DIGNITY HEALTH
ADMINISTRATIVE POLICY AND PROCEDURE

FROM: Compliance Oversight Committee

SUBJECT: Network Usage Policy (NUP) – Dignity Health Personnel

EFFECTIVE DATE: January 17, 2012

REVISED: December 15, 2011; April 13, 2009; December 19, 2008; November 1, 2006; May 1, 2005; (9.901) October 1, 2002; March 14 2001

ORIGINAL EFFECTIVE DATE: (9.901) March 14, 2001

REPLACES: (110.1.037) Network Usage Policy (NUP): April 13, 2009; December 19, 2008; November 1, 2006; May 1, 2005
(9.901) Network Usage Policy: October 1, 2002; March 14, 2001

APPLIES TO:		
	System Offices:	X
	Acute Care Entities:	X
	Non-acute Care Entities:	X

I. POLICY:

It is the policy of Dignity Health to provide Personnel appropriate access to the Dignity Health Network and its information systems and portals, which in any event shall require approval by the individual's supervisor. Upon written request and approval in accordance with Dignity Health policies and procedures, Dignity Health will provide access to its Network as necessary for the User to carry out the obligations of his or her job. Use of the Network by any person other than a duly designated User, shall be a violation of this Policy.

Dignity Health wishes to respect a User's desire for privacy and free speech; however, it is Dignity Health's policy and each User's responsibility, to ensure the integrity, security and appropriate use of Dignity Health's e-mail systems, technology and network resources, information systems, and data. As such, Dignity Health may monitor the use and/or activities of a User on the Dignity Health network. A User is advised that his or her activities on the Dignity Health Network are neither private nor confidential.

The Dignity Health Network is a private network of Dignity Health. Its information systems are a critical component for the provision of timely quality care to patients and business operations. Protected Health Information (**PHI**) and other Confidential and

Sensitive Information reside on the Network and are protected by law and strict Dignity Health privacy and data security policies. The intent of these laws and policies is to protect the confidentiality, integrity, and availability of this information. Users are expected to be familiar with this Network Usage Policy (the "**Usage Policy**" or "**NUP**"); Dignity Health's privacy, data security, and compliance policies as relevant; and any updates or revisions thereof which are available online). Users are also expected to use their common sense and exercise good judgment at all times.

A. **Introduction:** Dignity Health's network includes its internally and externally hosted information systems, mobile applications, internet, extranets, intranet, e-mail, instant messaging, telecommunication services provided by or on behalf of Dignity Health (collectively, the "**Dignity Health Network**" or "**Network**")**.** The Network also includes all Dignity Health-issued electronic devices, regardless of whether such usage is in audio, video, or other media format. This Usage Policy describes the acceptable uses of the Network and the obligations and responsibilities of each user of the Network.

The scope of this Policy includes, but is not limited to, the examples of technologies, applications, and network services listed below:

1. Pagers;
2. Cell phones;
3. PDAs, tablets, and smartphones (handheld devices);
4. Computers;
5. Printers;
6. Portable media such as USB drives, floppy disks and CD ROMs;
7. Computer applications;
8. Medical devices attached to or interfaced to the Network; and
9. Fax, phones, or any other electronic communications device or information system device in a Dignity Health Facility.

B. **Non-Compliance**: Violations of this Network Usage Policy or other privacy, data security and compliance policies, will be investigated and documented in accordance with the **Investigation, Response and Notification of Privacy and Data Security Incidents** policy #110.1.028. Violations can lead to immediate revocation of Network privileges and/or disciplinary action up to and including termination of employment, any and all contractual relationships with Dignity Health, or other privileges as applicable. In addition to other legal remedies Dignity Health may have available to it for damages incurred as a result of any violation of its policies, Dignity Health reserves the right to seek injunctive relief in a court of law to immediately bar a User from the use or benefit of Dignity Health's facilities or resources. Dignity Health may also be required by law to report certain activities to enforcement agencies, or may elect to do so in a proactive manner.

C. **Variances**: Any exceptions or variances to the provisions of this policy, or any other data security policy, must be reviewed and approved by the Chief Data Security Administrator (CDSA) in accordance with the provisions of the **Data Security Policy** #110.1.036.

D. **Monitoring of User Content and Activity:** Dignity Health Network access is a privilege and is granted to Users to facilitate the performance of Dignity Health-related business and may be changed or revoked at any time at the sole discretion of Dignity Health. THE CONTENTS AND HISTORY OF A USER'S NETWORK SESSION AND ACTIVITY ARE, THEREFORE, THE SOLE AND EXCLUSIVE PROPERTY OF DIGNITY HEALTH. WHILE DIGNITY HEALTH DOES NOT ASSUME ANY OBLIGATION TO REGULARLY MONITOR AND LOG A USER'S NETWORK ACTIVITY, DIGNITY HEALTH MAY ACCESS, MONITOR, LOG, REVIEW AND DISCLOSE AS IT DEEMS NECESSARY, IN ITS SOLE DISCRETION, ALL CONTENT CREATED OR RECEIVED BY A USER, INCLUDING BUT NOT LIMITED TO, A USER'S WEB BROWSING, INSTANT MESSAGE, E-MAIL, APPLICATION ACTIVITY, FOR ANY PURPOSE AND TO ANY PARTY, AND ANY DATA STORED OR CACHED ON A USER'S COMPUTER HARD DRIVE OR NETWORK FOLDER. DIGNITY HEALTH MAY ALSO DISCLOSE THE CONTENT OF A USER'S NETWORK ACTIVITY TO LAW ENFORCEMENT OFFICIALS AND APPROPRIATE DIGNITY HEALTH MANAGEMENT WITHOUT PRIOR NOTICE TO OR CONSENT OF A USER. AS A RESULT, A USER SHOULD NOT EXPECT ANY CONTENT A USER CREATES OR RECEIVES, OR STORES ON A DIGNITY HEALTH ISSUED OR APPROVED ELECTRONIC DEVICE TO BE PRIVATE OR PERSONAL. TO ENABLE ACCESS TO THE NETWORK, A USER SHALL SIGN AN ACKNOWLEDGEMENT (BY INK OR ELECTRONIC MEANS) FORM. A USER SHALL HAVE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY OR SIMILAR RIGHTS TO OR IN ANYTHING A USER CREATES OR RECEIVES ON OR VIA THE NETWORK.

E. **Users Obligations and Responsibilities**: A User is required to:

1. Use the Network for the benefit of Dignity Health;
2. Maintain and use appropriate safeguards to protect the privacy and confidentiality of all data in accordance with the HIPAA Policies Published in the Administrative Policy Manual;
3. Not share his or her User-ID and password. Each User is responsible for protecting the User-ID and password (including access badges, certificates and other forms for authentication) from use by anyone else and is responsible for any activities having occurred through the use of his or her User-ID and password;

4. Use appropriate protections (personal firewall, anti-virus and anti-spyware software) and obtain approval from the Dignity Health Facility's IT Site Director before connecting (hardwired, wireless or other electronic means) a personal computers, portable media, smartphone, tablet or other electronic device to the Network; except, however, Dignity Health IT Site Director approval is not required when accessing the Network through an approved access method over the Internet;
5. Comply with requirements for anti-virus protection, personal firewall settings, screen savers, session and screen timeouts, encryption and other workstation settings necessary to safeguard the Network;
6. Promptly notify the Dignity Health Helpdesk when unable to log in to the Network;
7. Disable or hinder any Dignity Health issued software automation application;
8. Log out of all electronic devices and/or applications when leaving them unattended, or, alternatively, lock the device or utilize a screensaver with the password function activated;
9. Report security violations or attempts immediately to the Dignity Health Helpdesk, IT Site Director, Dignity Health IT security operations, the Facility Privacy Official, or the Chief Data Security Administrator; and
10. Comply with all third-party software license requirements and Dignity Health policies relating to software procurement and installation.

F. Acceptable use of the Network: In the performance of their job, a User may :

1. Access websites as they relate to the User's job duties;
2. Use only Dignity Health approved e-mail, instant messaging, social media websites, externally-hosted applications, external storage services (e.g., flash drives, approved network attached storage (NAS), etc.), blogs, texting applications and other Dignity Health-approved means to communicate with Dignity Health employees and non-employees, including members of the public, and, as applicable, in accordance with **E-mail** Policy #110.1.046;
3. Access externally-hosted web applications (ASP), software-as-a-service (SaaS) that have been reviewed and approved in conformance with the requirements of the **Website Lifecycle** Policy #110.1.043 when outward facing, that is, viewable by patients, physicians or members of the public;
4. Use Dignity Health-IT provided or approved online applications and materials, subject to any requirements and limitations necessary for such;
5. Use Internet resources for limited personal use during breaks, outside of normal work hours, and while on business-related travel provided that:
    i. Dignity Health may, at any time and at its sole discretion, deny Internet access for non-business use;

ii. the use does not involve activities that are unlawful or otherwise not in conformance with this Policy or other Dignity Health policies;
iii. the use does not involve non-Dignity Health commercial use;
iv. the use does not involve audio or video streaming or other large consumption of Network resources; and
v. the use does not interfere with normal business operations of any Dignity Health workstation, device, department, application or other resource.

G. Prohibited Uses of the Network: A User is prohibited from engaging in activities that are unlawful, may result in damage to the Network, may cause interruption of service, interferes with normal business operations, or are contrary to the mission and values of Dignity Health or its policies and procedures. A User is further prohibited from attempting to bypass login or security controls or place Dignity Health's confidential data at risk. The following is a non-exhaustive list of examples of prohibited uses of the Network, both during and after business hours:

1. Using or accessing the Network account, including e-mail, files or application accounts, of another User except as provided in Use of Network Logs and User Files policy 110.1.045 and Account Deactivation & Quarantine policy # 110.1.044;
2. Sending e-mail from a generic, shared or anonymous e-mail accounts, unless specifically approved by the Chief Data Security Administrator or Dignity Health legal counsel;
3. Using the Network to send or forward spam or chain letters or using any means to make Dignity Health Network be the recipient of spam or chain letters;
4. Knowingly creating, receiving, posting or forwarding material, or creating hyperlinks thereto, for illegal, libelous, unethical or pornographic purposes, or to negatively depict race, national origin, gender, sexual orientation, religion, creed, age, disability, or to otherwise violate Dignity Health's policy against harassment, or contribute to an intimidating or hostile work environment;
5. Broadcasting unsolicited personal views on social, political, or religious areas not within the User's job duties, or other non-business related matters;
6. Accessing or disclosing Confidential Information, Sensitive Information, or Strictly Confidential Information that is not within the scope of the User's Dignity Health-related duties and responsibilities (see **Confidentiality and Data Classification** policy # 110.1.039) ;
7. Acting in a deliberate manner that is likely to damage or disrupt the Network, alter its normal performance, or cause it to malfunction or be accessed by a party without authorization, regardless of location or duration;

8. Introducing a computer virus, Trojan horse, spyware, or other malicious programs into the Network, or into external systems and networks;
9. Encrypting, decrypting or attempted decrypting of any Network component, Network content, User ID, passwords, or any other User's encrypted files or User accounts without proper authorization;
10. Using modems, remote access clients, or other communication services or protocols (e.g. GoToMyPC) that have not been provided or approved by Dignity Health IT;
11. Using programs that scan ports, sniff packets, or otherwise attempt to probe Network activity unless the activity is specifically authorized in writing by the Dignity Health IT VP, Technology and Infrastructure;
12. Transmitting Confidential or Sensitive Information off site without appropriate authorization and the use of minimum safeguards documented in the **Confidentiality and Data Classification** Policy #110.1.039 and other applicable policies;
13. Accepting or agreeing to be bound by any terms and conditions of use (other than standard terms and conditions of use for access to Web sites that do not require the disclosure of Sensitive Information or Dignity Health's intellectual property), license agreements, or other types of online agreements without review by Dignity Health legal counsel;
14. Without the prior written authorization of the Dignity Health IT Site Director:
    a. copying Dignity Health software for use on a User's home computer;
    b. providing copies of Dignity Health software to any independent contractor or consultant of Dignity Health or to any third person without the approval of Dignity Health legal counsel or IT Contracting Director or their respective designees;
    c. downloading, updating or installing unapproved software (including screen savers and games) on a workstation, Dignity Health-approved device , or the Network, unless the software is:
        (i) a browser applet (within a browser);
        (ii) necessary for a web-based webinar or teleconference, such as GoToMeeting or WebEx;
        (iii) an update or upgrade to a generic desktop application, such as Adobe; or
        (iv) an update or upgrade to a business application unique to the User's department.
    d. modifying, copying, revising, transforming, recasting, or adapting any software unless it is within the scope of the both the software license and the User's job excluding User level configuration;

e. reverse engineering, disassembling, or de-compiling any software on or from the Network;
f. altering copyrighted works which changes, obscures, or removes information relating to the copyright owner, copyright notice information, the author of the work, the terms and conditions of use of the work, or identifying numbers or symbols referring to the foregoing information or links to such information;
g. backing up or copying Network content from a computer, smartphone, tablet or other mobile media, personally-owned or otherwise, to or on Internet storage, Cloud storage or other remote storage, or maintaining Network content on such Internet, Cloud or remote storage.

H. Public or Non-Dignity Health Forums including Social Media, Blogs, Messaging, Chat and Discussion Groups, List-serves, and Newsgroups.

It is inappropriate to discuss or reveal Sensitive Information or Confidential Information in public or in other non-Dignity Health forums. A User shall identify himself or herself honestly, accurately, and completely when participating in both Dignity Health and non-Dignity Health forums, and when setting up Dignity Health-related accounts on outside computer systems. A User should understand that each of his or her postings will leave an "audit trail" indicating at least the identity of Dignity Health's Internet servers, and most likely, a direct trail to the User. Inappropriate postings may damage Dignity Health's reputation and could result in business or individual liabilities. Accordingly, a User must make every effort to be professional in making comments online. Each User should make clear that any comment, opinion or point of view that he or she expresses on such non-Dignity Health online forums is his or hers as individuals and not necessarily representative of Dignity Health's point of view or opinions.

I. Disclaimer of Liability for Internet Use:

WHILE Dignity Health MAY USE CERTAIN TECHNOLOGIES TO BLOCK INAPPROPRIATE EMAIL OR WEBSITES, NEVERTHELESS, Dignity Health IS NOT RESPONSIBLE FOR MATERIAL VIEWED OR DOWNLOADED BY USERS FROM THE INTERNET. EACH USER ACCESSING THE INTERNET DOES SO AT HIS/HER OWN RISK. DIGNITY HEALTH IS NOT RESPONSIBLE FOR THE MATERIAL VIEWED OR DOWNLOADED BY A USER FROM THE INTERNET. DIGNITY HEALTH'S USE OF TECHNOLOGY TO BLOCK INAPPROPRIATE EMAIL OR WEBSITES DOES NOT GUARANTEE THAT ANY OR ALL OFFENSIVE MATERIAL WILL BE BLOCKED AND INACCESSIBLE TO THE USER. EACH USER IS ADVISED TO EXERCISE APPROPRIATE CAUTION IN ACCESSING THE INTERNET IN ORDER TO AVOID OFFENSIVE CONTENT.

J. Miscellaneous:

This Policy is not intended to, and does not grant, the User any contractual rights.

If a User is unsure of any of the above requirements, or is otherwise unable to comply with any of the requirement of this Usage Policy, a User shall contact the Dignity Health IT Site Director or the **CDSA** for assistance with any questions.

If a User wishes to confidentially report a problem or issue relating to this Usage Policy. or a violation thereof, he or she may do so by calling the **Dignity Health Compliance Hotline at 1-800-938-0031.**

II. PURPOSE:

The purpose of this policy is to implement certain aspects of Dignity Health Privacy Principles (110.1.001) in order to comply with the Health Insurance Portability and Accountability Act ("**HIPAA**") and other federal and state laws governing protection of confidential health information and sensitive information. The Dignity Health Board has delegated certain of its authority to the Dignity Health Chief Privacy Administrator and Dignity Health Chief Data Security Administrator to ensure that necessary policy and procedures are written and implemented to comply with the Privacy Principles.

III. DEFINITIONS:

Capitalized terms not defined herein shall be as defined in the **Dignity Health Privacy and Security Definitions** Policy#110.1.024.

- "**Acknowledgement Form**" – See **Exhibit A** attached.
- "**Authorized Access**" or "**Authorized Use**" – See Section IV.A.1.
- "**Business Associate**" – See Dignity Health Privacy Definitions Policy # 110.1.024.
- "**CDSA**" – Dignity Health's Chief Data Security Administrator.
- "**Dignity Health**" – Dignity Health and its affiliates and managed entities.
- "**Facility Privacy Official**" (FPO) is the individual appointed by the facility administrator to be responsible for facility level implementation of the Dignity Health Privacy Principles.
- "**Network**" – See Section I.A herein.
- "**Personnel**" – Permanent employees, temporary employees, interns, registry personnel, student trainees and others who are under Dignity Health's supervision including volunteers.

- "**Protected Health Information**" (PHI) -- See Dignity Health Privacy Definitions Policy # 110.1.024.
- "**User(s)**" – All Personnel that have been given access to Dignity Health Network including information systems and portals.

IV. PRINCIPALLY AFFECTED DEPARTMENTS:

This policy applies to all facilities and departments with Users and each shall receive or provide required education as applicable.

V. PROCEDURES FOR ALL FACILITIES:

It is the responsibility of each Dignity Health Facility and Dignity Health IT Department to implement practical methods for carrying out this policy. At a minimum each Dignity Health Facility shall adhere to the following:

A. General Requirements:

1. Copies of the signed acknowledgements, whether signed electronically or in ink, must be retained for a minimum of six (6) years in a filing system or repository that provides read access;
2. Re-acknowledgement of the provisions of this Usage Policy is required whenever it is revised.

B. Users are authorized to access and/or use th*e* Network *("**Authorized Access** or **Authorized Use**")* only as long as the User complies with each of the following:

1. prior to being granted Network access, has signed or acknowledged (in writing or by on-line acknowledgement) Exhibit A, **Acknowledgement Form to Comply With Dignity Health's Network Usage Policy** (the "**Acknowledgement Form**");
2. if signed in ink, the originally signed Acknowledgement Form must be stored in the Dignity Health Facility's Human Resources Department or Volunteer Services Department, as applicable; and
3. if signed or acknowledged electronically, Dignity Health IT Department shall be responsible for its maintenance and integrity.

C. To maintain and continue their Authorized Access, Users are also required to do each of the following:

1. Complete required new-hire security and privacy awareness education within thirty (30) days of hire.

2. Re-sign the Acknowledgement Form at least every thirty-six (36) months or sooner if the policy is revised or as requested by Dignity Health; and
3. Complete required periodic security and privacy awareness education.

VI. STATUTORY/REGULATORY AUTHORITIES:

Notes as footnotes in policy if applicable

VII. EXHIBITS:

Exhibit A - Acknowledgement Form to Comply with Dignity Health's Network Usage Policy

Exhibit A
Acknowledgement Form to Comply with Dignity Health's Network Usage Policy

I hereby certify that I have received, read, understood, and will fully comply with Dignity Health's Network Usage Policy (NUP).

I acknowledge that I am responsible for my possession and use of any informational resources of Dignity Health. I will actively protect these informational resources from unauthorized disclosure, modification, deletion, and usage.

I acknowledge and hereby agree that my compliance with the policies and procedures described in Dignity Health's NUP is a requirement for my continued access to the Network (defined in Section I.A of the NUP). I understand that access to the Network is a privilege, which may be changed or revoked at any time at the sole discretion of Dignity Health.

I agree to promptly report all violations or suspected violations of the NUP to the Dignity Health IT management or in confidence to Dignity Health's Compliance Hotline at **1-800-938-0031**.

I acknowledge that Dignity Health may need to change or update the NUP periodically and will post any revised policy on the Network. I will comply with all revisions to the NUP.

I understand that if I am unsure of any of the elements of the NUP or if I subsequently learn that I am otherwise unable to comply with certain of its requirements, I should contact the IT Helpdesk for assistance with any questions I may have.

Signature of User: _____ **Date** _____
(Must be signed by all facility Personnel including volunteers as required in the Usage Policy)

Print Name of User: _____

Facility Name: _____

Department: _____

Print Supervisor's Name: _____ **Date** _____
(Required)

Supervisor's Signature _____
*(Required only if User is **not** a permanent employee nor a volunteer of Dignity Health facility*)