**身边案例：内蒙古乡镇地区医疗机构患者数据安全管理**

**案例需求分析**

**学情分析**：

在内蒙古乡镇地区，随着医疗信息化的推进，越来越多的医疗机构开始使用电子病历等信息系统。然而，由于技术水平和安全意识的限制，患者数据的安全管理成为一个挑战。学生普遍对医疗信息化和数据安全有所了解，但缺乏实际操作和深入理解的机会。因此，设计一个与乡镇医疗机构患者数据安全管理相关的案例，有助于提升学生的数据安全意识，并培养他们在实际环境中应用数据安全知识的能力。

**课标分析**：

本案例紧扣高中信息技术必修一第二模块“数据处理与应用”最后一小节“数据安全”的课标要求，通过模拟乡镇医疗机构患者数据泄露的情境，引导学生分析数据安全的重要性、识别威胁、制定防护措施，并培养学生的实际操作能力。

**教学内容分析**：

本案例将介绍数据安全的基本概念、医疗数据安全的特殊性、常见的安全威胁和防护措施。通过案例分析、角色扮演和小组讨论等方式，帮助学生深入理解数据安全在医疗领域的重要性，并提升他们的数据安全意识和技能。

**案例目标**：

1. 理解数据安全在医疗领域的重要性和特殊性。
2. 识别医疗数据面临的常见安全威胁和防护措施。
3. 能够分析医疗数据安全事件的原因，并提出相应的防护措施。
4. 通过角色扮演和小组讨论，培养学生的团队协作和沟通能力。

**案例描述**

**背景**：

内蒙古某乡镇卫生院近年来实现了医疗信息化，使用电子病历系统来管理患者数据。然而，最近发现一些患者的隐私数据被非法获取，引发了数据安全问题。

**任务**：

1. **数据泄露发现**：

卫生院管理人员发现部分患者隐私数据出现异常，如个人信息被篡改、诊断结果泄露等。

1. **原因分析**：

学生分组扮演卫生院管理人员、信息技术人员、医护人员等角色，共同分析数据泄露的原因。可能是系统漏洞、内部人员疏忽、外部黑客攻击等。

1. **制定防护措施**：

针对不同的原因，制定相应的防护措施。如加强系统安全性、提高员工数据安全意识、定期备份数据等。

引入加密技术保护患者隐私数据，确保即使数据被非法获取也无法轻易解密。

1. **实际操作与验证**：

在信息技术教师的指导下，学生进行实际操作，如设置强密码、安装杀毒软件、进行定期数据备份等。

**案例分析**：

内蒙古某乡镇卫生院在推进医疗信息化进程中遭遇了数据泄露事件，凸显了乡镇医疗机构在数据安全保护方面的挑战。通过模拟发现数据泄露并深入分析其可能原因，卫生院管理人员、信息技术人员和医护人员共同参与了问题的解决过程。这一跨部门的协作不仅提高了问题解决的效率，也增强了全体员工的数据安全意识。针对系统漏洞、内部疏忽和外部攻击等潜在原因，制定了相应的防护措施，包括加强系统安全性、提高员工意识、定期备份数据以及引入加密技术等。在信息技术教师的指导下，学生们通过实际操作验证了防护措施的有效性，增强了实践能力。这一案例展示了从问题发现到原因分析，再到制定和实施防护措施的完整过程，对于提高乡镇医疗机构的数据安全管理水平具有积极的启示作用。

**核心素养与学科逻辑体现**

**核心素养**：

1. **信息意识**：学生意识到医疗数据安全的重要性，能够在医疗信息化环境中保持对数据安全的敏感性。
2. **计算思维**：在分析数据泄露原因和制定防护措施时，学生运用计算思维进行逻辑推理和问题解决。
3. **数字化学习与创新**：学生通过实际操作和模拟验证，掌握数据安全的基本知识和技能，并能够在实际问题中应用这些技能进行创新。

**学科逻辑**：

1. **概念理解**：学生理解数据安全在医疗领域的重要性和特殊性，掌握数据安全的基本概念、威胁和防护措施。
2. **问题解决**：学生在分析数据泄露原因和制定防护措施的过程中，运用所学知识解决实际问题，提升解决问题的能力。
3. **实践操作**：学生通过实际操作和模拟验证，将理论知识转化为实践技能，加深对数据安全的理解和掌握。
4. **跨学科整合**：本案例将信息技术与医疗领域相结合，体现了跨学科整合的学科逻辑。学生通过学习数据安全知识，可以更好地保护乡镇医疗机构的患者数据安全，促进信息技术与医疗服务的融合发展。