Subject:	Confidentiality in the VMC	**Policy Section:**	10-VMC-F
Applicable to:	All VMC clinicians, staff, and students	**Pages**:	1
Author:	Hospital Director	**Submitted Date:**	05/19/2014
Review:	Hospital Management Team	**Review Date:**	05/19/2014
Approval:	Hospital Management Team	**Approval Date:**	11/07/2014
Related policies and procedures:		**Replaces version Dated:**	05/30/2014

POLICY:
The Veterinary Medical Center (VMC) has ethical and legal responsibilities to protect and safeguard client, patient, and business information. Employees may see or hear information that must be kept confidential including clinical patient information, personal and financial client information, and University information.

1. Employees may not access any information other than what is necessary for them to do their assigned job.
2. Employees may disclose confidential VMC, patient, and/or client information, only if such disclosure is necessary for patient care/treatment, payment, or VMC operations, and the employee is authorized to make such disclosures. Such disclosures must be made according to established policies and procedures of the VMC and the University of Minnesota.
3. Employees may not make, use, and/or publish information, photographs, or any other reproduction of a patient or client's physical likeness for any communication efforts (such as pamphlets, booklets, video tapes, slide shows, social media, or internet sites).
4. Employees may not make, use and/or publish information, photos, or any other reproduction of the University of Minnesota Veterinary Medical Center building (internal or external) for any communication efforts (such as pamphlets, booklets, video tapes, slide shows, social media, or internet sites).
5. Employees must guard against incidental or inadvertent disclosures of confidential information by adopting work practices that minimize the risk of such disclosures including:
    a. Exercising discretion when conducting conversations in public or semi-public areas;
    b. Not leaving confidential information unattended in public or semi-public areas, including documents, computer screens, printers, and fax machines;
    c. Restricting access to confidential information to only those persons who need the information to perform assigned job duties;
    d. Shredding documents containing confidential information before discarding them;
    e. Adhering to VMC technical security policies and procedures.
6. Employees may not make inquiries for information on behalf of any individual or party who is not properly authorized to access the information.
7. Employees may not disclose, transmit, copy, modify, or purge confidential information unless they are properly authorized to do so.
8. Any entries that employees make in VMC information systems must be made under their person login and password. Employees are solely responsible for any activities performed under their login and password.

9. Employees may not share their personal login and password with anyone. Employees must inform their supervisor immediately if they know or suspect that someone has learned or used their login or password.
10. Employees must inform their supervisor immediately if they observe unauthorized or untrained persons accessing or harming VMC information systems.
11. Employees must use all VMC property, data and products, including computer software, in accordance with applicable licensing/leasing agreements and contracts.
12. Upon termination with the VMC, employees must immediately return all VMC property including identification badges, keys and documents, and refrain from accessing VMC information systems.
13. Employees understand that failure to comply with this confidentiality policy may result in disciplinary action up to, and including, suspension, restriction or loss of privileges, termination of work with the VMC, and possible personal civil and criminal fines and penalties.

OVERSIGHT/FOLLOW THROUGH:

All employees are responsible to report any infractions to this policy to their supervisor. Directors and supervisors are responsible for compliance of this policy.