Origination:	*04/2016*
Last Approved:	*02/2017*
Last Revised:	*02/2017*
Next Review:	*02/2018*
Owner:	*Jeff Mcqueen*
Policy Area:	*Information Technology*
References:	

Acceptable Use

POLICY

This Acceptable Usage Policy covers the security and use of all of DWMHA's information and Systems. "Systems" include but are not limited to desk-top computers, laptops, corporate cell, voice, and mobile devices. Wi-Fi Hot Spots and any other device provided by DWMHA in the performance on corporate operations operations. It also includes the use of email, internet, voice and mobile IT equipment. This policy applies to all Users.

This policy applies to all information, in whatever form, relating to DWMHA's activities and to all information handled by DWMHA relating to other organizations with whom it deals. It also covers all IT and information communications facilities operated by DWMHA or on its behalf.

PURPOSE

The purpose of this policy is to outline the acceptable use of IT systems at DWMHA. These rules are in place to protect the employee and DWMHA. Inappropriate use exposes DWMHA, the User, and Consumers to risks including virus attacks, compromise of systems and services, potential leak of consumer's personal and health care related information, and legal issues.

APPLICATION

1. Who is required to implement and adhere to this policy: DWMHA Board, All DWMHA Staff, Contracted Staff and vendors.
2. Who does this policy serve: N/A
3. What service line does this policy impact: All Service Lines

KEY WORDS

Systems

All IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, phones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

STANDARDS

1. System Use
    a. All data stored on DWMHA's systems is the property of DWMHA.
    b. DWMHA's systems exist to support and enable the business and operations of DWMHA. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleague's productivity and nor should it result in any direct costs being borne by DWMHA other than for trivial amounts (e.g., an occasional short telephone call).
    c. DWMHA trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain they should consult their manager.
    d. Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorized access is prevented (or at least made extremely difficult). However, this must be done in a way that does not prevent–or risk preventing–legitimate access by all properly-authorized parties.
    e. DWMHA can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.
    f. DWMHA reserves the right to regularly audit networks and systems to ensure compliance with this policy.
2. Data Security
    a. Users must take all necessary steps to prevent unauthorized access to confidential information including Protected Health Information (PHI).
    b. Users are expected to exercise reasonable personal judgment when deciding which information is confidential.
    c. Users must not send, upload, remove on portable media or otherwise transfer to a non-DWMHA system any information that is designated as confidential, or that they should reasonably regard as being confidential to DWMHA, except where explicitly authorized to do so in the performance of their regular duties.
    d. Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with DWMHA's safe password policy.
    e. Users who are supplied with computer equipment by DWMHA are responsible for the safety and care of that equipment and the security of software and data stored on those devices as well as other DWMHA systems that they can access remotely using it.
    f. DWMHA staff are not to sub-loan equipment to any other individuals without adhering to the checkout procedure of the DWMHA Information Systems Helpdesk.
    g. Because information on portable devices, such as laptops, tablets, and phones are especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.
    h. All workstations should be secured with a "lock-on-idle" setting, activated within 30 minutes of

inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

i. Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

j. Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into DWMHA's systems by whatever means and must report any actual or suspected malware infection immediately.

3. Unacceptable Use

All employees should use their own judgment regarding what is unacceptable use of DWMHA's systems. The activities below are provided as examples of unacceptable use, however, it is not exhaustive. Should an employee need to compromise these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

a. All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.

b. All activities detrimental to the success of DWMHA. These include sharing sensitive information outside the company, such as consumer information and customer lists, as well as defamation of the company.

c. All activities for personal benefit, that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).

d. All activities that are inappropriate for DWMHA to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.

e. Circumventing the IT security systems and protocols which DWMHA has put in place.

QUALITY ASSURANCE/IMPROVEMENT

The Authority shall review and monitor contractor adherence to this policy as one element in its network management program.

COMPLIANCE WITH ALL APPLICABLE LAWS

In using DWMHA IT Systems, Authority staff, contractors and subcontractors are bound by all applicable local, state and federal laws, rules, regulations and policies, all federal waiver requirements, state and county contractual requirements, policies, and administrative directives, as amended.

LEGAL AUTHORITY

N/A

RELATED POLICIES

1. HIPAA Privacy Manual and Policies
2. HIPAA Security Manual and Policies

3. Safe Password Policy

RELATED DEPARTMENTS

1. Administration
2. Claims Management
3. Clinical Practice Improvement
4. Compliance, Customer Service
5. Information Technology
6. Integrated Health Care
7. Legal, Managed Care Operations
8. Management & Budget
9. Personnel, Purchasing
10. Quality Improvement
11. Utilization Management
12. Recipient Rights
13. Substance Use Disorders

CLINICAL POLICY

NO

INTERNAL/EXTERNAL POLICY

INTERNAL

EXHIBIT(S)

Attachments:

No Attachments

Approval Signatures

Approver	Date
Ronald Hocking: Chief Operating Officer	02/2017
Dana Lasenby: Deputy Chief Operating Officer	02/2017
Allison Smith: Project Manager, PMP	02/2017
Crystal Palmer: Director, Children's Initiatives	02/2017
Stacie Durant: CFO Management & Budget [AS]	02/2017
Julia Kyle: Director of Integrated Care	02/2017
Darlene Owens: Director, Substance Use Disorders, Initiatives	02/2017
Michele Vasconcellos: Director, Customer Service	02/2017

Approver	Date
Muddasar Tawakkul: Director of Compliance/Purchasing	02/2017
tracey Lee: Director Claims Management	02/2017
Jody Connally: Director, Human Resources	02/2017
Rolf Lowe: Assistant General Counsel/HIPAA Privacy Officer	02/2017
Lorraine Taylor-Muhammad: Director, Managed Care Operations	02/2017
Kip Kliber: Director, Recipient Rights	02/2017
Corine Mann: Chief Strategic Officer/Quality Improvement	02/2017
Jeff McQueen	02/2017
Sarah Sharp: Consultant	02/2017
Diana Hallifield: Consultant	02/2017
Jeff McQueen	02/2017
Bessie Tetteh: CIO	02/2017