DIVISION OF INFORMATION TECHNOLOGY – HEALTH INFORMATION TECHNOLOGY

Howdy,

To protect the confidentiality, integrity and availability of university data, sensitive information must be properly secured. As part of the university's information security program, university-owned computing devices are scanned for files containing sensitive information.

The TAMU device assigned to you (**##-#######**) has at least one file that has been identified as possibly containing sensitive information. You may forward this notice to HealthTechCare@tamu.edu to have an IT technician either move or remove data.

> **File(s):** [C:\Users\username\documents\document.txt] and/or [See Attached]
>
> **Data Type:** [Social Security Number] and/or [Health Information]
>
> **Action Required:** Please review the file(s) in this notice and reply to report the status within seven (7) business days

If this is your personal data, please remove the information from your system or store it in a place that is not a university-owned asset.

If this is university data, please move the data from your system and store it in "OneDrive – Texas A&M University" or on a network share. You may also store it in Teams or a SharePoint site.

Make sure the Recycle Bin/Trash has been emptied.

If the information is required for business purposes, please ensure the data is properly encrypted and secured as per University Control SC-13.

Once action has been taken or the data has been removed, please reply to this email.

View the Spirion Sensitive Data Manager knowledge base article for more information. Please also visit the Safe Computing guides for more tips.

If you need further assistance, please contact the Health Technology Care Team at HealthTechCare@tamu.edu, 979.436.0250 or 979.845.8300 (Option 2). You may also visit our website.

Thank you for partnering with the Division of IT to ensure that university data is safe.

Texas A&M Division of Information Technology – Health Information Technology