大连医科大学文件

大医发〔2019〕305号

关于印发《大连医科大学信息化个人信息保护管理办法（试行）》的通知

各单位（部门）：

现将《大连医科大学信息化个人信息保护管理办法（试行）》印发给你们，请根据工作实际认真贯彻落实。

大连医科大学

2019年12月27日

大连医科大学信息化个人信息保护管理办法（试行）

第一章　总则

第一条　为规范学校信息化工作中个人信息的处置，明确信息化工作中对个人信息保护的管理要求，避免个人信息处置不当造成师生、学校及其他相关部门、人员利益受损，按照《中华人民共和国网络安全法》（2016年主席令第53号）、《中华人民共和国刑法》（2017年修正）等法律法规要求，根据国标《信息安全技术个人信息安全规范》（GB/T35273-2017）相关要求，特制定本办法。

第二条　本办法适用于学校信息化工作中所涉及的个人信息采集、存储、使用、共享、公开及删除等各环节。在学校信息化工作中，符合国家及相关主管部门在学籍、教务、人事、财务、档案、设备、资产管理等方面的法律法规及规章制度要求，可依照本办法处置校内师生的个人信息。校内师生有义务提供相关个人信息。

第三条　根据国家法律法规和国家标准，本办法中个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息，包括但不限于如下信息：

姓名、出生日期、身份证件号码、个人生物识别信息、银行账号、住址、个人通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、成绩信息等。

个人敏感信息指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，包括但不限于如下信息：

身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

第四条 在学校信息化工作中，个人信息保护应遵循如下原则：

（一）合法原则：不得违反相关法律、法规的规定；

（二）最小必要原则：在满足信息化工作必要需求前提下，在最小范围内采集、存储、使用个人信息，对于个人信息的处理采用最小操作权限划分，不得超范围处置个人信息；

（三）安全原则：信息化工作中应采用必要的安全技术措施和管理手段，保障个人信息的完整性、保密性及安全性，避免个人信息泄露、损毁和丢失；

（四）知情同意原则：学校在科研、教学及其他校务管理中，依法依规对个人信息进行采集和使用，默认个人同意使用；其他

情况下使用个人信息，应明确告知相关个人，确保个人知情并自愿同意后，方可使用。

第二章　责任分工

第五条　学校信息化工作中个人信息保护工作由学校网络安全与信息化领导小组负责领导，由现代教育技术中心（网络信息中心）负责组织实施、监督检查，其他二级部门负责具体落实本部门管理的个人信息的安全保护工作。

第六条　在学校信息化工作中，校内师生有权查询本人的个人信息，有权更正错误的个人信息，有权对信息化工作中违规处置个人信息的行为进行反馈和报告。信息化主管部门在接到举报反馈后，应及时处理、反馈并依情况继续向学校报告。

第七条　校内师生作为个人信息提供者和所有者，有义务及时更新必须的个人信息，保证信息的准确性和完整性，并妥善保管个人信息。由于师生个人原因造成的个人信息泄露、损坏、丢失，由本人承担相应责任；如对他人信息造成不良后果，将根据本办法的追责条款，追究相关责任人的责任。

第三章　个人信息的采集、存储、使用、共享、公开与删除

第八条　学校信息化工作中的个人信息采集，由相关数据的主管部门负责。采集到的个人信息，除存储在相关的业务系统数据库中，还应通过相关数据交换途径，共享到学校公共数据平台。对于未纳入业务部门管理的个人信息数据的采集，也须由学校公

共数据平台进行。没有管理权限的其他业务部门或信息化项目组不允许另外进行相关个人信息的采集。

个人信息主管部门原则上应通过业务系统进行数据采集，不进行线下采集。对采集的个人信息要进行审核，并提供方便、快捷的信息更新渠道，对发生变更或采集有误的数据进行更新，保证个人信息的准确性和完整性。

第九条 个人信息在存储和信息系统间传输过程中需进行加密处理或采用其他安全技术。学校信息化平台管理部门需采取有效技术手段和管理措施保护存储个人信息的服务器和数据库，避免个人信息的泄露、损坏或丢失。

信息系统里的个人信息原则上均须在学校服务器本地存储，不得在校外、或非管理机构的其他服务器上存储。

信息化业务系统对于个人信息的查询、修改等操作应保留不少于 180 天的最新操作日志，并尽力提供审计功能，审计对个人信息的各类操作。同时严格把控对个人信息数据的批量导出功能。执行重要操作前（如批量修改、拷贝、导出等），需由相关数据主管部门审批，通过后方可进行操作。

第十条 个人信息数据的申请使用流程参照《大连医科大学信息化数据管理办法》（大医发[2016]275 号）相关规定进行。

使用个人信息时应严格遵循前文所述的合法原则、最小必要原则、安全原则和知情同意原则。要严格按照申请时所确定的用

途使用个人信息，严禁将个人信息挪作他用。

可接触到个人信息的人员需签订信息化数据使用保密协议，对相关个人信息严格保密，严禁未经授权对外提供个人信息。

非我校信息化工作需要而进行个人信息查询的，原则上只接受公安部门等上级主管部门依法依规的查询请求，受理部门为相关个人信息数据主管部门，其他部门不得代为受理。

第十一条 校内信息管理系统，确需使用个人信息的，需充分评估合法性、必要性和安全性，达到可以满足个人信息保护要求后，可依法依规使用或进行个人信息共享。非数据源信息系统原则上不得共享个人敏感信息。

第十二条 在信息化工作中，确因工作需要进行个人信息的公示公开或通过特定界面（如显示屏幕、纸面）进行展示，必须满足相关法律法规要求，并进行相关个人信息的去标识化处理，不得直接公开完整的个人信息。具体方法，请参考附件的校内个人信息去标识化参考指南处理。

去标识化后的个人信息数据应无法识别特定个人且不能复原，可直接应用于学校的科研、教学、校务管理等工作中，相关信息数据的所有权及其相关知识产权归学校所有。

公开个人信息遵循最小化原则，即通过信息组合能识别特定自然人身份并满足公示要求即可，严禁超范围公开其他相关信息。

对于以下个人敏感信息不宜公开，包括：银行账号、通信记

录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息以及14岁以下（含）儿童的个人信息。

第十三条　注销的信息化项目或报废的存储设备，要确保承载的个人信息已被清理。

对于违反法律法规及本办法采集、存储的个人信息，应依法依规删除相关个人信息数据。

第四章　责任认定及追责

第十四条　现代教育技术中心将依照本办法对各信息化项目中个人信息处置相关的审计记录和日志等进行检查，或者通过其他网络安全检测手段检查个人信息的采集、存储、使用及处理情况。对于出现的违规行为将比照网络安全事件进行处置，校内相关部门及个人应遵守本办法，及时、彻底的就出现问题进行整改。

第十五条　对于造成重大损失或整改不力的违规行为，由现代教育技术中心负责汇总相关情况，提交学校网络安全与信息化领导小组进行责任认定，学校将按照《大连医科大学网络安全工作责任制实施细则》确定相关责任人、责任部门，进行后续追责。对于违反国家法律法规的行为，学校将配合公安、网信等部门进行处理。

第五章　附则

第十六条　本办法由现代教育技术中心负责解释。

第十七条　本办法自发布之日起施行。

附件

校内个人信息去标识化参考指南

在大连医科大学信息化工作中，如需对个人信息进行去标识化处理（数据脱敏），应保证处理后的信息无法或很难进行复原。举例如下：

姓名可隐藏名字中的1-2位；

出生日期可隐藏2位日期；

身份证件号码可隐藏结尾后6位；

学号、教工号可隐藏结尾后3位；

个人手机号可隐藏结尾后4位；

个人通信地址及家庭住址可隐藏具体门牌号；

车牌号可隐藏后五位中的任意2-3位。

大连医科大学党政办公室　　2019年12月27日印发