《人工智能时代的医学数据隐私与伦理》教学大纲

一、课程基本信息

课程名称/英文名称	人工智能时代的医学数据隐私与伦理/ Medical Data Privacy and Ethics in the Age of Artificial Intelligence	课程代码	BME2133
课程层次 [1]	研究生课程	学分/学时	3.0/48
主要面向专业 [2]	生物医学工程	授课语言	中文, English
先修课程 [3]	无	建议先修说明 [4]	Python 程序设计
开课单位	生物医学工程学院	课程负责人	万之瑜

注 1：课程层次填写“本科生课程”、“研究生课程”或“本研一体课程”

注 2：主要填写全校 10 个本科专业（或若干个专业的组合）或“全体本科生”或“全校学生”

注 3：显示课程信息里的“强制先修课程”信息，强制先修课程是本课程的选课强制约束条件；教师在录入课程教学大纲时，该信息显示但不可修改

注 4：可在此填写教师对学生修读本课程之前应具备哪些知识基础的建议

二、课程简介

《人工智能时代的医学数据隐私与伦理》是生物医学工程专业研究生的一门专业选修课，也是生物医学工程专业工程硕士研究生的一门公共基础课。本课程聚焦人工智能时代下医学数据隐私与伦理问题，深入探讨医学数据的隐私保护技术、伦理困境和法律法规。课程内容涵盖医学数据在收集、共享、处理和使用过程中可能涉及的伦理挑战和隐私保护策略。通过讲座、讨论、案例分析和项目实践等形式，本课程旨在培养学生在智能医疗系统设计、生物医学数据管理方面的能力，帮助他们理解在医疗数据驱动的 AI 系统中如何平衡隐私保护与技术创新，帮助他们为未来的医疗数据处理相关工作奠定坚实的伦理、法律及技术实践基础。

本课程的内容包括四个基本模块：第一部分讲解人工智能时代的医学数据隐私与伦理的基本概念与主要挑战，第二部分讲解社会法律层面对于数据隐私与伦理的保护方案，第三部分讲

解技术层面对于数据隐私与伦理的保护方法，第四部分是实践隐私及伦理保护方法在具体案例中的应用。

三、课程教学目标

1.理解人工智能时代的医学数据隐私与伦理的核心概念、主要挑战和技术解决方案。

2.探讨人工智能在医疗数据处理中的伦理问题，如算法偏见、透明度和知情同意。

3.了解国内外相关法律法规（如 HIPAA、GDPR 等）对医学数据隐私的保护要求。

4.掌握医疗数据隐私保护的常用及前沿技术，包括差分隐私、加密方法和去识别化技术等。

5.培养在智能医疗中数据隐私和伦理方面的批判性思维，提升处理隐私与伦理问题的实际能力，为未来的人工智能医疗系统设计和实施提供支撑。

四、课程教学方法

本课程以课堂讲授为基础，通过小组讨论和文献阅读增强学生对于理论的理解，通过案例分析和项目实践增强学生对于理论和技术的应用，提高对实际场景中复杂的数据隐私及伦理问题的解决能力。采用课堂讲授、随堂测试、阅读理解、课后作业、案例研讨、专题讨论、课程研究项目等多种方式相结合。突出启发式的基于理解的教学方法，与国际接轨，提高学生的主动学习的热情和科研兴趣。同时可结合 MOOC、专家讲座等多种方式进行教学。授课语言口语中文为主，书写英文为主。

五、课程教学内容与安排

*（可按**教学周**或**章节名称**两种方式进行课程教学内容安排，列出主要知识点和教学方法。）*

以教学周方式安排教学内容

时间	章节名称	主要教学内容 （主要知识点）	学时安排	教学方法 （仅列名称）
第 1 周周三	一、课程介绍与数据隐私和伦理概述(a)(b)	医学数据在 AI 时代中的作用。 数据隐私的概念及其重要性。 伦理、道德的概念及其重要性。	2	课堂讲授+案例讨论+分组讨论

2 月 19 日 15：00- 16：40				
第 1 周周五 2 月 21 日 15：00- 16：40	一、课程介绍与数据隐私和伦理概述(c)	人工智能伦理：机器道德和伦理、自动化与就业。	2	课堂讲授+案例讨论+分组讨论
	二、生命科学、医学及信息学中的伦理问题(a)	科研伦理：人体实验、动物实验和科研的道德准则。 生命科学伦理：生殖技术、基因技术、干细胞研究等引发的争议。		
第 2 周周五 2 月 28 日 15：00- 16：40	二、生命科学、医学及信息学中的伦理问题(b)(c)	医学伦理问题：堕胎、安乐死、公共卫生问题、以及针对特殊人群（幼儿、青少年、精神病患者等）的医疗伦理问题。 信息安全隐私问题：个人数据泄露、监控技术、面部识别。 网络安全和犯罪：黑客行为、网络暴力。	2	课堂讲授+案例讨论
第 3 周周三 3 月 5 日 15：00- 16：40	三、数据共享与医疗 AI 的伦理问题(a)(b)	生物医学数据共享的重要性及隐私挑战。 数据治理与数据生命周期管理。 算法偏见与公平性问题。 透明性与可解释性在医学人工智能中的重要性。	2	课堂讲授+案例讨论
第 3 周周五	三、数据共享与医疗 AI 的伦理问题(c)	**进行随堂测试 1。** 患者知情同意的数字化实现。	2	课堂讲授+案例讨论

3 月 7 日 15：00- 16：40	四、法律法规框架(a)	国际上 HIPAA、GDPR 等法律法规对生物医学数据的影响。		
第 4 周周五 3 月 14 日 15：00- 16：40	四、法律法规框架(b)(c)	中国数据安全法和个人信息保护法。 数据所有权与使用权。 医学数据共享的合规性要求。	2	课堂讲授+ 案例讨论
第 5 周周三 3 月 19 日 15：00- 16：40	五、生物医学数据的特点与隐私风险 I(a)(b)	**进行随堂测试 2。** 电子病历数据的特点及隐私风险。 自然语言医学数据的特点及隐私风险。 基因数据的特点及隐私风险。	2	课堂讲授+ 案例讨论
第 5 周周五 3 月 21 日 15：00- 16：40	五、生物医学数据的特点与隐私风险 I(c)	医学图像数据的特点及隐私风险。	2	课堂讲授+ 案例讨论
	六、生物医学数据的特点与隐私风险 II(a)	主要攻击模型：重识别攻击、成员推理攻击及重建攻击。		
第 6 周周五 3 月 28 日 15：00- 16：40	六、生物医学数据的特点与隐私风险 II(b)(c)	隐私风险评估方法。 不同类型医学数据泄露的案例研究。 **布置课后作业 1。**	2	课堂讲授+ 案例讨论
第 7 周周三 4 月 2 日 15：00- 16：40	七、医学数据隐私保护的常用技术 I(a)(b)	数据去识别化技术：假名化、K 匿名化等。	2	课堂讲授

第 7 周周五 4 月 4 日 15：00- 16：40	七、医学数据隐私保护的常用技术 I(c)	用于最优化保护的博弈论模型。	2	课堂讲授
	八、医学数据隐私保护的常用技术 II(a)	差分隐私的基本原理与应用 I。 **开始课程项目选题。**		
第 8 周周五 4 月 11 日 15：00- 16：40	八、医学数据隐私保护的常用技术 II(b)(c)	差分隐私的基本原理与应用 II。 访问控制技术及审计技术。 **布置课后作业 2。**	2	课堂讲授
第 9 周周三 4 月 16 日 15：00- 16：40	九、医学数据隐私保护的常用技术 III(a)(b)	密码学基础。 用于医学隐私计算的同态加密技术的原理及应用。 用于医学隐私计算的加密硬件技术的原理及应用。	2	课堂讲授
第 9 周周五 4 月 18 日 15：00- 16：40	九、医学数据隐私保护的常用技术 III(c)	用于医学隐私计算的多方安全计算技术的原理及应用。	2	课堂讲授
	十、医学数据隐私保护的前沿技术进展及未来趋势 I(a)	联邦学习模型及其在隐私保护中的应用。		
第 10 周周五 4 月 25 日 15：00- 16：40	十、医学数据隐私保护的前沿技术进展及未来趋势 I(b)(c)	合成数据生成技术及其在隐私保护中的应用。 **布置课后作业 3。**	2	课堂讲授

第 11 周周三 4 月 30 日 15：00-16：40	十一、医学数据隐私保护的前沿技术进展及未来趋势 II(a)(b)	区块链技术在医学数据隐私中的潜力。	2	课堂讲授
第 11 周周五 5 月 2 日 15：00-16：40	十一、医学数据隐私保护的前沿技术进展及未来趋势 II(c)	医学数据隐私的未来研究趋势。	2	课堂讲授
	十二、用于医疗的前沿 AI 技术中的隐私与伦理问题 I(a)	大语言模型的介绍。 大语言模型在医学中的应用介绍。		
第 12 周周五 5 月 9 日 15：00-16：40	十二、用于医疗的前沿 AI 技术中的隐私与伦理问题 I	大语言模型的隐私风险问题。 **进行开题宣讲。**	2	课堂讲授
第 13 周周三 5 月 14 日 15：00-16：40	十三、用于医疗的前沿 AI 技术中的隐私与伦理问题 II(a)(b)	大语言模型的公平性问题。 大语言模型的其他伦理问题。	2	课堂讲授+案例讨论
第 13 周周五	十三、用于医疗的前沿 AI 技术中的隐私与伦理问题 II(c)	大语言模型的伦理问题的解决方案及未来方向。	2	课堂讲授+案例讨论

5 月 16 日 15：00- 16：40	十四、用于医疗的前沿 AI 技术中的隐私与伦理问题 III(a)	生成式人工智能的介绍。 生成式人工智能在医学中的应用。		
第 14 周周五 5 月 23 日 15：00- 16：40	十四、用于医疗的前沿 AI 技术中的隐私与伦理问题 III(b)(c)	基于生成式人工智能的医学诊疗模型的潜在隐私风险及伦理问题。 通用人工智能产生后的潜在伦理及隐私问题探讨与展望。	2	课堂讲授+案例讨论+分组讨论
第 15 周周三 5 月 28 日 15：00- 16：40	十五、专题讲座(a)(b)	拟邀请 2 名专家讲解在特定应用场景（不同模态、不同疾病）中的医学数据攻击或者保护案例。	2	课堂讲授
第 15 周周五 5 月 30 日 15：00- 16：40	十五、专题讲座(c)	拟邀请 1 名专家讲解在特定应用场景（不同模态、不同疾病）中的医学数据攻击或者保护案例。	1	课堂讲授
	十六、课程项目汇报(a)	分组汇报及点评。	1	分组汇报
第 16 周周五 6 月 6 日 15：00- 16：40	十六、课程项目汇报(b)(c)	分组汇报及点评。	2	分组汇报

以章节名称方式安排教学内容

章节名称	主要教学内容（主要知识点）	教学周	学时安排	教学方法（仅列名称）

/	/	/	/	/

六、考核方式和成绩评定方法

（成绩评定方法需符合《上海科技大学课程考核及成绩管理办法（试行）》文件要求。）

本课程没有期末考试，主要采用基于团队课程项目（team-based course project）的方式考核学生对教学内容的掌握。每 1-2 个学生组成团队来完成课程项目，各个团队将从课程负责人制定的选题列表中选定某一自己感兴趣的项目，开展文献调研，查找现有的解决方案，发现并总结尚存的问题，并提出自己的解决思路，然后寻找相关数据集进行实验验证。每一个团队都需要有基于数据的实验结果，并进行口头汇报，最后以英文论文的形式提交项目报告。在提前告知并得到课程负责人同意的前提下，学生也可在选题列表之外自寻项目进行研究。课程项目的日程安排如下：

教学周	**课程项目设计计划**
8	发布课程项目选题，学生开始组队。
9	学生组队完成，开始选择课程项目题目。
10	各团队**完成项目选题**并开始准备初步项目计划（Preliminary Project Proposal）
12	每个团队在课上进行 5 分钟的**开题宣讲**并**上交初步项目计划** （4-page proposal）
13	老师和助教对各团队的初步项目计划开展中期评定，并反馈指导意见给各团队。学生基于反馈意见，准备最终课程项目(Final Course Project)
16	每个团队在课上进行 10 分钟左右的**口头课程汇报**（时间按总人数调整，汇报顺序不提前确定。注意：第一个报告前，所有团队须提交 PPT）。授课老师、特邀专家、助教及全体学生对各团队口头课程汇报进行公平公正的排名和打分。
17	学生**上交最终课程项目报告**(更新后的 10-page project report。注意：报告作者排名不分先后，但需要在报告中标明各人负责的部分和个人贡献。)
18	授课老师和助教对最终课程项目报告开展期末评定。

课程项目的打分比例为：中期评定（20%）+口头汇报表现（40%）+课程项目报告（40%）。初步项目计划及课程项目报告的打分由助教参与评分，由授课老师最终确定。口头汇报表现的得分由授课老师（50%）、特邀专家（20%）、助教（10%）及全体学生（20%）加权平均获得。全

体学生的分数由除了该团队的人员以外的学生实名打分且去掉一个最高分、去掉一个最低分后平均获得。

总体考核比例如下表所示：

1	课程项目	50%
2	课后作业	30%
3	课前文献阅读理解	10%
4	随堂测试	5%
5	出勤与课堂表现	5%
	总分	100%

测试及提交的作业以英文为主。一共三次课后作业，包含问答题、计算题及编程题等，不允许交流合作。三次作业的权重相等。从第二周到第十三周共 12 周每周都有 1 篇课前的文献阅读理解以及 2 篇可选阅读文章，按照要求写阅读小结，平均分计入总成绩的 10%。随堂测试（闭卷）共两次，分别在第三周和第五周，分别测验 1-2 周以及 3-4 周的学习效果。两次随堂测试的权重相同。课后作业、课前阅读及随堂测试的成绩和评语在两周内反馈给学生。出勤率采取抽查的方式，上课时随机抽取学生回答问题，如果学生不在现场并且没有请假，扣除总成绩的 1%，最多扣 5%。请事假的学生可以酌情免除扣除出勤分数。最终的总成绩按百分制换算至等级制。换算关系参考下表所示：

等级	A+	A	A-	B+	B	B-	C+	C	C-	F	EXC	P	NP	N
绩点	4.0	4.0	3.7	3.3	3.0	2.7	2.3	2	1.7	0	N/A	N/A	N/A	N/A
参考百分制转换关系	95-100	90-94	85-89	80-84	75-79	70-74	67-69	63-66	60-62	0-59	根据课程规定	>=60	<60	未有成绩记录

建议如果班级规模大于 30 人，A-及以上不超过 40%，不及格率不超过 10%。

七、教材和参考书目

（需符合《上海科技大学教材选用管理办法》文件要求）

（一）推荐教材*（说明：书名、作者、出版社、出版年月、ISBN 为必填项；译者为选填项）*

推荐教材 1：

*书名：Medical Data Privacy Handbook	*作者：Aris Gkoulalas-Divanis, Grigorios Loukides	译者：	*ISBN：9783319236322
*出版社：Springer	*出版年月：2015 年 12 月	*版次：第 1 版	

推荐教材 2：

*书名：工程伦理	*作者：李正风、王前、丛杭青	译者：	*ISBN：9787302524670
*出版社：清华大学出版社	*出版年月：2019 年 6 月	*版次：第 2 版	

（推荐教材信息可复制以上表格依次添加）

（二）参考书目

参考书目 1：

书名：Ethics of Medical AI	作者：Giovanni Rubeis	译者：	ISBN：9783031557439
出版社：Springer	出版年月：2024 年 3 月	版次：2024 年版	

参考书目 2：

书名：Guide to the De-Identification of Personal Health Information	作者：Khaled El Emam	译者：	ISBN：9780429100659
出版社：Auerbach Publications	出版年月：2013 年 5 月	版次：第 1 版	

参考书目 3：

书名：Ethics and Data Science	作者：Mike Loukides, Hilary Mason, DJ Patil	译者：	ISBN：9781492043881
出版社：O'Reilly Media, Inc.	出版年月：2018 年 7 月	版次：第 1 版	

参考书目 4：

书名：Responsible Genomic Data Sharing: Challenges and Approaches	作者：Xiaoqian Jiang, Haixu Tang	译者：	ISBN：9780128163399
出版社：Academic Press	出版年月：2020 年 3 月	版次：第 1 版	

（参考书目信息可复制以上表格依次添加）

八、学术诚信教育

本课程高度重视学术诚信，严禁抄袭、作弊等行为。

“在学习、科研、实习实践等活动中，学生应恪守学术道德，坚守学术诚信，保护知识产权，坚持勇于创新、求真务实的科学精神，努力培养自己严谨求实、诚实自律、真诚协作的科学态度，成为良好学术风气的维护者、严谨治学的力行者、优良学术道德的传承者。”

（具体请参见《上海科技大学学生学术诚信规范与管理办法（试行）》文件要求，如果教师有更具体的要求，请详细列出。）

九、其他说明（可选）

（【建议文字格式】中文：宋体，小四；英文：Times New Roman，小四；1.5 倍行间距；首行缩进 2 字符。）