Minnesota Urology P.A.	
Policy Title	Electronic Signature Policy
Department	Administration
Departments/Individuals Affected	All Divisions; All Departments; All Employees and Physicians
Date Effective / Written By	June 1, 2018/Dave Carpenter, CEO
Version Number	v.06.01.18

Rationale/Purpose: Electronic signature is used for health records as a means of attestation of electronic health record entries, transcribed documents, and computer-generated documents. Properly executed electronic signatures are considered legally binding as a means to identify the author of health record entries, confirm content accuracy and completeness as intended by the author, and to ensure e-signature integrity is maintained for the life of the electronic health record.

It is the policy of Minnesota Urology to accept electronic signatures as defined within this policy for author validation of documentation, content accuracy and completeness with all the associated ethical, business, and legal implications. This process operates within a secured infrastructure, ensuring integrity of process and minimizing risk of unauthorized activity in the design, use, and access of the electronic health record**.**

Scope: This policy applies to all Minnesota Urology physicians, licensed practitioners and other authorized personnel who are required to enter information into the electronic medical record system (EMR).

Policy:

1) Only those physicians, licensed practitioners, and other authorized personnel ("individual/s") who provide care to a patient may enter information into the EMR of the patient.
2) Each individual authorized to access the EMR has been assigned a password and/or unique identifier and only the individual to which the password/unique identifier is assigned may use the password/unique identifier. Individuals will take precautions to safeguard their passwords/unique identifiers and will not permit anyone else to use the password/unique identifier. Individuals will notify Administration immediately in the event of any disclosure or sharing of a password for electronic signature.
3) Individuals are responsible for the accuracy, completeness and authenticity of all data entered into the EMR.
4) Individuals agree not to access the EMR from any public internet location, e.g. internet cafes or hotel workstations.
5) Individuals will access the EMR only from computers, laptops, or other devices which are owned or issued by the practice, the individual, or a health care/hospital system in which the individual is credentialed to provide care, and all such equipment shall be continually update with virus protection software. In addition, when accessing the EMR remotely from a health care/hospital system computer, individuals shall follow the established technology usage policies of the health care/hospital system.
6) The EMR system includes protections against modification of an entry into the EMR and software protections in compliance with the HIPAA privacy and security rule.