全球数据安全观察

总第 81 期 2022 年第 09 期

（2022.03.07-2022.03.13）

大数据协同安全技术国家工程研究中心

目录

政策形势

1、工信部印发《车联网网络安全和数据安全标准体系建设指南》

工业和信息化部近日印发《车联网网络安全和数据安全标准体系建设指南》，提出到2023年底，初步构建起车联网网络安全和**数据安全标准体系**。重点研究基础共性、终端与设施网络安全、网联通信安全、**数据安全**、应用服务安全、安全保障与支撑等标准，完成50项以上急需标准的研制。到2025年，形成较为完善的**车联网网络安全和数据安全标准体系**。完成100项以上标准的研制，提升标准对细分领域的覆盖程度，加强标准服务能力，提高标准应用水平，支撑车联网产业安全健康发展。

https://mp.weixin.qq.com/s/ppu5-vfmx4wmuERcHytn7A

2、《河南省数据条例(草案)》征求意见

近日，河南省大数据管理局组织起草了《河南省数据条例（草案）》（征求意见稿），现通过局门户网站向社会公众公开征求意见。该征求意见稿共七章五十二条，分别为总则、公共数据、非公共数据、数据开发利用、**数据安全**、法律责任、附则。

其中第五章强调数据处理者开展数据处理活动时，应**健全全流程数据安全管理制度等数据安全保护措施**，同时提出重要数据处理者应明确数据安全负责人和管理机构，定期对数据处理活动风险评估并报送报告，加强**数据安全风险评估**、报告、信息共享、检测预警等要求。

https://mp.weixin.qq.com/s/u8LwXf5rfoQ9XnxkLggINg

3、《智能网联汽车数据安全评估指南》公开征求意见

3 月 9 日，由国家工业信息安全发展研究中心牵头编制的《智能网联汽车数据安全评估指南》团体标准(以下简称“标准”)正式公开征求意见。标准旨在进一步落实《汽车数据安全管理若干规定》《车联网网络安全和数据安全标准体系建设指南》等政策法规要求，不断优化标准供给结构，提高行业服务能力，对规范智能网联汽车行业数据处理行为具有重要意义。

智能网联汽车数据安全评估主要有**数据安全风险评估、数据安全合规性评估和数据出境安全评估**三种类型。本标准规定了**智能网联汽车数据安全评估**的技术要求，共分为八部分，包括范围、规范性引用文件、术语和定义、**数据安全风险评估实施流程、数据安全合规性评估实施流程、数据安全评估结果**、参考文献、附件内容。

https://mp.weixin.qq.com/s/KYJs9AMrRY5zKXIozRsDYg

4、《上海市电子证照管理办法》公开征求意见

3 月 9 日，上海市人民政府办公厅数据发展管理办公室对《上海市电子证照管理办法（征求意见稿）》征求意见。该征求意见稿共五章三十条，分为总则、制发与归集、应用于服务、日常管理与监督考核、附则。

其中强调了综合管理部门负责建立全市电子证照的安全管理制度，指导有关单位落实安全管理责任。市大数据中心负责建立市电子证照库的安全保障体系，**明确安全管理要求**，对市电子证照库实行异地备份和安全等级保护，制定应急预案和数据备份恢复制度，保障市电子证照库的安全运行。发证单位、用证单位、社会化用证主体应当严格执行市电子证照库的安全管理要求，加强本单位业务系统和电子证照的**数据安全管理**，保障电子证照合法合规使用，保护持证主体的商业秘密和个人隐私。

https://mp.weixin.qq.com/s/9gz8Cjxfn4Tht0YgK_XfRQ

5、工信部召开会议 强调扎实做好工业领域数据安全管理工作

2022 年 3 月 10 日，工业和信息化部网络安全管理局组

织召开工业领域数据安全管理试点推进电视电话会议，深入解读试点工作方案、配套标准规范和管理服务平台，研究部署下一步重点工作。部消费品工业司、原材料工业司、装备工业二司对于本行业本领域**数据安全管理**提出了工作考虑，海南、江西、贵州、辽宁、江苏五省工业和信息化主管部门作交流发言。

会议强调，扎实做好**工业领域数据安全管理**工作，是贯彻落实习近平总书记重要指示批示精神和党中央、国务院决策部署的根本要求，是筑牢工业经济发展安全底座、保障国家安全的迫切需要，是促进产业高质量发展、建设制造强国和网络强国的重要基础。试点工作要在工业和信息化领域数据安全工作总体框架下，验证**工业领域数据安全**工作体系运转的有效性和制度规范的科学性，重点解决执法队伍建设、**数据出境安全管理**、监测预警能力建设等关键难点问题，着力探索出**工业领域数据安全**工作的方法、路径和模式。各相关单位和试点企业要以试点工作为契机，将**数据安全**监管与业务管理工作同谋划、同部署、同落实；要加强组织领导，将责任落实到人，任务落实到位；要加强监督指导，积累经验，固化成效，努力打造试点标杆；要加强协调联动，共同探索构建**工业领域数据安全管理体系**。

https://mp.weixin.qq.com/s/eH6OhNP93qZnmEuAzlmV7A

6、拜登签署《关于确保数字资产负责任发展的总统令》

近日，拜登总统签署了一项期待已久的关于加密货币监管战略的行政命令。该文件名为“关于确保数字资产负责任发展的行政命令”，主要要求各政府机构对加密货币、数字资产和区块链或数字分类账技术进行研究和提出新的政策建议。命令指出，加密发展在很大程度上存在于“现有国内法律法规的范围内”，但“不断增长的发展和采用以及不一致的控制”需要建立一个协调一致的政府途径。该命令讨论的一些计划可能会对加密货币施加限制。该命令称，政府旨在保护消费者、投资者和企业，保持金融稳定，限制非法融资，并降低国家安全风险。其他政策似乎会促进加密货币的发展。该命令称，政府打算加强美国的领导地位，创造安全且负担得起的金融服务，并支持数字资产和支付领域的技术进步。该命令还涉及能源，认识到需要推广减少“来自某些加密货币挖矿.....的气候影响和环境污染”的技术。在接下来的 90 到 210 天（3 到 7 个月）内，将根据上述目标生成各种报告。

https://mp.weixin.qq.com/s/UrjeXGB8uup7MIWJt4onSw

技术、产品与市场

1、NIST 网络安全和隐私年度报告中的“密码关注”

2021 年 9 月，美国国家标准与技术研究院（NIST）发布《2020 年网络安全和隐私年度报告》（2020 Cybersecurity and Privacy Annual Report）。在这份最新的“年度工作总结”中，NIST 全面回顾了其在 2020 年为解决“网络安全和隐私挑战”所作出的努力和取得的成就。

NIST 列明了九项优先领域，密码标准和验证工作是其中重要组成部分。NIST 旗帜鲜明的指出，在当今系统、网络和移动设备日益开放和互联的环境中，网络和数据安全至关重要。用于加密、密钥建立和数字签名的密码标准、算法和方法为移动设备通信、电子商务交易安全等提供了重要基础。

https://www.secrss.com/articles/39916

2、国际云安全联盟发布数字安全框架

数字经济的发展离不开健全的数字经济治理体系和可靠的数字经济安全体系。为了助力数字经济安全发展，国际云安全联盟大中华区联合各界安全精英经过一年的精心打磨，于 2022 年 3 月 11 日**正式发布数字安全框架。该框架涵盖了数字安全的定义、REE(Regulation, Execution ,**

Evaluation)数字安全框架、数字身份框架和元安全框架。。

其中，**数字安全**是指在数字时代与数字化相关的一切安全要素、行为和状态的集合，既包括保障数字经济的安全性，也包括将数字技术用于安全领域。数字安全以数字身份为核心，以元安全为基础底座，涵盖了信息安全、网络安全、数据安全、隐私保护等领域或场景，并可扩展（如元宇宙安全）。除此之外，数字安全还包括利用数字技术保障数字基础设施的物理安全。虽然数字安全更偏重数字经济与数字技术，但是它与偏重国家网络主权的网络空间安全在法律、标准、技术上也是相通的。

REE 数字安全框架共分为规则层（数字安全框架的战略指引）、执行层（规则层落地所需的一切资源/工具及使用这些资源/工具的具体行动）、评价层（针对组织的数字安全成熟度进行评估、验证及考核）三层。

数字身份是连接安全与业务的基座，提供所有的人、数字人、物、设备等的数字标识、认证、访问全生命周期管理。当元宇宙兴起之时，数字身份更是连接现实世界和虚拟世界的标识和桥梁。

元安全是指下一代互联网原生安全，包括云计算、大数据、AI、5G/6G、IoT、区块链、量子计算等新兴技术所涉及的系统的原生安全，是数字安全的地基，需要硬件信任根的

支持。

https://mp.weixin.qq.com/s/IsHBO6g6fwGTaZW_UsMUZw

3、2023 年网络安全市场规模将达到 809.11 亿

日前，华安证券分析师尹沿技发布的《科技赋能、新基建，数字经济大有可为》报告指出，数据保护、政策与新技术三方推动，网络安全已成刚需。网安未来 3-5 年将保持高景气，将迎来新一波投资机遇。

在网安 2.0 时代，网安厂商围绕数据的采集、传输、使用等环节提供安全解决方案，保证数据全生命周期的安全防护。网安行业驱动力主要来自于政策要求，如等保 2.0 实战演练；（2）防御需求：政企及个人用户需面对来自外界的安全攻击事件；安全运营需求：用户自身系统在使用和升级的过程中，不可避免会产生安全漏洞。

数字经济时代，数据成为生产的关键要素，华安证券预见，上游硬件与软件系统技术水平将会为网安赋能；下游应用场景随着产业数字化得到拓展，跟随数据伴生的网络安全市场也将得到相应增长。根据 CCIA 数据，2023 年网络安全市场规模预计达到 809.11 亿元，同比增速 15%。华安证券预计，网安未来 3-5 年将保持高景气，将迎来新一波投资机遇。

https://www.cnbeta.com/articles/tech/1245371.htm

4、隐私计算 2022：三种共识与四种展望

目前隐私计算产业市场已经达成**既要数据流通又要隐私安全的监管共识、多元实现路径并存的技术共识、从基础设施建设到垂直场景运营的市场共识**。在此之下，隐私计算会在 2022 年获得更长足的发展。

立足当下，隐私计算行业迎来了前所未有的发展机遇。放眼未来，接下来就需要去进行**更安全、更可信的算法迭代**，做到更加“原语化”的**互联互通**，需要提供**数据和场景的连接**而不是一个单一厂商的平台。此外，在隐私计算业务生态方面，将会形成一张更广域的**数据智能流通网络**。

https://mp.weixin.qq.com/s/sRBcQKTPmzpYATg8dPMPpQ

5、美国 CISA 发布基于零信任架构的企业移动安全计划

随着对手继续努力破坏所有经济部门的网络，拜登政府正在推进建立新的网络安全范式的紧急措施。拜登总统发布的关于改善国家网络安全的行政命令(EO 14028) 侧重于为联邦政府推进安全措施，以显著降低网络攻击成功的风险，特别是 EO 14028 要求联邦民事机构制定计划以推动**采用零信任(ZT)架构**。

为了支持联邦机构和其他组织实现零信任，美国 CISA 发布了将零信任原则应用于企业移动性。这份新出版物强调了对移动设备和相关企业安全管理功能的特殊考虑的必要性，因为它们的技术发展和无处不在。它将指导联邦民事机构和其他组织开发和实施其特定的网络安全功能，以实现企业移动性，从而实现其 ZT 目标。

https://www.secrss.com/articles/40087

业界观点

1、最高检副检察长孙谦：全链条打击电信网络诈骗犯罪

全国两会期间，最高人民检察院副检察长孙谦指出，公民个人信息已成为网络犯罪实施的“基础物料”，非法泄露公民个人信息也成为多数网络犯罪的源头行为。以电信网络诈骗犯罪为例，犯罪分子或是通过非法获取的公民个人信息注册手机卡、银行卡，以此作为诈骗犯罪的基础工具；或是利用这些信息对诈骗对象进行“画像”实施精准诈骗，严重侵害公民合法权益，扰乱社会公共秩序。

孙谦表示，去年发布的个人信息保护法对个人信息保护作了全面规范，也对检察履职提出了新的要求。下一步，检察机关要结合办理电信网络诈骗等网络犯罪案件，依法从严打击侵犯公民个人信息犯罪，坚持“一案双查”，在查办网络犯罪的同时，溯源上游个人信息泄露的渠道和人员；围绕信息获取、流通、使用等各环节，同步加强全链条打击。突出打击重点，对于行业“内鬼”侵犯公民个人信息的行为，依法从严惩处，从重提出量刑建议。

孙谦认为，与刑事打击相比，行业、企业内部监管起到“防火墙”作用，更为关键、重要。结合司法办案，推动涉案企业加强合规建设特别是数据合规，引入第三方监督评估

机制，督促相关企业加强对数据的监管，特别是对要加强对公民个人信息的监管。

https://www.spp.gov.cn/zdgz/202203/t20220310_548720.shtml

2、全国政协委员胡卫：加强快递业个人信息保护刻不容缓

2021 年，我国快递行业年发件量正式迈入“千亿件时代”，快递成为连接千家万户的必需品。不过，在提供便利的同时，因快递面单导致个人信息泄漏的事件频发，也使得加强个人信息安全保护的呼声越来越高。

全国政协委员胡卫认为，造成这种局面的主要原因在于：利益勾连导致个人信息贩卖活动屡禁不止；快递企业寄递服务信息安保机制不健全；同时，存在相关监管部门对快递行业个人信息泄露问题查处不力的现象。

对此胡卫提出几点建议：

（1）及时修订《快递暂行条例》及《寄递服务用户个人信息安全管理规定》，从而强化其中的法律责任，为快递业个人信息保护提供更为坚实的法制保障；

（2）建立健全常态化日常监管制度。进一步完善对快递企业的定期巡检和飞行检查制度，督促快递企业将个人信息保护落实到内部管理全流程、各环节；

（3）相关部门要切实加大执法力度；

（4）加强技术防护和安全教育。

https://new.qq.com/omn/20220311/20220311A0BCBE00.html

3、全国政协委员李大进：应设立网络安全和数据保护窗口

全国政协委员李大进表示，近年来网络安全与数据保护领域的立法正处于活跃期，企业在面对大量法律法规及指导文件时，难以准确把握相关要求的落实；同时日益完善的个人信息保护制度赋予了其广泛的权利，但在行使权利的过程中却无法及时得到有效的反馈与响应。

对此李大进提出建议：

一是加强履行相关职责部门之间的统筹和协调。在打破部门界限，形成监管合力的同时，也应当明晰统筹工作的具体内涵外延；

二是设立网络安全和数据保护的窗口提供指导咨询服务。对于涉及不同主管部门的咨询内容，窗口应该具备能力进行内部的资源共享、协调统合，通过统一窗口给出权威的答复；

三是尽快落实和明晰个人信息保护投诉、举报渠道和方式。公开投诉举报渠道，对于投诉举报的问题应当依法进行处理并公示相关结果。李大进认为，“这样既能彰显法律规定的威慑效力，同时也是监管部门借助社会力量广泛掌握实

际情况，提高监管工作效率的有效途径。”

https://www.jwview.com/jingwei/html/m/03-04/468839.shtml

4、全国政协委员雷军：加强电子废旧物循环利用中的个人数据安全保障

根据《中国废弃电器电子产品回收处理及综合利用行业白皮书 2020》，现阶段我国每年电子废旧物处理量已达到8000 万台左右。另外一则数据显示，目前我国规范回收率不足 20%，而欧洲已达到 42.5%。

当前，我国公众对信息泄露风险的担忧也不断加深，在一定程度上导致了电子废旧物回收率难以实现大幅提升。

对此，雷军在全国两会上建议，在电子废旧物循环利用各环节中，严格落实个人信息保护操作规范，打通个人信息安全的“最后一公里”，有效提升电子废旧物回收率。

https://tech.gmw.cn/2022-03/07/content_35568527.htm

5、全国政协委员彭静：仍有数据处理主体合规能力欠缺，可发挥第三方专业机构作用

2021 年《数据安全法》、《个人信息保护法》实施后，对数据处理者提出更高的合规要求，需建立并完善一整套数据处理机制，但不少数据处理主体数据合规意识淡薄、合规能力欠缺。

全国政协委员彭静建议，对数据治理、保护能力进行梳理，在各级党委、各地国有资产监督管理部门统一部署下，梳理数据保护重点行业、从事高风险数据处理活动的政府机关、国有企业，应当明确对外委托专业机构开展数据合规工作的类型。其次建立对外委托工作流程、考核机制，建立专业机构资质入库机制。

同时，彭静建议制定个人信息保护合规标准，保障第三方合规工作质量。她进一步指出，银行保险、证券、市场、卫生健康等行业监管机关应鼓励、采纳本行业协会、企业编制符合本行业实际与发展的数据保护行业标准及第三方合规工作认证机制。

彭静认为相关监管机关应与人民法院、人民检察院建立联席工作机制，实现相关行业第三方数据合规标准与《关于建立涉案企业合规第三方监督评估机制的指导意见》等司法合规制度无缝对接，确保第三方合规工作成果法律效力，整合企业事前、事后一体化数据合规能力。

https://m.21jingji.com/article/20220304/herald/8b4e417a795dc4e8b58f4ab1bc704f8a.html

6、四成消费者担忧个人敏感信息泄露 数据安全成为车企智能化竞争新“分水岭”

近日，“2022 中国消费者智能网联汽车数据安全和个人隐私意识与顾虑调查”（下简称“调查”）显示，现阶段中国消费者对智能汽车厂商能否妥善保护个人敏感信息整体信心不足——参与调查的消费者中，超过四成表示对此完全没信心或信心不太足。

调查显示，中国消费者对现阶段智能汽车厂商能否妥善保护个人敏感信息的整体信心不足。受访消费者总体信心指数仅为 45.7 分（满分为 100 分），仅有约三成（30.4%）受访者表示比较有信心或极其有信心，超过四成（41.0%）表示完全没信心或信心不太足。

调查认为“安全感”的缺失，有多个方面的原因:

1、与智能手机厂商相比，智能汽车厂商更少实施个人数据收集的告知措施，这使得用户对智能汽车收集个人信息的知晓程度更低;

2、智能汽车用户普遍担心个人信息泄露会带来严重后果，其中信息的转卖引发的不安感尤甚;

3、对个人信息保护法律法规的不了解以及不知道如何维权，加重了智能汽车用户对个人隐私泄露及后果的担忧。

调查还发现，超过九成（94.6%）受访消费者会有倾向性

地选择注重数据安全和保护个人敏感信息的汽车品牌。这其中，54.6%的消费者表示“一定会”购买数据安全保障能力强的品牌。

https://new.qq.com/omn/20220309/20220309A08MPC00.html

数据安全事件

1、Clearview AI 因收集意大利用户生物特征遭罚 2000 万欧元

2022 年 3 月 9 日消息，意大利的数据保护机构（GPDP）对 Clearview AI 处以 2000 万欧元罚款，控诉其未经同意对用户的生物特征进行监控收集。

此监控项目始于去年 2 月，共收集 100 亿份人脸数据，其中大量是在线收集的意大利用户信息。GPDP 发现违规行为后，发出 2000 万欧元罚单，并勒令 Clearview 删除意大利用户数据，Clearview 则辩解称 20 年 3 月于意大利的服务就已中断，此事与他们无关，并对欧洲 IP 进行屏蔽。

https://www.bleepingcomputer.com/news/legal/clearview-ai-fined-20m-for-collecting-italians-biometric-data/

2、东欧大型加油站服务商 Rompetrol 网络受到 Hive 勒索软件的攻击

2022 年 3 月 7 日，据报道，罗马尼亚的 Rompetrol 加油站网络遭到勒索软件攻击，目前已关闭其网站和加油站的 Fill&Go 服务。Rompetrol 是罗马尼亚最大的炼油厂 Petromidia Navodari 的运营商，BleepingComputer 了解到

Hive 勒索软件团伙是这次攻击的幕后黑手，要求 Rompetrol 支付 200 万美元的赎金，以接收解密器并且不泄露据称被盗的数据。

https://www.bleepingcomputer.com/news/security/rompetrol-gas-station-network-hit-by-hive-ransomware/

3、全球最大轮胎制造商之一普利司通遭数据泄露，并被喊话支付赎金

近日，LockBit 勒索软件团伙声称已经破坏了最大的轮胎制造商之一普利司通美洲公司的网络，并窃取了该公司的数据。普利司通美洲企业家族在美洲拥有 50 多个生产设施和 55,000 名员工。如果公司不支付赎金，Lockbit 计划在 2022 年 3 月 15 日 23:59 之前释放被盗数据。

https://mp.weixin.qq.com/s/HZZos9tXt1fBaQMsu3X0Og

4、三星数据泄露: Lapsus$ 团伙窃取了 Galaxy 设备的源代码

2022 年 3 月 9 日，据报道，三星披露了一起数据泄露事件，威胁者可以访问公司内部数据，包括 Galaxy 模型的源代码。此前， Lapsus$ 勒索软件团伙声称从三星电子窃取了大量敏感数据，并泄露了 190GB 的所谓三星数据作为黑客攻击的证据。本次被盗数据包含机密的三星源代码，包括:

安装在所有三星设备的 TrustZone (TEE) 上的每个受信任小程序 (TA) 的源代码、所有生物识别解锁操作的算法，包括直接与传感器通信的源代码、所有最新三星设备的引导加载程序源代码等。

https://securityaffairs.co/wordpress/128828/data-breach/samsung-data-breach.html

5、黑客组织 Lapsus$发起投票：根据结果公开公司数据

2022 年 3 月 11 日报道，在攻破 NVIDIA 之后，嚣张的黑客组织 Lapsus$ 近日在 Telegram 上发出投票帖，通过投票结果来决定接下来公开哪家公司的数据。在投票选项中包括运营商 Vodafone 的源代码、Impresa 的源代码和数据库、MercadoLibre 和 MercadoPago 的数据库。投票将于 3 月 13 日结束。

https://www.cnbeta.com/articles/tech/1245685.htm

6、沃达丰开始调查黑客组织 Lapsus$ 所声称的数据泄露事件

2022 年 3 月 11 日，据外媒报道，Lapsus$ 网络犯罪组织声称窃取了跨国电信公司沃达丰大约 200 GB 的源代码文件，据称这些文件包含在 5,000 个 GitHub 存储库中。沃

达丰表示，它正在与执法部门合作，调查黑客组织 Lapsus$ 提出的数据泄露指控，还表示勒索中所引用的存储库类型包含的是专有源代码，并不包含客户数据。

https://securityaffairs.co/wordpress/128903/cyber-crime/vodafone-investigates-data-breach.html

7、电子商务巨头 Mercado Libre 确认源代码数据泄露

2022 年 3 月 8 日报道，阿根廷电子商务巨头 Mercado Libre 已确认“未经授权访问”其部分源代码。Mercado 还表示，威胁参与者访问了大约 300,000 名用户的数据。目前，Mercado 的 IT 基础设施没有受到影响，敏感信息似乎没有受到损害。

https://www.bleepingcomputer.com/news/security/e-commerce-giant-mercado-libre-confirms-source-code-data-breach/

8、日本电装德国分部大量机密数据被窃取 黑客威胁将公开

2022 年 3 月 13 日消息，丰田汽车旗下零部件制造商日本电装宣布，其德国当地法人受到了网络攻击。该公司确认其网络感染了勒索软件。被认定发动了此次攻击的黑客集团已经发布了勒索声明，涉及数据为 1.4TB，文件超过 15 万 7 千份，内容为设计图、订购书扫描件、邮件和打印机的印刷数据等。公司称虽然目前并没有立刻对公司经营造成影响，

但是“关于受害的详细情况正在调查中”。公司已向德国当地政府提交了受害报告。

https://www.cnbeta.com/articles/tech/1246433.htm

9、英国渡轮运营商 Wightlink 在网络攻击后潜在数据泄露

2022 年 3 月 11 日，据外媒报道，英国渡轮运营商 Wightlink 遭到“高度复杂”的网络攻击，可能已经泄露了属于“少数客户和员工”的个人数据。Wightlink 表示，发生在 2 月的攻击影响了某些后台 IT 系统，但没有影响其渡轮服务、预订系统或网站。执法部门和英国信息专员办公室 (ICO) 以及潜在的违规受害者已收到通知。

https://portswigger.net/daily-swig/uk-ferry-operator-wightlink-flags-potential-data-breach-after-highly-sophisticated-cyber-attack?&web_view=true

10、超过 20 万名南丹佛心脏病学协会患者收到数据泄露通知

2022 年 3 月 11 日，据外媒报道，南丹佛心脏病学协会 (SDCA) 近日披露，他们于 1 月 4 日首次检测到数据安全漏洞。启动事件响应计划后，经调查确定 SDCA 的网络在 2022 年 1 月 2 日至 2022 年 1 月 5 日期间受到了未经

授权的访问。在此期间，存储在系统上的某些文件被访问，这些文件包含受保护的患者健康信息，例如姓名、出生日期、社会安全号码和/或驾驶执照号码、患者帐号、健康保险信息和临床诊断信息等等。根据通知，目前没有迹象表明有任何滥用信息的迹象，但 287,652 名患者被告知该数据泄露事件，并通过 IDX 提供监控和身份恢复服务。

https://www.databreaches.net/287652-south-denver-cardiology-associates-patients-notified-of-breach/?web_view=true