

# **POLICY REGARDING PEER-TO-PEER FILE SHARING PROGRAMS AND PROTECTED HEALTH INFORMATION**

## **INTRODUCTION**

The United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA) to ensure the security and privacy of patient records. These laws mandate that healthcare institutions take the necessary steps to protect patient information, especially electronic data and the risks associated with these Peer-to Peer (P2P) applications.

The HIPAA Privacy Rule requires all organizations that handle protected or patient health information (PHI) to put in place administrative, physical and technical safeguards for PHI in all forms, including electronic media. The recently published Security Rule focuses on electronic PHI to further stress the importance of protecting health information. This policy is designed to reduce the risk of violating confidentiality requirements due to insecure file sharing.

## **SCOPE**

The scope of this policy includes all computer systems within a Covered University Unit<sup>1</sup>. All students, faculty, staff, vendors and contractors who have access to electronic PHI are subject to this policy.

## **POLICY**

P2P file sharing applications within the University are prohibited on all systems with access to PHI. P2P file-sharing applications allow users to covertly communicate and share virtually any file with an unauthorized party. File-sharing programs, such as *KaZaA*, *Napster*, *Gnutella*, *iMesh*, *CuteMX*, *Scour Exchange*, and *FreeNetfile* can easily locate open computer ports on a firewall to defeat blocking attempts. The existence of these programs on a machine with access to PHI places the user in violation of this policy.

## **NEGATIVE EFFECTS OF FILE SHARING**

Beyond the unintentional or deliberate sharing of sensitive information, peer-to-peer file sharing can expose the University to security risks that directly cause or indirectly facilitate HIPAA violations. These violations can occur through a variety of ways including:

- Files downloaded from P2P networks may contain viruses, worms, or hostile code. CUU's with any P2P users may be at risk as viruses and worms can spread undetected to a co-worker on the network.
  - *This would violate the HIPAA requirement for guarding against malicious software.*

- Vulnerabilities in P2P applications may allow hackers to illegally access and alter PHI.
  - *This would violate several HIPAA requirements pertaining to accessing and maintaining the integrity of PHI.*
- Spyware contained in P2P programs may allow the unauthorized collection and distribution of PHI or other confidential information.
  - *These programs are a part of the standard installation of Morpheus, KaZaA, and Bearshare. Exploitations using spyware would constitute a HIPAA access violation.*
- P2P file sharing programs may hinder network performance causing valuable information to become unavailable on the network.

## COMPLIANCE

Violations of this policy should be reported to the HIPAA Security Officer at 919-9626041 or [hipaa@unc.edu](mailto:hipaa@unc.edu). Systems in violation of this policy may be denied network access.

The failure to comply with Information Security Policies and Standards may result in disciplinary action, up to and including dismissal, in accordance with applicable University procedures, or, in the case of outside affiliates, termination of the terms of affiliation. Failure to comply with Policy Regarding Peer-To-Peer File Sharing Programs And Protected Health Information by students may constitute grounds for corrective action in accordance with University procedures.

## ADDITIONAL INFORMATION

If you have installed a peer-to-peer file sharing application and need assistance to remove the application consult your departmental support person or contact the University Response Center at 962-HELP, or send an e-mail message to [help@unc.edu](mailto:help@unc.edu)

If you have questions and would like additional information, *you may email [HIPAA@unc.edu](mailto:HIPAA@unc.edu), or you may contact the University HIPAA Security Officer.*

*General University HIPAA information is available on the web at [www.unc.edu/hipaa](http://www.unc.edu/hipaa).*

### **Other related policies and standards:**

- **UNC-Chapel Hill Data Network Acceptable Use Policy**
- ***[UNC-Chapel Hill Privacy of Protected Health Information Policy](#)***
- **Information Security Policy**
- ***[UNC-Chapel Hill Basic Computer Security Checklist](#)***
- **Copyright Policy**