Ethics in terms of cybercrime in healthcare can prove to be a difficult topic to discuss. It is not limited to a theoretical discussion about the pros and cons of the subject as other topics might include. In this industry, when cybercrime takes place, real people can suffer and potentially have their lives ruined. Through the research my group members and I conducted during our project to gain a better understanding of the topic, I quickly realised the extent of the damage to this critical infrastructure cybercrime can have, and consequently, the damage caused to patients themselves. Cybercrime, by definition, is by no means an ethical practice. It violates essentially all preconceived societal standards of ethics generally relating to a person's career such as respect and consideration of others, respect and adhering to the laws that govern your activities, and reducing the harm that your actions cause against other people. However, this is not to be confused with the practice of ethical hacking. Ethical hacking is the authorised and intentional penetration testing of systems utilised by an organisation by a professional using typical hacking methods for the purpose of detecting vulnerabilities and strengthening cyber resilience. The threat to society as a whole that cybercrime poses cannot be overstated, and I'd like to use this reflection to look at the ethical perspectives of the healthcare sector that this topic encompasses, and what should be done to address them.

Network intrusions with the aim of stealing sensitive or personal data in something that we have found to be the key target for threat actors in the healthcare sector. In the healthcare sector, this PHI (protected health information) data is stolen by hackers for their own personal gain. This could be through the means of identity fraud, taking stolen personal data and using it to conceal one's own identity for criminal purposes such as opening illegitimate lines of credit; ransoming necessary data relating to multiple patients' well-being such that they cannot receive effective care until the ransom has been paid; or in rare cases, manipulating the outcome of diagnosis or clinical trials such that the data is incorrect, possibly under political or wider societal motivations. These types of attacks also cause damage to the healthcare organisation in relation to their ethical policies. There are four principles of ethics related to healthcare as a whole. According to Varkey (2020), These principles include:

- Beneficence: provide palatable care and act to prioritise and benefit the patient's care and well-being
- Nonmaleficence: do no harm and do not cause offence or negative implications to a patient's quality of life.
- Autonomy: treat an individual patient's wishes with respect and respect their right to accept or deny certain medical care.
- Justice: equally distribute medical resources according to need and treat all patients with the same level of care and consideration.

These attacks perpetrated by threat actors to steal private information can prevent healthcare providers from adhering to and acting under these principles. This in turn can have the effect of a growth in distrust of the healthcare system. For example, if a hacker were to maliciously edit a patient's health records such that a debilitating illness was to be left undiagnosed or mistreated, serious injury or a negative impact on quality of life could occur. This would violate the principles of beneficence and nonmaleficence as adequate care has not been provided to the patient and what care that is provided might result in further health complications. Moreover, a hacker could steal protected health information for the purpose of identity fraud which would result in a patient’s personal life being affected. This could result in the form of significant financial distress if multiple lines of illegitimate credit or loans are abused under a patient’s name. This would also be a violation of the nonmaleficence principle, as a patient’s quality of life is negatively affected by extension.

While it may seem as though it is not the fault of the organisation, as it wasn’t their intention, it is technically their fault as it was caused by vulnerabilities within their system. Depending on the extent of their cybersecurity efforts, they may be either legally liable or not liable. However, I personally believe that regardless of their legal liability, the organisation or institution is ethically responsible for any damages suffered by patients that result from cyber attacks in cases where it was preventable. For instance, the Anthem medical data breach of 2015 where an estimated 80,000,000 customers were subject to a massive server data breach exposing social security numbers, addresses, employment and income information. It is believed that this hack was caused by threat actors obtaining stolen login credentials from a senior administrator of Anthem. It is also believed that basic security measures like two-factor authentication were neglected and could have considerably lessened the impact of the intrusion which caused the breach (Rea, 2015)

It is clear that ethical perspectives on healthcare become a difficult subject when cybercrime is introduced. The very nature of black hat hackers is unethical. In doing what they do, they go against all defined laws and ethics pertinent to the use of computer systems. The Computer Ethics Institute originally compiled a list of computer ethics that all programmers and IT professionals should adhere to, known as the “Ten Commandments of Computer Ethics”. Though quite old and comically inspired by religious texts, being originally published in 1992, the content of the code still remains relevant to modern-day computing and applicable to this topic. Of the commandments listed, the ones most violated by malicious hackers in relation to healthcare cybercrime include:

- Thou shalt not use a computer to harm other people.
- Thou shalt not interfere with other people's computer work.
- Thou shalt not snoop around in other people's computer files.
- Thou shalt not use a computer to steal.
- Thou shalt think about the social consequences of the program you are writing or the system you are designing.
- Thou shalt always use a computer in ways that ensure consideration and respect for other humans.

(Johnson, 2005)

Black hat hackers ignore this code of ethics and use their expertise to intentionally cause harm to patients and by extension, society as a whole. In doing so, they can either intentionally or unintentionally cause healthcare organisations and institutions to suffer a breach of their code of ethics through neglect of systems to protect patient privacy. To address the ethical concerns that this topic proposes, it is important to understand that the core of what causes them is cybersecurity weaknesses and vulnerabilities. The choices page in our project already defines what we believe should be done about said weaknesses. Proposed implementations like greater staff education on cybersecurity, adhesion and development of regulatory standards and best practices, and collaboration/partnership with third-party cybersecurity organisations would all contribute considerably to the combined effort of robust and reliable systems to safeguard patient data.

The future of cybercrime is only expected to grow in scope and severity. If healthcare organisations are to uphold their code of ethics against criminals who ignore their own, it is imperative that they take strong affirmative action to bolster their defence for the continued longevity of their industry.

Sources:

Varkey, B. (2020). *Principles of Clinical Ethics and Their Application to Practice*. *30*(1), 17–28. https://doi.org/10.1159/000509119

Rea, S. (2015, February 14). Anthem Hack: Was It Preventable? Digicert.com. https://www.digicert.com/blog/anthem-hack-preventable

Johnson, C. (2005, May 6). CPSR - The Ten Commandments of Computer Ethics. Cpsr.org. http://cpsr.org/issues/ethics/cei/