Guidance on the Use of R and RStudio

R and RStudio are powerful open-source software tools widely used for data analysis, statistical modeling, and data visualization. R is a programming language, while RStudio is an integrated development environment (IDE) that provides a user-friendly interface for working with R. These tools offer essential capabilities for researchers, data analysts, and statisticians to process and visualize data, enabling informed decision-making and valuable insights.

Ann & Robert H. Lurie Children's Hospital is actively developing a risk management framework to ensure the appropriate and secure use of R and RStudio within the organization. This framework aims to align with legal and regulatory requirements to safeguard patient and confidential information.

As we develop our risk management framework, this guidance serves as a crucial interim measure to protect sensitive information and maintain the highest standards of data security.

1. **Avoid Cloud-Based RStudio**
   Posit provides a cloud-based RStudio environment that is not approved for use by Lurie staff. Do not enter or upload any patient, personally identifiable, or confidential information into cloud-based versions of RStudio. Do not enter or upload any patient, personally identifiable, or confidential information into cloud-based versions of RStudio. This practice is essential to uphold internal regulatory standards and protect sensitive data from unauthorized access.

2. **Managed Installation on Devices**
   Ensure that the installation of R and RStudio on organizational devices is performed by the IM department and not by individual end-users. This ensures consistency and adherence to organizational security standards.

3. **Adherence to Information Security Policies**
   Follow information security policies, standards, and processes that <u>do not</u> permit downloading unauthorized software or plugins onto organizational equipment. This minimizes potential security risks and prevents unauthorized access to sensitive data.

4. **Download Packages from Trusted Sources**
   Only download R packages from reputable sources: Comprehensive R Archive Network (CRAN) and Bioconductor. These trusted repositories provide vetted packages, reducing the risk of downloading malicious or compromised software. Ensure you are using an official CRAN mirror for package installation (https://cran.r-project.org/mirrors.html).

5. **Use HTTPS when downloading packages.**
   All CRAN and Bioconductor mirrors support the HTTPS protocol for downloading packages. Using HTTPS limits the risk of man-in-the-middle attacks and is a security best practice. R is configured to use HTTPS in v3.2.2 (released 2015) and later, and should not be disabled.

6. **Be Vigilant for Information Security Risks**
   Be on high alert for phishing emails and other risks to information security. Cybersecurity threats can compromise the confidentiality and integrity of data, so it is essential to remain vigilant and promptly report any suspicious activities.