Code: IM:0038

Subject: E-Mail Usage

Responsible Department, Division Or Committee
Information Technology

Policy:

Stony Brook University Hospital (SBUH) workforce members will utilize the e-mail system and other communication system networks for approved purposes and in an appropriate manner as defined in the procedures contained in this policy.

Definitions:

Protected Health Information (PHI) - Any information, including but not limited to, specimens, radiographs, photographs, any portion of the paper or electronic medical record or research data that contains patient identifiers; such as name, medical record number, social security number, date of birth, encounter number, test results, diagnoses, dates when services were provided, dates of admission, dates of discharge, date of death, etc., that relates to the past, present or future physical or mental health condition of an individual, the provision of health care to an individual, or payment for the provision of health care to an individual. This definition applies to information that is spoken, written or electronic in form and either directly identifies the individual or could reasonably be used to identify the individual. Any form of information that can identify an individual who has received, is receiving or will be receiving health care.

Workforce - An employee, volunteer, trainee, or other individual affiliated with SBUH whose work is under the direct control of SBUH regardless of whether they are paid by SBUH.

SBUH operational information - Administrative, financial, legal, regulatory and quality improvement activities that are necessary for SBUH to conduct health care related business activities and support the core functions of treatment and payment. These activities include but are not limited to: quality assessment, quality improvement and patient safety activities, population-based activities to improve health care or reduce costs, protocol development, case management, care coordination, contacting providers or patients with information about treatment alternatives or options, reviewing competence, performance or qualifications of health care professionals including but not limited to potential misconduct, reviewing performance of health plans, conducting training programs for students, employees or non-health care professionals,
accreditation, certification, licensing or credentialing activities, fraud and abuse
detection and compliance monitoring, conducting medical review, legal counsel services,
to meet regulatory requirements, auditing activities, business planning and development,
business management, general administrative activities (creating de-identified health
information or a limited data set, fundraising, some marketing activities, customer service
and internal grievance resolution).

Procedures:

A. e-mail is to be used for Hospital business and should not be misused. e-mail is an efficient
way to send urgent messages for those designed to communicate with multiple people
simultaneously. SBUH workforce members will use extreme caution to ensure that the correct
e-mail address is used for the intended recipient(s).

B. Users must not use an electronic mail account assigned to another individual to either
send or receive messages, unless the original individual delegates such rights under user
access privileges from the users own e-mail account.

C. For security and network maintenance purposes, authorized individuals within the
Hospital's Information Technology Department may monitor equipment, systems and network
traffic at any time, in accordance with the Information Technology Department's audit
procedure. The Hospital reserves the right to audit networks and systems on a periodic basis
to ensure compliance with this policy.

D. The Hospital may access and monitor e-mail at any time for any reason without notice.
SBUH workforce members should not expect or treat e-mail as confidential or private. Except
for Hospital personnel authorized by Legal Counsel or Human Resources, no one is permitted
to access another person's e-mail. Password sharing is not permitted. SBUH workforce
members will ensure their unique username and password is secure from co-workers and
anyone else that asks about the password. Authorized users are responsible for the security
of their passwords and accounts.

E. System users should exercise extreme caution, good judgment and common sense when
distributing messages.

F. Confidential SBUH operational information must NEVER be disseminated via email outside
the Hospital network to an unauthorized source(s).

G. Protected Health Information (PHI) is strictly prohibited from being sent via e-mail outside
the Stony Brook network to another email provider such as aol, gmail, hotmail, optonline, a
vendor email account or other health system email account.

H. SBUH workforce members will abide by copyright laws, ethics rules, quality privilege and
other applicable laws.

I. The use of the Stony Brook email system to solicit for any purpose without the
authorization of the CEO or the CEO's designee is strictly prohibited.

J. Users must be aware that the majority of viruses are transmitted via e-mail. If you
receive any suspicious email (spam, phishing attempts) or if the sender is not familiar to you;
do not open any attachments or click on any links contained in the suspicious email and
contact the HELP Desk immediately for further instruction.
contact the HELP-Desk immediately for further instruction.

K. Sending harassing, abusive, intimidating, discriminatory, or other offensive e-mails is strictly prohibited. If a SBUH workforce member receives a message containing defamatory, obscene, offensive or harassing information, or that discloses personal information without appropriate permission/authorization, the workforce member will immediately contact the Compliance Office or call the Compliance Helpline and will not delete the message or forward it unless otherwise instructed to by the Compliance Officer.

L. Auto forwarding of SBUH official e-mail system to any other e-mail system is not permitted.

M. The SBUMC Outlook email system will be programmed to contain the following statement: 

Note: This SBUH e-mail message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by e-mail and destroy all copies of the original.

N. The confidentiality message above will only appear in the first email transmission (or at the bottom of an email thread). Therefore, the following message must be included in a user's signature line: This email is subject to the confidentiality provisions noted below. The statement may be copied and pasted into the SBUMC Outlook user's signature line. Contact the HELP-Desk for assistance and/or instructions on how create/update signatures in the SBUMC Outlook system.

O. Sanctions: SBUH workforce members engaging in the transmission of inappropriate e-mails or using another user's ID or password, as determined by the Hospital's Information Security Officer, will be subject to discipline, up to and including termination.

Forms:

Keywords:
e-mail, notes, monitoring, audit, access, PHI, password, confidential

Policy Cross Reference:
IM:0021 ID and Password Assignment for Computer System Access

Relevant Standards, Codes, Rules, Regulations, Statutes:
Federal Regulations: Department of Health & Human Services Security Standards; Final Rule February 20, 2003; 45 CFR Part 164.530 (C)(1){82827}, 164.530 (D) (2) {82827} and 142.308 (B) {43268}


Scope: Hospital Wide

Author: Last Review Date: 8/12/2011
Effective Date Original Policy: 3/31/2003
Effective Date Revised Policy: