统，计划于 2027 年中完成全球部署。英国 NCSC 于 2025 年 3 月发布 PQC 迁移指南，明确要求 NHS 优先保护患者数据，设定三步走路线图，在 2028 至 2032 年间实现量子安全医疗记录。

我国也已迈出重要一步。2025 年 2 月，商用密码标准研究院启动了新一代商用密码算法全球征集活动（NGCC），算法提案提交截止时间为 2026 年 6 月 30 日，正式迈出国密 PQC 标准化的重要步伐。

五、唯一的正确路径：国密混合 PQC

面对上述双重挑战：前向安全缺失（TLCP 的固有缺陷）与量子计算威胁（所有公钥算法的共同危机），我国医疗行业需要一条既满足当前国密合规要求，又为量子时代做好充分准备的技术路径。

1. 为什么国密混合 PQC 是唯一的正确选择？

国密混合 PQC 方案，即“国密 SM2 + 国际 PQC 算法 MLKEM768”的混合加密方案，由我国密码团队主导提出，被国际互联网号码分配机构（IANA）正式授予官方编号 4590，标志着这一融合方案已纳入全球互联网的基础协议体系。该方案建立在国密 TLS 1.3（RFC 8998）之上，具备三重无可替代的核心优势：

优势一：强制前向安全。 基于国密 TLS 1.3 协议，每一段会话使用临时密钥，即使未来私

钥泄露，过去的所有加密历史数据也无法被解密。这从根本上解决了 TLCP 方案的根本性安全缺陷。

优势二：国密合规无忧。 使用 SM2/SM3/SM4 国密算法和国密 SSL 证书，完全满足 GB/T 39786-2021 对信息系统密码应用的要求，可顺利通过密评三级评估。

优势三：立即获得量子安全。同时融合国际 PQC 算法 MLKEM768，今天部署即可有效防御“先收集后解密”攻击，保障医疗数据在量子时代的持续安全。待我国正式发布纯国产 PQC 算法后，可通过在线升级无缝完成迁移，无需二次采购和部署。

2. 国密混合 PQC vs. 其他方案的根本差异

我们来对比一下各种密改技术方案，如下表所示，前四种方案都至少在一个关键维度上存在短板。明文 HTTP 直接违反法规要求；TLCP 虽能通过密评但缺乏前向安全和量子安全；纯国密 TLS 1.3 解决了前向安全问题，但仍无法抵御量子攻击；国际混合 PQC 不支持国密无法通过密评。**只有国密混合 PQC 方案，同时满足密评合规、前向安全和量子安全三重保障，是真正能保障医疗数据在现在和量子时代持续安全的唯一选择。**

方案对比	合规(密评)	前向安全	量子安全	长期数据安全保障
明文HTTP	✗	✗	✗	✗
TLCP 国密	✓	✗	✗	✗
TLS 1.3 国密	✓	✓	✗	✗
国际混合 PQC	✗	✓	✓	✓
国密混合 PQC	✓	✓	✓	✓

六、零信技术的解决方案

面对上述挑战，零信技术提供了一套端云一体的完整解决方案，以一台网关实现从国密合规到后量子安全的平滑升级。

1. 国密混合 PQC HTTPS 加密：成熟方案，马上落地

零信 HTTPS 加密自动化网关兼容 TLCP 国家标准、基于国密 TLS 1.3（RFC 8998）标准，已完整支持国际混合 PQC 算法 X25519MLKEM768 和国密混合 PQC 算法 SM2MLKEM768。

网关支持高性能 HTTPS 加密卸载和流量清洗，支持反向代理部署，让原医院管理系统 Web 服务器零改造即可实现 HTTPS 加密。网关自动完成双算法 SSL 证书（国密 OV + 国际 DV）的申请、验证、部署和续期，即使证书有效期缩短至 47 天，也能实现 5 年零人工干预。

零信 HTTPS 加密自动化网关 HTTPS 加密支持自适应加密算法，常用的国际浏览器采用国际混合 PQC 算法，是抗量子的；其他国密浏览器采用 TLCP 国密算法，仅满足国密合规要求。目前只有零信浏览器优先采用 SM2MLKEM768 实现国密混合 PQC 加密，不仅满足国密合规要求，而且确保用户访问医疗数据能获得量子安全的加密通道。

2. 一次投资，储备多重战略价值

部署零信国密混合 PQC HTTPS 加密方案，医疗机构将同时获得三重核心价值：

第一重：满足密评合规要求。方案兼容支持 TLCP 方案，并基于国密 TLS 1.3 协议，使用 SM2/SM3/SM4 国密算法和国密 OV SSL 证书，完全满足 GB/T 39786-2021 对信息系统密码应用的要求，可顺利通过密评三级评估，满足《三级医院评审标准（2025 版）》的前置性要求。

第二重：实现真正的医疗数据安全。方案强制前向安全，每一段会话使用临时密钥，即使未来私钥泄露，过去的所有加密会话数据也无法被解密。这从根本上解决了传统国密方案（TLCP）的核心安全缺陷。

第三重：量子安全就绪。方案采用国密混合 PQC 算法 SM2MLKEM768，立即获得抗量子能力，有效防御“先收集后解密”攻击，保障医疗数据在量子时代的持续安全。待我国正式发布纯国产 PQC 算法后，可通过免费在线升级无缝完成迁移，无需二次采购和部署。

3. 端到端安全闭环

零信技术提供从云端到服务器端的证书自动化管理，再从用户端到服务端的国密混合 PQC 加密的全链路安全闭环。免费配套提供基于 Chrome 内核、支持 RSA/ECC/SM2/PQC 四算法的高性能的零信浏览器，优先采用国密混合 PQC 算法安全访问医院管理信息系统，在浏览器地址栏展示量子安全“**Q**”标识和国密“**m**”标识，让安全合规状态一目了然。

4. 数字签名 PQC 就绪：正在开发中

医疗文书的数字签名同样面临量子时代的严峻挑战。零信技术已将此列为下一阶段核心研发方向，目前正在开发中，计划推出文档签名自动化服务、签名加固和混合签名能力。在功能正式发布前，医疗机构可优先部署成熟的国密混合 PQC HTTPS 加密方案，确保传输通道的量子安全，同时为未来的签名升级做好技术储备。

七、医疗数据安全，选对技术方案是关键

医疗数据安全正处于一个关键的历史转折点。密评已成为医疗合规的刚性门槛，而量子安全威胁正在加速逼近。与金融数据或一般个人隐私数据不同，医疗数据具有极长的有效生命周期，病历保存 30 年，基因数据跨越代际。今天签发的每一份电子诊断报告、每一份电子病历，都需要在 20 年甚至 50 年后依然具备法律效力。

政策法规要求医疗机构必须加密、必须用国密、必须过密评，但如何落实这些要求，选择什么样的技术路线，责任在医疗机构自身。选择不同的技术路线，医疗数据的安全保障程度天差地别：

(1) 基于 TLCP 的传统国密方案，即使通过了密评，也无法保障数据长期安全，因为它不支持前向安全；

(2) 国密 TLS 1.3 方案，解决了前向安全问题，但无法抵御量子攻击；

(3) 国际混合 PQC 方案，不支持国密，无法同现有国密算法共存，无法满足密评要求；

(4) **只有国密混合 PQC 方案（国密 TLS 1.3 + SM2MLKEM768），才能同时满足密评合规、前向安全和量子安全三重保障。**

零信技术的国密混合 PQC HTTPS 加密方案已完全成熟，可立即部署。一次投资，同时完成国密合规改造、前向安全升级和后量子密码迁移三大刚需任务，再加上内置的 WAF 防护能力，这些正是医疗机构应对当下合规要求与未来量子威胁的唯一正确选择。

CHIMA 2026 大会正是医疗信息化同仁共同探讨这一重大课题的最佳平台。期待有机会在珠海与各位同行深入交流，共同推进医疗数据安全的量子时代升级。

王高华

2026 年 4 月 22 日于深圳

欢迎关注零信技术公众号，实时推送每篇精彩 CEO 博客文章。
已累计发表中文 271 篇(共 80 万 5 千多字)和英文 119 篇(16 万 6 千多单词)。