ABOUT YOUR PRESENTER:

Louis M. Schlesinger obtained his Bachelor of Science Degree in Zoology from LSU in 1977, his Doctorate Degree in Optometry from The Southern College of Optometry in Memphis, TN in 1982, and his Masters Degree in Management Information Systems from Georgia College and State University in 1996. Working with microcomputers since 1983, he wrote one of the first sphero-cylindrical over-refraction programs used for astigmatic soft contact lens design, *Taming Soft Torics*®, and along with Ophthalmic Surgeon Johnny L. Gayton, MD, the first nomogram software used for calculating the corneal incisions required for the Radial Keratotomy refractive surgery procedure, *Reliable Keratotomy*®. Louis has over 400 hours of classroom and laboratory training in the field of Digital Forensics. He has testified as an expert witness in State Superior Courts and Federal District Courts in a wide variety of civil and criminal cases accumulating the second-highest number of witness stand hours logged by any Digital Forensics Expert in the State of Georgia. He is a member of The International Information Systems Forensics Association, The International Society of Forensic Computer Examiners, The American College of Forensic Examiners (Diplomate), the Digital Forensics Certification Board, The Georgia Association of Professional Private Investigators, and the Investigative and Security Professional Association of Georgia.

POINTS TO REMEMBER

- EMR's are capable of storing information paper records can't record
  - ✓ Embedded information about the dates and times a document was created
  - ✓ Information about the camera or diagnostic equipment used to create a photograph or perform a diagnostic test
  - ✓ Information related to dates and times that emails were written and/or sent
- EMR's store a higher volume of information on each patient than paper
  - ✓ Dates and times entires are made are automatically recorded
  - ✓ The identify of the user logged in at the time the entry is made is automatically recorded
  - ✓ The number of entries, photos, documents, test results, etc. is only limited by the amount of storage capacity the EMR system contains, and that capacity can be inexpensively increased at any time.
- EMR's store information that the user may be totally unaware exists
  - ✓ Hidden information such as that mentioned in the previous two bullets can be used against a provider who attempts to lie during the course of malpractice litigation proceedings
  - ✓ This same hidden information can exonerate a provider falsely accused of wrongdoing
- Every staff member must have their own unique EMR login username and password
  - ✓ Having departmental login ID's makes it impossible to determine which person is responsible for entries made into the EMR system.
  - ✓ An inability to correctly identify the person responsible for making a given entry in the EMR system severely limits your ability to defend yourself against claims of wrongdoing.

- No staff member should be allowed to make entries into the EMR system unless they are logged-in as themselves using their own UN and PW
    - ✓ Evidence that staff members use the EMR system when logged in as someone other than themselves can destroy the integrity and credibility of much of the information contained in the EMR system itself.
    - ✓ If your EMR can no longer be used to defend your claim of innocence, most of your defense is lost altogether.
- Writers and Assistants should make entries logged in as themselves even while in the examination room
    - ✓ Otherwise it will appear the provider made all of the entries himself/herself
    - ✓ The provider cannot claim entry errors made by ancillary personnel when the EMR indicates the provider made all of the entries himself/herself.
- The EMR should be reviewed for accuracy and completeness prior to being electronically signed or closed out
    - ✓ The more time that passes between the dates of the actual office visit (Doctor-Patient encounter) and the dates entry corrections or additions are made, the more suspicious the entries look from a Judge or juror's perspective.
- All supporting documents should be uploaded and attached to the EMR in their original, digital format
    - ✓ Printed documents that are simply scanned into the EMR system contain none of the important, hidden metadata that can support claims of innocence in a litigious situation.
    - ✓ The EMR system's record of when documents were scanned into the system may even make the provider look like he/she is being less than truthful.

- If uploading of digital files is not possible, make notes in the EMR indicating where the original digital file can be found
    - ✓ Being able to locate the original digital files containing the important metadata may be of paramount importance when attempting to prove your innocence in a malpractice suit.
- When entries are made to the EMR subsequent to the actual office visit, state a reason for the delay in entry
    - ✓ Since date and time differences between the actual Doctor-Patient encounter and the date/time an EMR entry is made regarding that Doctor-Patient encounter can be misconstrued as indicating a lack of honesty, having an explanation for any delays in entry corrections or additions is important.
    - ✓ Explanations accompanying EMR entries make it difficult for opposing attorneys to make an issue of the date/time discrepancies between the patient visit and the entry.
- Set programs to enable their metadata recording
    - ✓ Consult your legal counsel with regards to this suggestion
    - ✓ If you enable the metadata, be sure you have established policies, and be sure to stick to those policies
- Always carbon copy yourself on any emails related to patient care
    - ✓ Carbon copies inform the recipient that you will be getting a copy of the email yourself which makes it less likely they will claim they never received your email
    - ✓ Carbon copies provide you with the hidden metadata needed to prove the email was sent and, in many instances, prove the recipient did indeed receive the email regardless of their claims to the contrary.

- Make a note of any photo that has been altered, state what alteration was done, state why the alteration was necessary, and save a copy of the original, unaltered photo.
    - ✓ Photos that are altered look suspicious at best, and proof-positive of wrongdoing at worst, to the Judge and jury.
    - ✓ The original, unaltered photo can demonstrate to the Judge and jury the reason it required adjustment and exactly what changes were made.
- Never store a digitized copy of your signature on a computer system
    - ✓ Digitized signatures stored on a computer or computer network are an invitation to staff members to forge your name on documents, including prescriptions for medications and/or optical devices.
- The outcome of a lawsuit depends less on what the truth actually is than on what the Judge and Jury believe the truth to be
    - ✓ Enough said!