To: Peter Lennie, *Provost & Dean of the Faculty of Arts, Sciences & Engineering*

From: Julie Myers, *Associate CIO*
Mike Pinch, *Chief Information Security Officer, URMC*

Cc: David E. Lewis, *Vice President for IT & Chief Information Officer*
Jerry Powell, *Associate Vice President and CIO, URMC*
Jonathan Maurer, *Chief Information Security Officer*

Date: April 20th, 2016

Re: Personal Information Collection and Retention

This memo is in response to your request to explain the University's practice for the collection and retention of personal information and electronic communications (e.g. e-mail, website usage). University Information Technology was asked to document the types of information collected, data collection practices, the retention period for collected data, and the policies that govern privacy and the use of such information by the University. The discussion below covers services managed by University Information Technology (UIT) and the Information Systems Divisions (ISD). It does not cover departmental IT administrative practices and policies, nor all affiliate hospital practices and policies.

Personal Information:

University-related faculty and staff personal information is stored on secured University managed and contracted systems. A limited number of UIT and ISD staff members have administrative privileges on these systems. This access allows these staff members to view personal information when necessary to effectively manage these services. The number of staff members needing this type of access is reviewed and approved regularly. To ensure awareness of and compliance with University policy, employees in both UIT and ISD are given annual updates to training and/or sign off on acknowledgement of responsibilities. This additional agreement explicitly states that such accounts may only be used as business needs dictate, and not for personal gain.

Health Information:

The employee health plan does not maintain protected health information (PHI) about its employees. The University uses two third party administrators (TPAs) , Aetna and Excellus, who manage and maintain information about health care claims and use the information as needed to manage care and improve employees' health.

Personal Communications:

UIT and ISD policies distinguish between two types of monitoring activities for electronic communications and web activities. The first involves the examination of system content or network traffic, including the content of personal communications. The second focuses on the monitoring of network, application, and computer logs, and does not involve evaluation of the content of communications. Specific rules and regulations authorize UIT and ISD to conduct each type of monitoring.

Inspection of the content of personal communications occurs only when necessary to support University operations, to protect University information from malicious intent, and to ensure compliance with federal, state, local and industry regulations. As a result, the Medical Center may be required to implement more restrictive controls for its population. Authorization for review occurs on a case-by-case basis at the formal request of the responsible University unit. The conditions under which this occurs are outlined in IT policy:

> *According to this policy, an employee's personal information/communications may be examined at the formal request of University Counsel, University Audit, or legal authorities; to investigate or prevent a violation of law or University Policy; to protect health or safety; and to minimize or stop computer activity that interferes with the University's network or other computer operations.*[1]

When inspecting personal communications, UIT and ISD always take appropriate measures to safeguard collected information from inappropriate use by outside attackers and University employees.

UIT and ISD do routinely monitor network, application, and computer logs to appropriately maintain system operations and performance, comply with legal regulations, and to prevent, detect, and respond to threats to the organization. For example, logs are monitored to proactively protect the University against known information security threats or to conduct investigations on

[1] University IT policies are available at http://www.rochester.edu/it/policy/index.html.

security incidents. This type of routine monitoring does not normally extend to examining the content of personal communications.

ISD also routinely monitors and audits Electronic Medical Records (EMR) to track access to sensitive patient information. This monitoring exists to protect patient privacy in accordance with federal regulations.

In all cases, UIT and ISD work closely with other University departments including Audit, Legal, Privacy and IT Security Governance Groups (Data Security Task Force / Privacy and Security Executive Committee) to ensure the appropriate controls are in place and adhered to.