"Cyber Events" defined:

- Apparent unauthorized access to EMR, company network, system, application, data, or other resource.
- Suspicious impairment to the normal authorized functionality of networks, systems, or applications.
- Inadvertent clicking on suspicious link in email, text message, etc.
- Improper or inappropriate usage or transmission of PHI or PII - violation of HIPAA privacy and security standards involving computers, including email breach (e.g., emailed PHI to wrong patient).
- Website compromise.
- Inadvertent divulging of sensitive information to phone scammers.
- Inadvertent transfer of funds to wrong account.
- Any other suspicious activity involving the computer.

Pre-Cyber Event

1) Ensure that an appropriate level of cyber insurance coverage is in place.

2) Conduct an annual HIPAA Security Risk Assessment.

3) Conduct annual HIPAA training for all staff members.

4) Conduct HIPAA penetration testing (i.e., simulate a cyberattack on a computer system to evaluate its security in an effort to identify any vulnerabilities that attackers could exploit).

5) Identify first, second, and third level contacts within the practice for purposes of any Cyber Event (the "Breach Contacts") and ensure that all staff members have the Breach Contacts names and cell numbers stored in their personal cell phones.

1st Contact: _____ **Cell:** _____

2nd Contact: _____ **Cell:** _____

3rd Contact: _____ **Cell:** _____

6) The Breach Contacts, on a quarterly basis, should ensure that they have (i) updated personal cell phone numbers for all staff for notification purposes if/when there is a Cyber Event, (ii) the IT Vendor's contact phone numbers, and (iii) the Sterling Seacrest Pritchard ("SSP") phone numbers listed below (collectively, the "Contact Phone Numbers"). The Breach Contacts should keep a copy of the Contact Phone Numbers stored in their cell phones.

7) Make a list of at least three alternative medical practices (e.g., a pediatric practice within close proximity, urgent care centers, etc.) to whom you could direct sick patient visits if you have to close the office temporarily due to a Cyber Event (the "Backup Practices").

8) Instruct staff to report all Cyber Events to the Breach Contacts. If in doubt, make a report.

Post-Cyber Event

1) If/when a Cyber Event occurs, the discovering party should immediately contact the Breach Contact by cell phone in the order available. For example, if the 1st Breach Contract does not answer, contact the 2nd Breach Contact….

2) The first Breach Contact who answers should make note of all pertinent information regarding the Cyber Event and then immediately call SSP in the following order (regardless of the day or time):
    a. Brent Reece (Cell: 706-300-2033)
    b. Bartley Miller (Cell: 404-386-5574)
    c. John Miller (Cell: 404-307-4430)

3) SSP will notify (i) the appropriate cyber insurance carrier(s) and (ii) Kids Health First via Barbara Douglas. The insurance carrier, in turn, will trigger an emergency breach response team (if necessary) who will contact the Breach Contact with next steps.

4) Depending on the magnitude of the Cyber Event, the Breach Contact will:
    a. Contact the practice's IT vendor.
    b. Notify your website vendor, EMR vendor, etc. depending on the type of Cyber Event.
    c. Notify all staff by text message via their personal cell phones.
    d. Ask staff to (i) log-out of the system if logged-in, or (ii) not log-in.
    e. Instruct staff not to discuss the Cyber Event with anyone outside of the medical practice (e.g., no social media posts, no Facebook announcements, etc.).
    f. Notify the authorities (FBI Internet Crime Complaint Center; Georgia Cybersecurity Incident Reporting System).

5) Consider whether patient appointments must be cancelled (e.g., cannot access the EMR). If they must be cancelled, identify which staff members will be responsible for contacting patients' parents, starting with the first appointment scheduled for that day. Refer them to the Backup Practices.

6) Apologetically excuse any patients already in the waiting room and let them know you will contact them in the next several days with an update. Refer them to the Backup Practices if they need to be seen that day.

7) Consider posting an announcement on the practice's website (e.g., banner), but do not reference a cyber breach. Instead, post something like: "OUR COMPUTER SYSTEM IS CURRENTLY OFFLINE AND WE ARE UNABLE TO SEE PATIENTS AT THIS TIME. PLEASE CONTACT US AT _____ WITH ANY QUESTIONS AND TO RESCHEDULE YOUR UPCOMING APPOINTMENT, IF NECESSARY."

8) Change the office voice-mail system (and/or alert your answering service) to state "THE OFFICE IS CURRENTLY CLOSED BECAUSE OUR COMPUTER SYSTEM IS OFFLINE. PLEASE CALL 911 FOR ANY EMERGENCIES. PLEASE LEAVE A MESSAGE FOR ANY NON-EMERGENCIES."

9) Change the sign on the door to "Closed".

10) For any calls from authorities and/or the media, direct those to the Breach Contact, e.g., "YOU WILL NEED TO DIRECT ANY QUESTIONS REGARDING THIS MATTER TO _____ AT _____." If the Breach Contact receives a call from the media, the response should be something like: "WE ARE STILL ASSESSING THE SITUATION AND ARE UNABLE TO COMMENT FURTHER AT THIS TIME."

11) Follow breach counsel's advice.
