Course Syllabus p. 1

UMA Technical Skills

Instructor: Eric Clift
E-mail: clifte@ohio.edu
Phone: 740-593-2514

Course Description

This course will give you a base knowledge of the technical skills required to function in the University Medical Associates (UMA) medical office setting. This course can be viewed at any time either in its entirety or in particular sections, depending upon the end user’s needs.

Course Objectives

By the end of this course, you should be able to:

1. Configuring Internet Explorer 11 for use with Athena Clinicals.
2. Access your UMA GoDaddy email via Outlook 2010/2013
   i. Add a .PST file to Outlook 2010
   ii. Create a signature file in Outlook 2010/2013
   iii. Create a contact group in Outlook 2010/2013
3. Use the Identity Finder/TrueCrypt software to scan/encrypt your computer for sensitive data.
   i. You will be able to permanently delete data
   ii. Encrypting sensitive data.
4. Use Secunia and Windows Updates to keep your computer up-to-date on the most current security patches.

Your Reading Material

This course does not use a textbook. You will be reading Internet articles, eGuides and presentation material on the various topics.

Course Outline

Below is an outline of the content and activities in each unit of the course.

Week 1: Configuring Internet Explorer 11 for Athena HER

1. Setting trust sites security level
   a. Adding links to trusted sites
2. Configuring pop-up blocker
3. Adding sites to compatibility settings
4. Using auto-configuration link on Athena site
Week 2: Use Secunia and Windows Updates

1. Configuring Windows Updates in Windows 7
2. Installing and Configuring Secunia

Week 3: OU Identity Finder and TrueCrypt

1. Installing OU Identity Finder
2. Scanning your PC for sensitive data
   a. Deleting sensitive data
3. Installing TrueCrypt
   a. Encrypting data

Week 4: GoDaddy email access

1. Setting up GoDaddy email on Outlook 2010/2013
   a. Add a .PST file to Outlook 2010/2013
   b. Create a signature file in Outlook 2010/2013
   c. Create a contact group in Outlook 2010/2013

Assessment

There will not be a graded assessment for this course, but you are expected to complete the summary assignment at the end of each week. This summary will help you to know if you understand the week’s material.

UMA Computer and Network Use Policies

Access to computer systems and networks owned or operated by UMA impose certain responsibilities and obligations and is granted subject to UMA policies, and local, state, and federal statutes.

Access to the UMA’s computing facilities and resources is granted solely to UMA physicians, nurses, staff, and individuals or entities outside UMA who are authorized to use services that have been made available through UMA. UMA reserves the right to limit, restrict, or extend computing privileges and access to its resources.

Computers and network resources can provide access to resources both on and off UMA property. Such open access is a privilege, and requires that individual users act in a responsible and acceptable manner. Acceptable use always is ethical, reflects honesty, and shows restraint in the consumption of shared resources. Acceptable use demonstrates respect for intellectual property, truth in communication, ownership of data, system security mechanisms, and individuals’ right to privacy and freedom of intimidation, harassment, and unwarranted annoyance. UMA considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to test and monitor

security, and copy and examine any files or information resident on UMA systems allegedy related to unacceptable use.

Those who do not abide by the policies and guidelines listed below should expect at least suspension of computer privileges and possible disciplinary action in accordance with UMA policy and existing judicial, disciplinary, or personnel processes. Offenders may also be subject to criminal prosecution under federal or state laws, and should expect UMA to pursue such action.

The office of the Designated Approving Authority (DAA) contact and the office of the Assigned Security Responsibility (ASR) contact will be notified of any violations of computer laws and policies, as well as any potential loopholes in the security of its computer systems and network. The user community is expected to cooperate with UMA Administration in their operation of computer systems and networks as well as in the investigation of misuse or abuse.

Any portable computing device (PCD) (ie…laptop, tablet, smart phone, etc.) used to access UMA patient information cannot be used to store patient information without written consent from the Chief Executive Officer of UMA. PCDs must be password protected. Users will logoff systems when not in use and all devices will have unattended lock out protection of 10 minutes or less.

Resources will not be applied to computer systems or peripherals deemed as obsolete or the repair exceeds the value of the system.

All UMA computing, network, printing, and information resource devices will be disposed of through designated UMA Information Technology personnel. Only approved information technology (hardware or software) purchased, inventoried and contracted through UMA will be supported. Any non-supported information technology can be denied resource access.

### UMA Procedures

UMA computers, networks, and other information resources (i.e., Athena Web Portal, Web pages and other information servers) may not be used in any manner prohibited by law or disallowed by licenses, contracts, or UMA regulations. Organizations, physicians, staff, and individuals are accountable for the information they publish across computing resources, and they must be aware of UMA, Health Insurance Portability and Accountability Act (HIPAA) and Family Educational Rights and Privacy Act (FERPA) policies regarding confidential information, harassment, use of UMA personal computing devices, and intellectual property.

#### I. Required Activities

In making acceptable use of resources, you must:

Use resources only for authorized purposes.

Protect all of your login IDs and systems from unauthorized use. Individuals are responsible for activities on their login ID or that originate from their system.

---

Access only files and data that are your own, which are publicly available, or to which you have been given authorized access. Be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

II. Violations of Policy
In making acceptable use of resources, you must NOT:
Provide login ID codes and system access for the purpose of using resources in violation policy, or in violation of Federal, State and/or local statutes.
Use copyrighted images, text, or software without permission or in violation of the copyright laws of the United States, or violate terms of applicable software licensing agreements.
Use resources to engage in any illegal activity.
Use resources for private financial gain or compensation or for partisan political purposes.
Use resources to intimidate or single out individuals or groups for degradation or harassment in violation of federal or state law and other UMA policies.
Use resources to provide materials whose nature or volume compromise the ability of the server to serve other users' documents.
Use a computer account for which authorization has not been granted, use the network to gain unauthorized access to any computer system, attempt to circumvent data protection schemes or uncover security loopholes, or mask the identity of an account or device.
Knowingly perform an act that will interfere with the normal operation of computers, terminals, peripherals, or networks, including (but not limited to) knowingly running or installing on any computer system or network, or give to another user, a program intended to damage or to place excessive load on a computer system or network. This includes programs known as computer viruses, Trojan horses, and worms.

III. Possible Penalties
Misuse of computing, networking, information, or World Wide Web resources may result in the loss of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Offenses that are in violation of local, state, or federal laws may be reported to the appropriate law enforcement authorities. Users may be held accountable for their conduct under any applicable UMA policies, or procedures. Complaints alleging misuse of computer resources will be directed to those responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment. Violators will be subject to UMA rules and regulations.

IV. Additional Use Policies
Additional use policies and terms and conditions may be in place for specific electronic services offered by UMA, such as the World Wide Web, Electronic Health Records, and Confidential Patient Data. You must familiarize yourself with any of these when you agree to use these services.
Extra Assistance

Please feel free to contact the OU-HCOM Technical Services Department (740) 593-2169 for immediate assistance or consultation.

Citations