General Privacy Policy

The first line of defense in privacy and data security is the individual user. All MidAtlantic Ophthalmology team members granted access to MidAtlantic Ophthalmology systems are responsible for the confidentiality and security of all data and communications which may come to them in various formats.

Communications and records include but are not limited to; patient and team member protected health information and personally identifiable information, financial and operational records and all internal communications. The privacy and security of data and communications is essential to MidAtlantic Ophthalmology functions and is required by law.

It is the responsibility of every MidAtlantic Ophthalmology team member and individuals given access to the MidAtlantic Ophthalmology network systems protect not only the privacy of communications and records within MidAtlantic Ophthalmology, but also the flow of information in data form that not handled appropriately could result in a breach and have serious personal and legal consequences for all the parties involved.

Access to confidential information is limited to authorized persons with a "need to know." Workforce members have an affirmative duty to report any compromise or even suspected compromise of any such information immediately to their supervisor. It is the policy of MidAtlantic Ophthalmology to train all members of its workforce who have access to PHI on its privacy policies and procedures.

MidAtlantic Ophthalmology has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA.

.

RULES OF PRIVACY:

Listed below are the basic rules for privacy. Violating any one of them is a breach in confidentiality subject to disciplinary action up to and including termination.

- Don't tamper with, alter or change any patient medical record or organization documents.
- Do not view, copy, print or disseminate any record unrelated to the purpose for which you were given access and within the scope of your role.
- Do not store electronic information outside of the secure network, except as permitted by policy. Always maintain information in a secure manner.
- Do not retain or remove electronic or paper copies of records unless specifically authorized to do so.
- Do not disclose information unless you are specifically authorized to do so.
- Do not intrude upon any patient and/or private communication to which you are not privileged.
- Do not listen to or repeat anyone else's communications inappropriately.
- Do not use information from any communication or patient record or even the fact that a communication has occurred or a record exists for your personal benefit or for the benefit of others.
- Do not disclose information about patients or vendor billing arrangements or the location of equipment or supplies to any unauthorized person.

EXAMPLES OF INAPPROPRIATE CONDUCT WHICH COULD LEAD TO A BREACH IN CONFIDENTIALITY:

1. Engaging in confidential discussions in inappropriate areas such as the elevators, hallways, lunch room and/or within listening distance of unauthorized persons.
2. Releasing and/or discussing confidential information by telephone to unauthorized and/or unidentified persons.
3. Visiting a patient and/or a staff member unit without authorization.
4. Discussing confidential information outside MidAtlantic Ophthalmology in a social setting with unauthorized persons.
5. Accessing information by computer that you do not need to know to fulfill your job responsibilities.
6. Allowing an unauthorized person to access systems using your sign on and password.
7. Accessing or obtaining a medical record not pertinent to your job responsibilities. .
8. Removing any medical record containing protected health information off site without being expressly authorized to do so.
9. Storing protected health information on any electronic device that is not approved by MidAtlantic Ophthalmology. All such devices are required to have the information stored in an encrypted form with strong password protections.

COMPLIANCE AND DISCIPLINARY ACTION

All workforce members (e.g. staff, physicians, nurses) and non-workforce members (e.g. vendors or business associates) must comply with all applicable HIPAA patient privacy and information security policies. If after an investigation you are found to have violated the organization's HIPAA privacy and information security policies then you are subject to disciplinary action.