Patient Privacy & Security Checklist

Gramercy Surgery Center would like to re-emphasize the importance of patient privacy and the crucial role every employee plays in ensuring the safety of sensitive health information. It is a team effort to protect the privacy of our patients but it is up to each individual at GSC to contribute to this team effort!

Protected Health Information (PHI) is any information relating to the identity of a patient (including name, age, demographics etc), the physical or mental medical conditions of that patient, the diagnosis, prognosis and care of the patient, or the patient's payment for medical services. Ensure that you only access Protected Health Information (PHI) on a need-to-know basis (i.e. when you are required to do so for your work). Additionally, ensure that PHI accessed or shared is the minimum information necessary to get the job done.

The following are some everyday best practices to abide by:

- □ **Emails:** Use only your secure GSC email account if you must email anything containing patient information. Yahoo, Gmail and personal email accounts are not secure.
- □ Do not use a patient's name in the subject line of an email.
- □ Clinical and Administrative staff should use the patient's identification number rather than the patient's name in any emails between staff and physicians regarding that patient. Be wary of discussing a patient or their case only with those staff that require the knowledge to perform their job.
- □ Billing and Scheduling staff should be sure to verify the identity of the person they are speaking with before transmitting sensitive information. For example, if you are faxing something to a number you have not dealt with before, send an initial fax requesting confirmation that the number does belong to the person/company, before transmitting sensitive information.
- □ **Login/Logout:** Always lock your computer when you step away from the desk for any reason and no matter how short the time. Log out properly at the end of each work day. Remember, non-GSC personnel occasionally have access to the building.
- □ **Phone Calls:** If you are taking a call within earshot of employees who do not need access to the information you are discussing, or members of the public, remain careful of using a quiet tone to avoid incidental disclosure
- □ **Cell Phones:** Avoid using personal cell phones to text regarding scheduling, cases etc. If you do need to contact each other or physicians after work hours consider having IT install your GSC emails on your cell phone, and communicate through this medium. It is as instant as text messaging and a safer channel. Alternatively speak to each other on the phone rather than texting so that nothing is preserved in text should your phone be lost/stolen. Make your best effort to ensure you communicate patient information only through our official GSC channels.
- □ **Shredding:** Do not under any circumstances use a box under your desk to gather documents for shredding. If something containing sensitive

information needs to be shredded take it to the shredding bin immediately. Do not use any other form of disposal for such documents.

- □ **Clean Desk Policy:** If you are leaving your desk for lunch/at the end of the day put away all documents that are not in use.
- □ **Front Desk Intake:** Be cognizant of the presence of other persons in the waiting room when speaking with a patient at the front desk. Keep your voice low to avoid incidental disclosures. If a patient is speaking particularly loudly, you may want to politely remind him/her that people may overhear what he is saying (don't worry too much about this, it's up to the patient whether or not they are concerned by this).
- □ **Vision:** Do not under any circumstances share your Vision password with anybody. Vision records access by user name and is monitored. Anyone found to have shared their password with someone who did not need to access Vision will be held responsible for any improper use of the information. Never leave Vision logged in and unattended.
- □ **Tablet:** The cover should remain on the tablet at the nursing station at all times when it is not in use. When it is in use be aware of anyone standing around you who may be able to see what you are viewing.
- □ **Patient Charts:** Do not leave these unattended at the nursing station or front desk. We will be installing cabinets with locks but until we do, put them in a drawer if the desk will be unmanned for any reason. When charts are out ensure they are turned face downwards so that patient information is not visible.
- □ **Discussing Cases/Charts at the Nurses Station or Front Desk:** Again be aware of who is around you and keep your voice low so that only the parties to the conversation can hear what is being discussed.
- □ **Pre-Op Interviews:** Our pre-op areas are open so be constantly aware of creating a greater environment of privacy. Always pull the curtain, always keep your voice low and always remember to read your patient for any signs of discomfort or uncertainty when you ask them sensitive questions. Make them feel safe and secure.

- □ Notify Ruth, the Privacy Officer, if you believe there has been any improper disclosure of patient information to a person /organization outside of GSC that is not privileged to receive such information.
    - This is not designed to punish GSC employees but to ensure that we try our best to mitigate any damage and to properly document these disclosures for the patient!

- □ Notify Ruth (the Privacy Officer) or Davie (the Security Officer) if you see any way that GSC can improve its patient privacy and security from any aspect.