# *Welcome!*

It is with great enthusiasm that we welcome you to University Health System!   As a valued team member, you will help us to pave our way into the future. You are truly our greatest asset, and we could not accomplish what we do without your support and dedication.

As part of the pre-employment process, please visit **UniversityHealthSystem.com/Welcome**.  You will find important information that will ensure a great beginning with University Health System.

Your official start date is contingent upon clearance of the pre-employment process.   Once all clearances are received, you will be contacted to confirm your start date and applicable orientations.  Employment does not begin until you have received notification of clearance from Human Resources.

The following instructions are designed to assist you in completing the new hire paperwork.  If you need additional assistance or clarification, please do not hesitate to speak to one of our Human Resources Representatives.

| | |
|---|---|
| **Employment  Letter:** | This document outlines details of the offer.  Please sign and date the letter. |
| **FLSA Notification:** | This document describes your exemption status under the Fair Labor Standards Act. Please sign and date the form. |
| **Agreement of Health Insurance Coverage:** | As stated in the University Health System Employee Handbook, all regular, full- and part-time employees budgeted to work at least 20 hours per week, must elect some form of health insurance coverage or provide proof of other coverage elsewhere to avoid being defaulted to employee only coverage under the University Family Care Plan. Employees must enroll within 30 days of the date of hire.  Please sign the form.  Please provide proof of alternative health care coverage if declining coverage. |
| **Referral Sources:** | How did you hear about us?  Your feedback is important!  Please check all boxes that apply. |
| **Direct Deposit Form:** | If you wish to elect direct deposit, please complete this form. Check the appropriate box and complete either the savings or checking account field. Attach a voided check to the form. |

University
Health System

# Welcome!

| | |
|---|---|
| **Immigration (I-9) Form:** | Completely fill out Section 1. Sign and date at the end of Section 1. For Section 2, you must present either one item from list A (see back of the form) *OR* one from list B and one from list C. |
| **W-4:** | Please complete the form. **Note: The address indicated must be a local address.** |
| **Texas Public Information:** | Please read this document carefully. Check the desired option. Print, sign and date the bottom of the form. |
| **New Hire Questionnaire:** | Please complete the entire document. |
| **Information System Confidentiality Agreement:** | Please read this document carefully. Sign and date the document. A Human Resources Representative will serve as the witness. The Information Access and Security policy is available for your review at UniversityHealthSystem.com/Welcome. |
| **Pyxis Access Form**: (if applicable) | If you accepted employment as a LVN or RN, please complete this form. |
| **Statement of Consent Influenza Requirement:** | Please read this document carefully. Print, sign and date the form. |
| **eLearning:** | Please complete the eLearning requirements within *two weeks* from your date of hire. You may find the eLearning instructions at UniversityHealthSystem.com/Welcome. |

## Documents to bring to your next pre-employment visit:

- ☐ All required licenses/certifications – original documents. _____
- ☐ Voided check or deposit slip if you are electing direct deposit.
- ☐ Identification for the I-9 form. _____
- ☐ Vehicle registration or title and proof of insurance for parking permit.

**University Health System**

# ORIENTation EXPRESS

As a part of your orientation to University Health System, you will be attending ORIENTation EXPRESS. The dates for this orientation will be given to you by Human Resources or your supervisor. Some important information to know about this:

## ▶ Dress Code

Orientation days are considered work time, so acceptable attire can range from business to business casual. Business casual means clean, neat, professional clothing. Anything you would wear to the gym, beach, bar, or to clean the garage should not be worn.

| _Examples of acceptable attire_ | _Examples of unacceptable attire_ |
| --- | --- |
| Suits and ties | Shorts |
| Pantsuits | Jeans |
| Khaki pants and a shirt | Open-toed shoes and sandals |
| Socks/stockings and shoes | Beachwear |
| Clean, scuff-free athletic shoes | Exercise clothing |
|  | T-shirts other than those endorsed by the Health System |
|  | Anything too revealing |

## ▶ Schedule

ORIENTation EXPRESS is held in the 3rd Floor Foundation Room at University Health Center - Downtown (UHC-D), beginning promptly at 8 a.m. Due to the nature of this program, if you arrive late, you will need to wait to attend the next regularly scheduled orientation session.

## ▶ Directions to University Health Center - Downtown
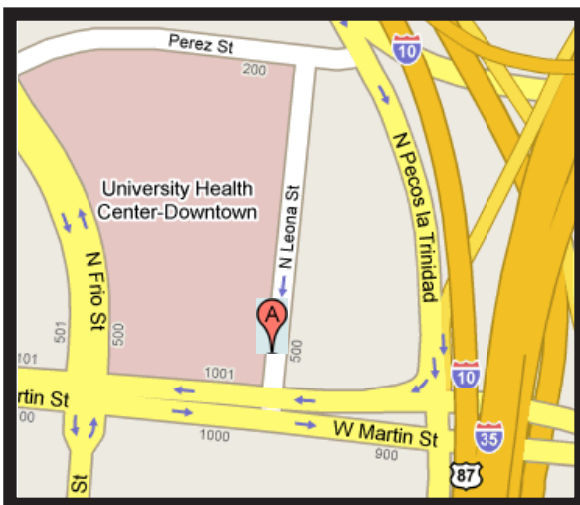


From University Hospital:
 -Take IH-10E (upper level)
 -Exit Santa Rosa St./Downtown
 -Turn right on Perez St.

The UHS employee parking lot is located on your right on Perez St. The security gate will be open until 9 a.m.

Use the University Health Center-Downtown employee entrance located directly across Perez St. Signs will direct you to the 3rd Floor Foundation Room.

**University Health System**

# Other Orientations

▶ *Departmental Orientation*

Once you start work in your department or unit, you will begin the departmental orientation. Topics that will be covered during your departmental orientation include:

- your job description
- time and attendance
- receiving pay
- paid time off
- the performance evaluation  process
- departmental safety program
- personal appearance/uniform requirements/dress code
- where and how to record your time
- other topics appropriate to your employment

▶ *Nursing Orientation to Clinical Excellence (NOCE)*

If you are a nurse in a clinical position, as part of your orientation, you may need to attend Nursing Orientation to Clinical Excellence. The dates of nursing orientation will be shared with you by Human Resources. The dress code for nursing orientation is the same as for ORIENTation EXPRESS.

University
Health System

# Parking Information

Parking at University Health System facilities is limited, therefore it is important for all of us to follow the parking rules and regulations to be sure everyone has an opportunity to park. We are in the process of upgrading our parking facilities to meet the rising demand for patient, visitor and staff parking.

- You are required to comply with all Health System parking regulations.
- Your vehicle must be registered with the Health System through the Department of Police/ Protective Services, Employee Registration and Identification, located on the sub-level of University Hospital.
  - To register your vehicle, you must provide proof of insurance and a copy of your vehicle registration or title.
  - Your vehicle hangtag must be displayed in your vehicle at all times.
  - Please park only in authorized areas. Parking is prohibited in/on: fire lanes, red curbs, patient loading and unloading areas, or areas where your permit is not authorized.

- University Health System provides sanctions for employees who violate the parking policies and regulations. These include:
  - Written Health System parking violations
  - Justice of the Peace citations for motor vehicle code violations
  - Booting of vehicle
  - Towing of vehicle
  - Possible termination for excessive violations

- If you park in a paid visitor parking area or in a paid employee parking area at any time (other than the listed exceptions) and are not paying, this is considered theft of service by the Health System. Appropriate criminal charges may be filed and may result in termination.

**University Health System**

## Facility-Specific Parking Information

▶ *University Hospital*

All employees must park in the employee B or C lots, with two exceptions:
- Third-shift employees may park in the visitors' parking lot after 10 p.m. If you stay past your normal shift, please contact your supervisor for the appropriate form to allow you to leave the lot without paying.
- Employees pay $14 per pay period to park in the employee parking garage. You may sign up for paid employee parking; however, there is a waiting list.
- Parking in any other areas without prior authorization form Police/Protective Services is prohibited.

If you enter the parking areas and lots B and C are completely full, proceed to the visitor parking lot entrance.
1. Pull a ticket.
2. Park on the roof of the garage (4th level only).
3. Sign your parking ticket and show your badge upon exiting the lot.

If you work at another facility and are at UH for official business (meeting, training, etc.), enter through the visitor's lot and park on the roof of the garage. Sign your parking ticket and show your badge upon exiting the lot. If you are here for a medical appointment or treatment, you must pay for parking. House staff physicians are only authorized to park on the 3rd level of the physician's parking garage or the 4th level of the employee parking garage.

## Ambulatory Clinics

▶ *University Health Center – Downtown (UHC-D)*

- Employees permanently assigned to UHC-D can obtain parking hangtags and access cards at Employee Registration and Identification, University Hospital.
- All employees must park in the employee parking lot located on Perez Street.

University Health System

- Employees assigned to second shift may park in the rear area of the visitors' parking lot located on Leona Street after 2:30 p.m.
- Parking in any other areas, without prior authorization from Police/Protective Services, is prohibited.

▶ *University Center for Community Health (UCCH)*

- Employees permanently assigned to UCCH can obtain parking hangtags at Employee Registration and Identification, University Hospital.
- All employees must park in the designated employee parking area.
- Parking in any other areas, without prior authorization from Police/Protective Services, is prohibited.

▶ *University Family Health Center Southeast, Southwest, North and Northwest*

- Employees permanently assigned to other facilities can obtain parking hangtags and at Employee Registration and Identification, University Hospital.
- All employees must park in the designated employee parking area.
- Parking in any other areas, without prior authorization from Police/Protective Services, is prohibited.

▶ *Parking at the facilities served by Detention Health Care Services*

- Parking at Adult and Juvenile Detention facilities are governed by that facility.
- Please contact facility personnel for proper parking location, registration, and other information.

Please contact the appropriate protective services office for assistance or if you have any questions regarding parking or security issues.

**University Health System**

Walgreens

Construction
Area

Wurzbach Rd

**West
Parking
Garage**
Patient and Visitor Parking

On Levels
G & 1

Medical Drive

Construction
Area

P

PEDESTRIAN WALKWAY

Construction
Area

PEDESTRIAN WALKWAY

PEDESTRIAN WALKWAY

Merton Minter Blvd.

Emergency
Center

P

P
Main
Entrance

**University
Hospital**

Shuttle Bus Stop

Elevators

11/2011

# Robert B. Green Campus



N Frio St

Staff North Parking Lot

Visitor Parking Lot

Perez St

Special Permit Parking

Morales St

N Leona St

A

Staff West Parking Lot

N Medina St

B

C

Construction Zone

Martin St

# Notification of Workers' Compensation Insurance

University Health System has Workers' Compensation Insurance coverage through 1-2-1 Claims to protect you. You can get more information about your workers' compensation rights from any office of the Texas Workers' Compensation Commission, or by calling (210) 593-0070.

You may elect to retain your common law right of action, if, no later than five days after beginning employment, you notify University Health System in writing that you wish to retain your common law right to recover damages for personal injury. If you elect your common law right of action, you cannot obtain workers' compensation income or medical benefits if you are injured.

For any questions, please contact Guadalupe Grijalva at (210) 358-2911.

University Health System tiene seguro propio para compensación de trabajadores.  Para mas informacion sobre sus derechos de compensación para trabajadores llame a la Línea Directa de Asistencia para el Trabajador Lesionado puede llamar al (210) 593-0070.

 Usted puede elegir retener su derecho de acciones bajo la ley comun si dentro de cinco dias de comenzar su empleo usted notifica en escrito a University Health System que desea retener su derecho.  Si usted elige retener su derecho de acciones bajo la ley comun no recibira pago por sus cuentas médicas si usted se lesiona en su empleo ni reemplazo de la pérdida de su salario.

Para cualquier pregunta que tenga llame al la oficina Compensacion al numero (210) 358-2911.

University
Health System

## Information, Instructions and Hints for
## Completing the eLearning Requirements

▶ *General Information*

Welcome to University Health System (UHS). If you are new to the healthcare industry, you will quickly come to realize that we are required to comply with comprehensive rules and regulations. You will learn a lot about these requirements during the general orientation for UHS. In fact, one of the requirements placed on UHS is that all new employees must complete a general orientation. The information covered in the general orientation is designed to familiarize you with University Health System, and provide the information that everyone needs to know to work safely and efficiently while accomplishing our goal of providing excellent patient care.

▶ *New, Full-time Employees (and others, at the request of their supervisors)*

Your general orientation consists of two separate requirements:

1. a classroom portion that we call ORIENTation EXPRESS, and
2. a series of eLearning lessons (eLearning is sometimes referred to as online training.)

You will be notified when and where you are scheduled to attend ORIENTation EXPRESS. A series of speakers will provide you with valuable information about University Health System, how we think, and how we function.

The eLearning lessons will provide information on many of the rules and regulations that we must comply with, as well as general information on a variety of topics. You must complete the eLearning lessons during your first two weeks of employment. You may take them at your own pace and schedule. These lessons are accessible from any computer connected to the UHS intranet (including computers that are able to access the UHS intranet remotely), and are available at all times.

**University
Health System**

▶ *Part-time, Float Pool, or Full-time Previous Employees Returning to the Health System within One Year of Departure*

Your entire general orientation will be completed online under the heading of **Self-Study Orientation**.

Anyone who needs assistance using the computer to take the eLearning lessons will receive help from their own department, and from the UHS eLearning staff when necessary.

The remainder of this document will provide all the information you need, including step-by-step instructions, to successfully complete the eLearning required as part of the general orientation. First, there will be some general information and helpful hints about eLearning at UHS, then step-by-step instructions for accessing and taking the eLearning.

Please keep the following information in mind while taking the eLearning.

1.  You must complete the lessons assigned for general orientation within two weeks of beginning work at UHS.
    The lessons required for general orientation are listed under ttwo heading:
    • **(UHS–Not CFHP) Required for new employees for General Orientation** for UHS employees**.**
    • **(CFHP EMPLOYEES ONLY) Required for new employees for General Orientation** for CFHP employees.
    You may be required by your department to complete other lessons, but only the ones listed under this heading are required to be completed within two weeks of beginning work at UHS. If you have been provided the option of completing the Self-Study Orientation, you must complete the lessons listed under the heading of Self-Study Orientation. These lessons must be completed within two weeks of beginning work at UHS.
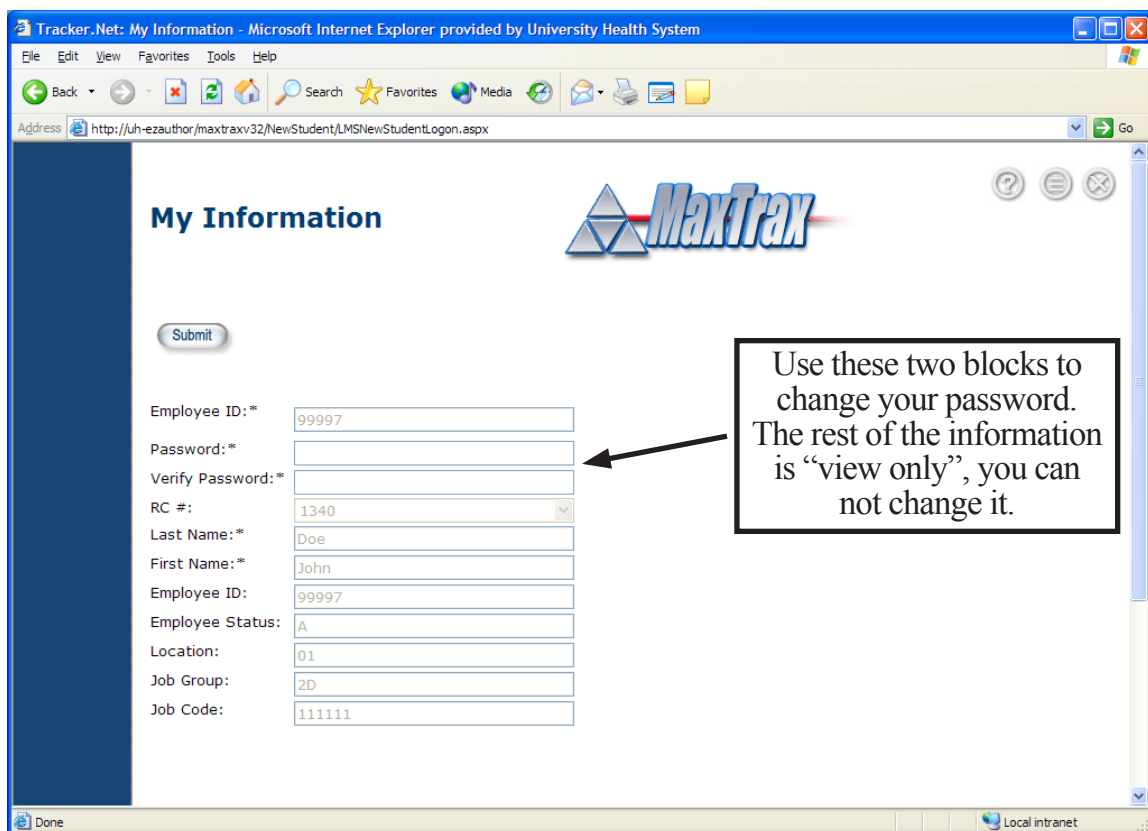
**University Health System**

2. The eLearning lessons are accessible from any computer connected (either internal or remotely) to the UHS intranet,. Your supervisor is responsible for making sure there is a computer available for you to use to complete the eLearning.

3. eLearning is completed at your own pace. You may take as much time, or as little time as necessary to understand and learn the information.

4. There is a quiz at the end of each lesson that is required for general orientation.

5. Most, but not all, eLearning lessons provide an opportunity for you to "test out." That means you can go directly to the quiz if you think you know the information covered in the lesson.

6. You do not need to take a lesson from start-to-finish all at once. You may exit (quit) a lesson and return to the lesson where you left off at a later time. (The computer remembers where you were.)

7. Successful completion of eLearning lessons is automatically recorded electronically. However, you may print a Certificate of Completion for your records if you wish.

8. Read and follow the instructions provided throughout the lesson! Special instructions (the words in blue) are provided on many screens. Be sure to follow these instructions.

9. Always exit (close) the lesson by using the Exit tab, DO NOT close the window by clicking the red square with an X in it. Your results will not be recorded properly if you do not exit properly.

10. Read the Tips for taking eLearning on the next page, then follow the directions starting on page 4.

**Follow the instructions provided in this packet and in the lessons.**

**University Health System**

## Helpful Hints for Taking eLearning

**Read and follow the instructions in blue text on the screen**

**For questions about logging on and passwords,
call the Help Desk: 358-4059**

**For questions about anything else concerning eLearning,
call the UHS eLearning Consultant: 358-8390**

1. eLearning can be taken from ANY computer in UHS.
2. Login using your Employee ID. Your Employee ID is 5 digits. It is not the same as your system User Name.
3. Password is welcome2 for first time users. You will be required to change your password the first time you log in. Passwords must be at least 6 characters, with a mix of letters and numbers.
4. After logging into MaxTrax – MAKE SURE your name is at the top of the screen. The person listed on the screen will receive credit for any training completed.
5. Group titles (Courses) specify if the lessons in the group are REQUIRED or OPTIONAL, and who the lessons apply to.
6. Be sure to READ and FOLLOW the directions on the screen when you successfully complete a lesson. You will not receive proper credit for the lesson if you do not follow the directions.
7. You have the option to "test out" of most lessons.
8. All lessons feature Bookmarking. You will re-enter a lesson at the same place you were when you exited the last time.

**University
Health System**

## Logging on to the UHS Network

**Follow these steps to log on to the UHS Network.**
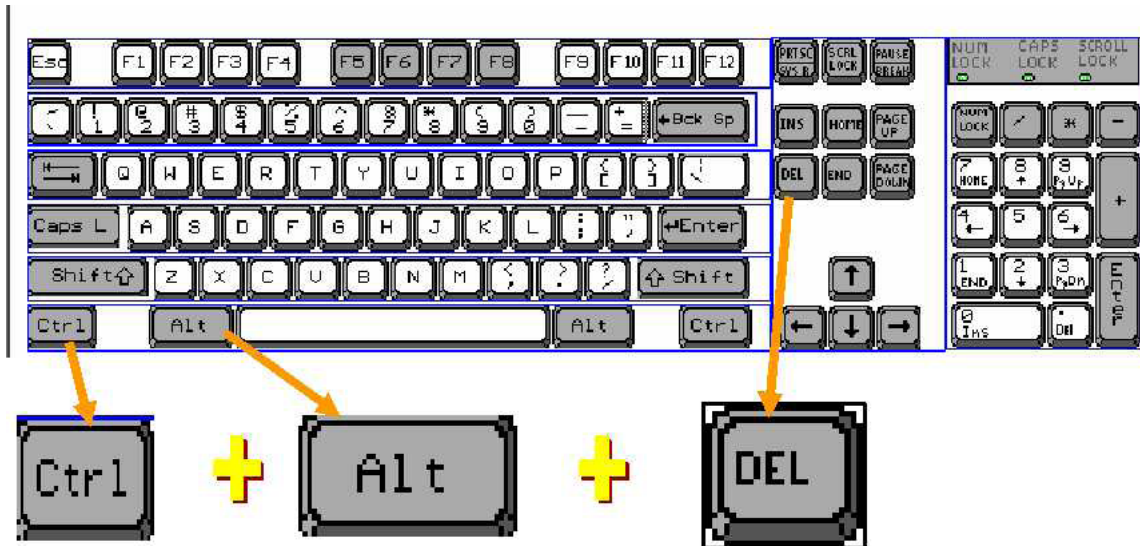


**The UHS intranet Home page will display after logging in.**

## Using MaxTrax

**Follow these steps to log on to MaxTrax (the UHS online training program).**



Click the triangle next to:
Online Training

# eLearning Instructions (cont.)
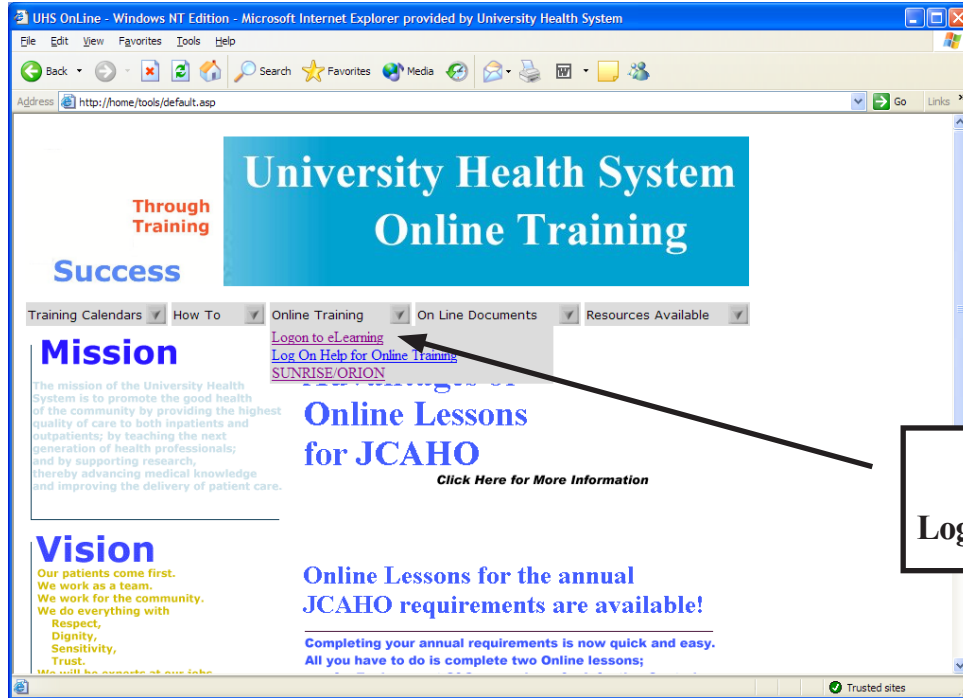
## Using MaxTrax



Click:
**Logon to eLearning**
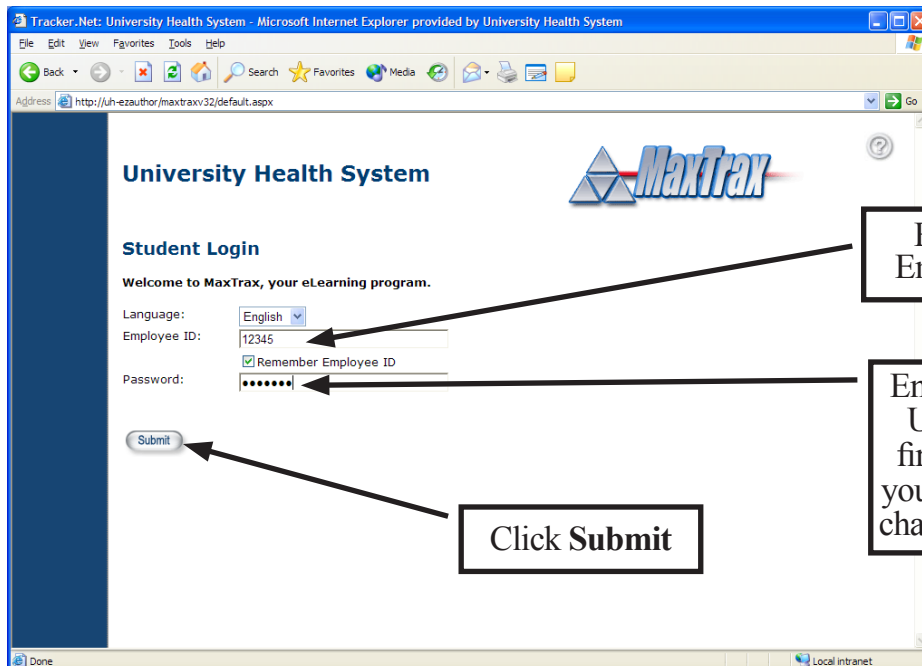


Enter your Employee ID

Enter your password. Use **welcome2** the first time you log in, you will be required to change your password.

Click **Submit**

University Health System

# eLearning Instructions (cont.)

## Using MaxTrax



Enter what you want to use as your password. (At least 6 characters, with a mix of letters and numbers.)

Enter your new password again for verification.

Click **Submit.** Note: you must click **Submit**, pressing the Enter Key will not work.



Verify that your name is shown here.

Click any of the 3 options available to:
- take lessons (My Courses)
- view a report of your training data OR to print a Certificate of Completion (My Reports)
- change your password (My Information)

University Health System

## Using MaxTrax

Click this link to display MaxTrax help.

Click this link to return to the Options screen.

Click this link to display MaxTrax help.
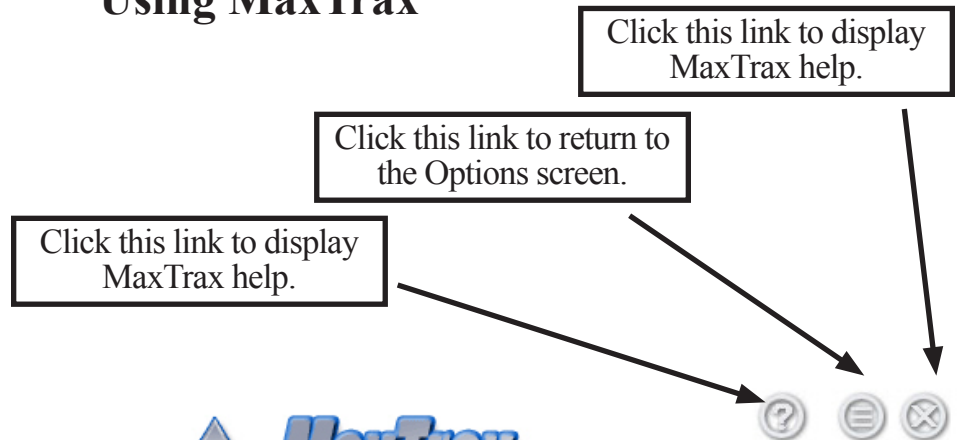
**My Courses**

**TEST My Courses**

**James Jones**          Desired 'My Courses' Interface: [TreeView ▾]

Group title.
Also called a **Course** title.

⊞ 🎲 **(UHS - NOT CFHP) 2008 Required Annual Training and System Level Competencies**

⊟ 🎲 **(UHS - NOT CFHP) Required for new employees for General Orientation.**

- ⦿ A Culture of Patient Safety
- ⦿ Awareness and Reporting of Patient Abuse
- ⦿ Age Specific Care
- ⦿ 2008 National Patient Safety Goals
- ⦿ Drug Free Workplace
- ⦿ Emergency Preparedness - 2008 (Fulfills the system level competency)
- ⦿ Environment Of Care - 2008 (Fulfills the system level competency)
- ⦿ HIPAA Privacy - 2008 (Fulfills the system level competency)
- ⦿ HIPAA Security - 2008 (Fulfills the system level competency)
- ⦿ Infection Control - 2008 (Fulfills the system level competency)
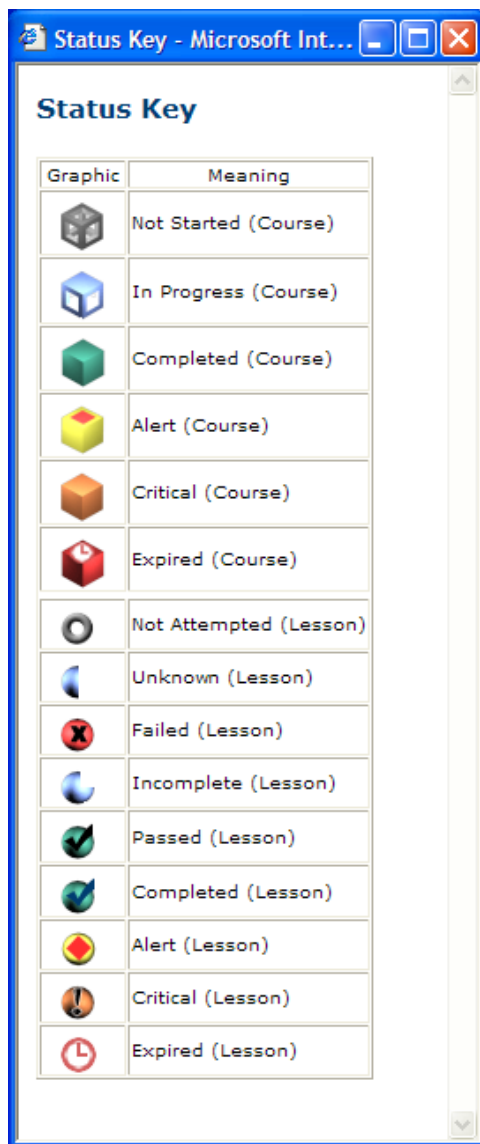- ⦿ Patient Management Topics

**Lessons** in the group.
Click a lesson title to take that lesson.

**University Health System**

## Using MaxTrax

A Status Key can be displayed by clicking the Status Key link at the bottom of the list of available Courses and Lessons.

**Status Key - Microsoft Int...**

### Status Key

| Graphic | Meaning |
|---|---|
| | Not Started (Course) |
| | In Progress (Course) |
| | Completed (Course) |
| | Alert (Course) |
| | Critical (Course) |
| | Expired (Course) |
| | Not Attempted (Lesson) |
| | Unknown (Lesson) |
| | Failed (Lesson) |
| | Incomplete (Lesson) |
| | Passed (Lesson) |
| | Completed (Lesson) |
| | Alert (Lesson) |
| | Critical (Lesson) |
| | Expired (Lesson) |

Status indicators for Courses are cubes.

Status indicators for Lessons are round.

NOTE: Not all available status indicators are used at UHS.

**University Health System.**

## Using MaxTrax

**My Reports**



*Screenshot callouts:*

A report of your eLearning training history is displayed.
A copy of the report can be exported and printed as explained below.

Click the certificate icon to print a Certificate of Completion. NOTE: You may need to set your printer to Landscape. Call the Help Desk at 358-4059 for assistance.



Certificate of Completion

Awarded to

*Don Bair*

For the Lesson

Emergency Preparedness

Completed On
11/1/2006
Most Recent Exam Score
90

## Using MaxTrax

### To print report

## Using MaxTrax

**My Information**



Use these two blocks to change your password. The rest of the information is "view only", you can not change it.

**TITLE:**          **INFORMATION ASSET SECURITY/USE**

**PURPOSE:**        To establish responsibilities and requirements for the protection and proper use of University Health System information assets as they relate to data, image, text and voice objects within internal and external systems by its employees, contractors, and other computer users.  To prevent misuse and loss of information assets; establish the basis for audits and self-assessments; and preserve management options and legal remedies in the event of asset loss or misuse.  This is a revised policy and supersedes policy dated 04/01/03.    [Key Words: Information Assets, Information System Access, Security, Protected Health Information]

---

**POLICY STATEMENT:**

It is the policy of the University Health System to protect the integrity and confidentiality of all information assets while providing access to these assets to appropriately authorized users.  The University Health System reserves the right to monitor any and all aspects of the computer system, including electronic mail, files, and internet access, to ensure compliance with this policy.  The computer equipment and access given to employees are to assist them in the performance of their jobs.  The computer and telecommunication systems belong to University Health System and may be used for business/management approved purposes only.  Any item developed and/or created while using this equipment is the property of University Health System.

**POLICY ELABORATION:**

    **I.**      **DEFINITIONS:**

        A.    "Information Assets" include but are not limited to: data, text, image, voice, computers, file servers, workstations, laptops,

software, printers, modems, printed reports, diskettes, CD ROMs, pagers, phones, and internal or external communications networks (Internet, commercial online services, and electronic mail systems) that are accessed directly or indirectly from University Health System's computer facilities.

B.    "Protect" includes preventing misuse, abuse, loss, or unauthorized access or disclosure of information assets.

C.    A "Department Head" is a UHS Department Director or above, who identifies, classifies, creates, maintains, and secures information assets within their areas of responsibility.

D.    A "User" refers to all employees, contractors, and other persons or third parties authorized to access or use University Health System computer or telecommunication or other information assets.

E.    A "Supplier of Information Technology Services" is a provider of information and/or information technology tools (hardware, software, reports, services, etc.) in support of business activities.

F.    "Negligence" the failure to use such care as a reasonably prudent and careful person would do under similar circumstances.

G.    "SPAM E-mail" is an unsolicited commercial message normally sent in bulk.

H.    "Information Services" is a division that consists of Business Applications, Clinical Applications, Technical Services, Operational Services, and HIPAA compliance management.

I.    "Protected Health Information" or PHI means generally, any

information, whether oral, written, electronic, or recorded in any form or medium (including demographic information that is collected from an individual) that identifies or may be used to identify the individual and relates to:

1.    the past, present or future physical or mental condition of an individual;
2.    the provision of health care to an individual; or
3.    the past, present or future payment for the provision of health care to an individual.

For the purposes of this policy, an individual such as a Department Head may simultaneously act as a User and/or Department Head, depending on the information used or provided by their department.

## II.    SCOPE:

This policy is applicable to all information assets and services which support business and clinical activities, and covers all staff, consultants, contractors, and other persons or third parties accessing or using University Health System's information assets.    There may be additional policy and/or departmental requirements for use of these resources, services, and authorization for access to and release of information.    Fulfillment of information asset security responsibilities is mandatory and may be considered a condition of continued employment or access to University Health System information assets.

## III.    RESPONSIBILITIES:

A.    DEPARTMENT HEAD:

A "Department Head" is responsible for:

(1)    Knowing the assets and services for which they're

responsible and the applicable control requirements;

(2) Authorizing Users to utilize information assets and ensuring that these assets are used for management-approved purposes only;

(3) Assigning custodial authority and responsibility for information asset controls;

(4) Ensuring effective use of control facilities;

(5) Ensuring staff education and awareness;

(6) Responding in a timely, effective way to loss or misuse of information assets and to identified information asset security exposures;

(7) Conducting assessments for compliance;

(8) Authorizing access level changes (including access origination, transfers and termination), assigning custody, and authorizing release of information;

(9) Notifying the Supplier of Information Technology Services of new hires, transfers, terminations and status changes of user accounts;

(10) Reviewing and updating, at least annually, the list of authorized individuals within the Managers area of responsibility with access to information assets.

B.    USER:

A "User" is responsible for:

1.  Complying with information asset security and application system controls as specified by the Supplier of Information Technology Services;

2.  Using information processing assets only when authorized by management and only for approved purposes;

3.  Ensuring that system, data, and application passwords meet specified requirements, are not shared, and are properly protected;

4.  Effectively using control facilities and capabilities;

5.  Bringing security exposures, misuse or non-compliance situations to management attention;

6.  Maintaining confidentiality of information accessed, accessing information that pertains only to their job function.

7.  The obligation to maintain the confidential information and security of confidential information continues upon termination of access.

C.  SUPPLIER OF INFORMATION TECHNOLOGY SERVICES:

A "Supplier of Information Technology Services" is responsible for:

1.  Administering owner-specified information asset security and application system controls for information and information processing assets in their custody;

2.     Providing for administration of access to information assets;

3.     Providing and administering physical and procedural safeguards for protection of information assets;

4.  Effectively communicating installation control facilities, rules and restriction to Users;

5.  Providing for timely detection and effective response to unauthorized attempts to gain access to data or restricted areas;

6.  Ensuring workstation use is authorized and from authorized locations;

7.  Bringing security exposures, misuse, or non-compliance situations to management attention.

8.  Establishing security controls and oversight of all UHS software applications to maintain centralized security administration.

## IV. GENERAL REQUIREMENTS

A.  Access to University Health System information assets is restricted to authorized individuals and used for business/management approved purposes only. All requests for access must be approved by the department supervisor, Information Services, and the user must sign a confidentiality agreement. Access will be assigned according to users job function.

B.  Users cannot attempt to access or gain access to data that they do not have direct responsibility for or authorization to access.

C.  User ID's follow Information Services standards to maintain consistency across all computing platforms. Generic user ids and

passwords are not permitted as an entry point for any application program. Passwords are set to automatically expire at system defined intervals. Each user is responsible for their user id and password. All user-chosen passwords must be difficult to guess. Users must never write down or otherwise record a readable password and store it near the access device to which it pertains. Passwords are to be kept confidential and not shared. Any action taken under that user id and password will be the sole-responsibility of the owner of that user ID and password.

D.    All users should attend a basic skills class conducted by Information Services or demonstrate required competency to qualified individuals before being granted access to University Health System computer systems. This will include security awareness training.

E.    Fraudulent, harassing, embarrassing, indecent, profane, threatening, obscene, intimidating, sexually explicit or other unlawful material may not be sent, accessed, displayed or stored on University Health System's Information Assets. Users encountering or receiving such material should immediately report the incident to their supervisor and/or the Integrity Office.

F.    Use of the Internet must be in compliance with all University Health System policies, and may not be used for personal financial gain in accordance with University Health System's conflict of interest policy 2.12.

G.    Internet addresses that are deemed inappropriate or non conducive to the work environment are blocked. Internet activity is monitored and recorded.

H.    Sensitive Programs, Restricted Utilities and other elements that may be used to bypass established controls must have procedures

to prevent unauthorized use, reproduction, or modification. Historical data and/or logs of usage of such elements/programs facilities must be available on demand.

I.      Internal applications under development, or undergoing major modification, whether the work is done within Information Services or elsewhere, should be reviewed and approved by the application owner and Information Services Management Team for information asset security compliance before becoming operational in a production environment.

J.      PHI/sensitive information on portable or fixed storage media, (floppy, CD, DVD, etc.), when no longer required, must be deleted or destroyed. All storage media must be destroyed prior to disposal. Cutting the media with scissors is a method of acceptable destruction or you may forward the media to Information Services Security Administration for destruction.

K.      All access to external systems must be approved by Information Services. Consideration must be given to the security of the electronic transmission of information. Additional security measures, such as encryption, may be appropriate.

L.      Computers or equipment that connect to University Health System computers or networks, which are not on University Health System premises and not under University Health System control, when used to access University Health System information, must be used for approved management purposes; must be certified for business necessity and interconnection controls and standards by appropriate levels of management to include Information Services, and must have Confidentiality Agreements and/or other appropriate contracts in effect. The Information Asset/Security Use Policy remains in effect when accessing the system from external sources.

Policy No.:            2.0802
Page Number:        10 of 17
Effective Date:       04/05/05

M.    Software purchased by University Health System is to be used for management approved purposes only.  All purchased software is company property and is subject to the license agreement as specified by the vendor and/or modified by University Health System contract.  Any duplication or alteration of licensed software, except for backup purposes, is strictly prohibited.  Individuals are not permitted to load or download any software onto their workstation or the network, this includes any software prompted requests for version updates or patches.  Such requests for software must be approved and installed by Information Services to ensure the software can be certified to work in University Health System's computing environment, and to protect from computer viruses, tampering and other exposures.

N.    In the event unauthorized and/or unapproved software is discovered on an individual computer or on the network, the computer may be formatted and reconfigured immediately without notice.

O.    Computers owned by and located within UHS facilities are programmed to automatically lock the workstation when the computer receives no input for a specified period of time.  The time out period will be limited to 15 minutes or less.

P.    To eliminate or minimize the possibility of unauthorized access to protected health and other confidential information, all University Health System workstations will be located in a manner that reduces the likelihood of information being viewed by unauthorized individuals.  In the event the workstation cannot be located in this manner, a privacy screen will be installed on the monitor

Q.    When a user leaves their workstation they must either lock the workstation or logoff of the system.  Users must logoff at the end

Policy No.:      2.0802
Page Number:    11 of 17
Effective Date:    04/05/05

of their shift.

R.    Computing installations and supporting facilities, as determined by management, must be administered as areas of restricted access when continued operation is considered essential or where sensitive information is stored.

S.    Information Services will establish/maintain a plan for responding to a system emergency that includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.

T.    Hardware acquired, installed, added, removed, connected/disconnected, or moved from University Health System infrastructure network or facilities will only be authorized and performed by Information Services.  Information Services will maintain an electronic inventory of all computing devices and network hardware.

U.    Protected Health Information may not be transmitted over any communication device unless authorized by Information Services.

V.    No hardware or software applications may be removed from University Health Systems' premises without written authorization, from Information Services.  Logs will be maintained of all equipment removals.

W.    Any loss of information assets due to negligence will require the user to reimburse the Health System for the replacement cost of the item.  No food, beverage, or liquid of any kind is to be placed on or near any information asset.

X.    A user cannot attempt to limit or restrict the Health System's right

to monitor any and all aspects of the computer system.

Y.    Users must not leave printers unattended while printing protected health and other confidential information.  An exception will be made if the area surrounding the printer is restricted such that persons who are not authorized to see the material being printed may not access it.

Z.    Software vendors who require access for diagnostic/support purposes will be required to gain access via a secured account that remains in the disabled state until needed.

AA.   Personal computing devices (laptops, PDA's, etc.) are not permitted to connect to UHS network unless authorized by Information Services.

BB.   The University Health System must ensure that information is available, updated, and properly maintained so that quality continuity of care is provided across inpatient and outpatient environments.  All individuals participating in the care of UHS patients are required to use information systems and other such information assets provided and maintained by UHS.  This includes physicians, nurses, and all others as defined in this policy.

## V.    E-MAIL REQUIREMENTS

A.    The E-mail system may not be used to create, forward, or attach any offensive, disruptive messages or chain letters.

B.    The E-mail system may not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary

financial information, or similar materials without authorization from the user's immediate supervisor.

C. All messages composed, sent or received on the E-mail system are and remain the property of University Health System. These messages are not the private property of any employee, contractor, or user of the system.

D. Notwithstanding the Health System's right to retrieve and read any E-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. It is the user's responsibility to ensure the accuracy of the E-mail address of the intended recipient. All inbound and outbound E-mails will contain a system generated disclaimer.

E. University Health System reserves and will exercise the right to review, audit, intercept, block, access and disclose all messages received or sent over the E-mail system for any purpose. The contents of any E-mail may be disclosed without the permission of the user.

F. University Health System will utilize software to automatically block any Spam E-mail.

G. E-mail that is sent internal to University Health System must be directed to the appropriate audience, and apply to all recipients. Discretion must be used in identifying those who receive carbon or blind copies. The E-mail system may be used for corporate wide (all users) communications, if approved by the area Vice President or their designee, Corporate Communications, and the Vice President of Information Services or their designee.

H. All E-mail sent via the internet containing PHI must be encrypted.

To encrypt an E-mail, type "PHI:" anywhere in the subject line.

I.   Due to the changing trends in virus contamination, allowable file type attachments will be permitted at the discretion of Information Services.

## VI. FACSIMILE REQUIREMENTS

A.   Transmission of protected health information via facsimile is restricted to information required for continuity of care where other means of delivery are not appropriate.

B.   All facsimiles must be accompanied by University Health System approved cover sheets (provided on the UHS HomePage). Individual or departmental cover sheets are not permitted under any circumstances.  Faxes containing PHI must use the Confidential Health Information cover sheet.

C.   If protected health information is to be sent by fax, the recipient must first have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception will be made if the area surrounding the fax machine is restricted such that persons who are not authorized to see the material being faxed may not enter.

D.   A "sender" of an outgoing fax is responsible for ensuring that the outgoing fax was sent to the correct destination by confirmation receipt. Written notification must be provided and filed with the Chief Privacy Officer for any misdirected faxes of protected health information.

E.   Protected Health Information whether inbound or outbound is not to remain in or around fax machines.

F.    Fax machines that send PHI should be pre-programmed to destination numbers whenever possible to eliminate errors in transmission from misdialing.  These numbers should be verified for accuracy on a monthly basis.

## VII.  TELEPHONE SYSTEM REQUIREMENTS

A.    PBX security software is installed on all University Health System phone switches.  This software is used to monitor, secure and track call activity.

B.    Area codes that are deemed inappropriate, or have the possibility of per minute charging will be blocked.

C.    Long distance calls require the use of an access code to complete the call.   All charges related to the call are billed to the appropriate Responsibility Center.

D.    The use of Cell Phones is permitted within University Health System; however discretion must be used to ensure patient care is not disrupted or compromised.  The use of camera phones for the purpose of taking pictures is prohibited on UHS property without proper authorization.  See Patient's Right to Consent, Policy No. 9.02.

E.    Users are prohibited from connecting modems of any type to the University Health System communications infrastructure. Requests for modems must be approved and installed by Information Services.

F.    Users are prohibited from connecting phones of any type to the University Health System communications infrastructure. Requests for phones must be approved and installed by

Information Services.

G.   Patient and confidential information may be left on voicemail only if you can verify voicemail is being used and not an answering machine, otherwise a call back number is to be left where you can be reached.  Patient and confidential information must not be left on answering machines.

H.   In order to prevent unnecessary costs to Health System, users should not use 1411 for information. A phone directory is available online that contains the Yellow, White, and Business pages for San Antonio and surrounding areas.  Phone books are also available.

I.   University Health System will not incur additional costs for personal phone usage to include phones, cell phones, and long distance use.  Each user is responsible for any of these additional charges.

## VIII.  POLICY VIOLATIONS:

Users encountering violations of this policy shall immediately report the incident to their supervisor and/or the Integrity Office.   Information Services should be notified immediately in incidents where assets are at risk.  It is the responsibility of the supervisor to notify the Integrity Office if the violation was not reported.  Each incident will be reviewed on an individual basis, and where appropriate, the supervisor may need to take disciplinary action, up to and including termination of employment/contract.   In addition, Information Services may revoke access to computer systems assets, if the violation is determined to put such resources at risk.  University Health System reserves the right to pursue legal action as needed.  Violations of state and federal law may subject persons to penalties of fines or imprisonment or both.

**REFERENCES/BIBLIOGRAPHY:**

UHS Conflict of Interest Policy, No. 2.12

UHS HIPAA Compliance Policy, No. 2.14

UHS Reporting Errors and Incidents of Misconduct Policy, No. 2.13

UHS Medical Records Policy, No. 10.03

Patient's Right to Consent Policy, No. 9.02

Information Security Policies Made Easy, Charles Wood, PentaSafe, 2003

Corporate Internet, Intranet and E-mail Policies, New York Law Journal, Internet, 2000

Society for Human Resource Management, Internet, 1998

UHS Information Services Standards Manual, 2004

Public law 104-191, 'Health Insurance Portability and Accountability Act of 1996'

IT Governance BS7799/ISO 17799

National Institute of Standards and Technology Special Publications 800 series

IT Governance Institute Control Objectives, 2000

**OFFICE OF PRIMARY RESPONSIBILITY:** Information Services

# Employee Assistance Program

The Employee Assistance Program (EAP) offered at University Health System is a free and confidential program that can help you and your family members balance the demands of daily living and find solutions for ongoing or serious concerns.

## The EAP can assist you and your family with:

▶ Dealing with aging parents
▶ Coping with loss and grief
▶ Adjusting to adoption
▶ Struggling with parenting concerns
▶ Financial and legal concerns
▶ Suffering from domestic violence
▶ Stress at home or in the workplace
▶ Resolving family/marital issues
▶ Coping with the impact of a tragedy
▶ Depression or Anxiety
▶ Managing healthy weight
▶ Quitting smoking
▶ Addressing a drug and or alcohol addiction

*Deer Oaks offers University Health System employees a team of trained counselors who specialize in a wide variety of personal and work-related issues.*

## What are the benefits of using the EAP?

▶ Professional counseling and resources
▶ It is easy to access and it's confidential
▶ It provides practical solutions and referrals
▶ Assistance is available 24 hours a day/ 7 days a week
▶ Offices and counselors throughout Texas
▶ Eight free counseling visits per family member

▶▶▶▶▶▶

Web site:  www.deeroaks.com
E-mail:  eap@deeroaks.com

▶▶▶▶▶▶

# Help is just a phone call away:
# (210) 614-2273

**University Health System**

# EMPLOYEE RIGHTS AND RESPONSIBILITIES
## UNDER THE FAMILY AND MEDICAL LEAVE ACT

**Basic Leave Entitlement**

FMLA requires covered employers to provide up to 12 weeks of unpaid, job-protected leave to eligible employees for the following reasons:

- For incapacity due to pregnancy, prenatal medical care or child birth;
- To care for the employee's child after birth, or placement for adoption or foster care;
- To care for the employee's spouse, son or daughter, or parent, who has a serious health condition; or
- For a serious health condition that makes the employee unable to perform the employee's job.

**Military Family Leave Entitlements**

Eligible employees with a spouse, son, daughter, or parent on active duty or call to active duty status in the National Guard or Reserves in support of a contingency operation may use their 12-week leave entitlement to address certain qualifying exigencies. Qualifying exigencies may include attending certain military events, arranging for alternative childcare, addressing certain financial and legal arrangements, attending certain counseling sessions, and attending post-deployment reintegration briefings.

FMLA also includes a special leave entitlement that permits eligible employees to take up to 26 weeks of leave to care for a covered servicemember during a single 12-month period. A covered servicemember is a current member of the Armed Forces, including a member of the National Guard or Reserves, who has a serious injury or illness incurred in the line of duty on active duty that may render the servicemember medically unfit to perform his or her duties for which the servicemember is undergoing medical treatment, recuperation, or therapy; or is in outpatient status; or is on the temporary disability retired list.

**Benefits and Protections**

During FMLA leave, the employer must maintain the employee's health coverage under any "group health plan" on the same terms as if the employee had continued to work. Upon return from FMLA leave, most employees must be restored to their original or equivalent positions with equivalent pay, benefits, and other employment terms.

Use of FMLA leave cannot result in the loss of any employment benefit that accrued prior to the start of an employee's leave.

**Eligibility Requirements**

Employees are eligible if they have worked for a covered employer for at least one year, for 1,250 hours over the previous 12 months, and if at least 50 employees are employed by the employer within 75 miles.

**Definition of Serious Health Condition**

A serious health condition is an illness, injury, impairment, or physical or mental condition that involves either an overnight stay in a medical care facility, or continuing treatment by a health care provider for a condition that either prevents the employee from performing the functions of the employee's job, or prevents the qualified family member from participating in school or other daily activities.

Subject to certain conditions, the continuing treatment requirement may be met by a period of incapacity of more than 3 consecutive calendar days combined with at least two visits to a health care provider or one visit and a regimen of continuing treatment, or incapacity due to pregnancy, or incapacity due to a chronic condition. Other conditions may meet the definition of continuing treatment.

**Use of Leave**

An employee does not need to use this leave entitlement in one block. Leave can be taken intermittently or on a reduced leave schedule when medically necessary. Employees must make reasonable efforts to schedule leave for planned medical treatment so as not to unduly disrupt the employer's operations. Leave due to qualifying exigencies may also be taken on an intermittent basis.

**Substitution of Paid Leave for Unpaid Leave**

Employees may choose or employers may require use of accrued paid leave while taking FMLA leave. In order to use paid leave for FMLA leave, employees must comply with the employer's normal paid leave policies.

**Employee Responsibilities**

Employees must provide 30 days advance notice of the need to take FMLA leave when the need is foreseeable. When 30 days notice is not possible, the employee must provide notice as soon as practicable and generally must comply with an employer's normal call-in procedures.

Employees must provide sufficient information for the employer to determine if the leave may qualify for FMLA protection and the anticipated timing and duration of the leave. Sufficient information may include that the employee is unable to perform job functions, the family member is unable to perform daily activities, the need for hospitalization or continuing treatment by a health care provider, or circumstances supporting the need for military family leave. Employees also must inform the employer if the requested leave is for a reason for which FMLA leave was previously taken or certified. Employees also may be required to provide a certification and periodic recertification supporting the need for leave.

**Employer Responsibilities**

Covered employers must inform employees requesting leave whether they are eligible under FMLA. If they are, the notice must specify any additional information required as well as the employees' rights and responsibilities. If they are not eligible, the employer must provide a reason for the ineligibility.

Covered employers must inform employees if leave will be designated as FMLA-protected and the amount of leave counted against the employee's leave entitlement. If the employer determines that the leave is not FMLA-protected, the employer must notify the employee.

**Unlawful Acts by Employers**

FMLA makes it unlawful for any employer to:

- Interfere with, restrain, or deny the exercise of any right provided under FMLA;
- Discharge or discriminate against any person for opposing any practice made unlawful by FMLA or for involvement in any proceeding under or relating to FMLA.

**Enforcement**

An employee may file a complaint with the U.S. Department of Labor or may bring a private lawsuit against an employer.

FMLA does not affect any Federal or State law prohibiting discrimination, or supersede any State or local law or collective bargaining agreement which provides greater family or medical leave rights.

**FMLA section 109 (29 U.S.C. § 2619) requires FMLA covered employers to post the text of this notice. Regulations 29 C.F.R. § 825.300(a) may require additional disclosures.**