f) 主体发现控制者所持有的该主体的个人健康医疗数据不准确或不完整时，控制者应为其提供请求更正或补充信息的方法。
g) 主体有权对控制者或其处理者使用或披露数据的情况进行历史回溯查询，最短回溯期为六年。
h) 主体有权要求控制者在诊断、治疗、支付、健康服务等过程中限制使用或披露个人健康医疗数据，以及限制向相关人员披露信息，控制者没有义务同意上述限制请求；但一旦同意，除非法律法规要求以及医疗紧急情况下，控制者应遵守商定的限制。
i) 控制者可以使用治疗笔记用于治疗，在进行必要的去标识化处理后，可以在未经个人授权的情况下使用或披露治疗笔记进行内部培训和学术研讨。
j) 控制者应制定、实施合理的策略与流程，将使用和披露限制在最低限度。
k) 控制者应确认处理者的安全能力满足安全要求，并签署数据处理协议后，才能让处理者为其进行数据处理，处理者应当按照控制者的要求处理数据，未经控制者许可，处理者不能引入第三方协助处理数据。
l) 控制者向政府授权的第三方控制者传送数据前，应获得加盖政府公章的相关文件，数据传送后，数据安全责任以及传输通道的安全责任由第三方控制者承担。
m) 控制者在确认数据使用的合法性、正当性和必要性，并确认使用者具备相应数据安全能力，且使用者签订了数据使用协议并承诺保护受限制数据集中的个人健康医疗数据后，可将受限制数据集用于科学研究、医疗保健业务、公共卫生等目的；使用者只能在协议约定的范围内使用数据并承担数据安全责任，在使用数据完成后，应按照控制者要求归还、彻底销毁或者进行其他处理。未经控制者许可，使用者不能将数据披露给第三方。
n) 如果控制者针对个人健康医疗数据汇聚分析处理之后得到了不能识别个人的健康医疗相关数据，该数据不再属于个人信息，但其使用和披露应遵守国家其他相关法规要求。
o) 控制者因为学术研讨需要，需要向境外提供相应数据的，在进行必要的去标识化处理后，经过数据安全委员会讨论审批同意，数量在250条以内的非涉密非重要数据可以提供，否则应提请相关部门审批。
p) 经主体授权同意，并经数据安全委员会讨论审批同意，不涉及国家秘密且不属于重要数据的，控制者可向境外目的地传送个人健康医疗数据，累计数据量应控制在250条以内，否则应提请相关部门审批。
q) 不将健康医疗数据在境外的服务器中存储，不托管、租赁在境外的服务器；使用云平台的应符合国家相关要求。
r) 对外进行数据合作开发利用时，宜采用“数据分析平台”开放形式，对数据使用披露进行严格管控。

8 安全措施要点

8.1 分级安全措施要点

可以根据数据保护的需要进行数据分级，对不同级别的数据实施不同的安全保护措施，重点在于授权管理、身份鉴别、访问控制管理。例如，从个人信息安全风险出发划分的数据分级和安全措施要点如表3所示。医生调阅场景下的数据分级及安全措施详见11.1。临床研究场景下的数据分级详见11.3。