BROWNWINICK LAW

666 Grand Avenue | Suite 2000 | Ruan Center | Des Moines, Iowa 50309
515-242-2400 | 888-282-3515 | brownwinick.com

HIPAA COMPLIANCE REQUIREMENTS

Implement and Maintain Reasonable and Appropriate Standard Policies and Procedures

- Draft and retain policies and procedures.
- Document actions, activities, and assessments required by HIPAA.
- Maintain records for a minimum of six (6) years from the date of creation or the date the policy or procedure was last in effect.
- Must make documentation available in printed manuals and/or on Intranet websites.
- Documents need to be reviewed frequently and updated as necessary to reflect current policies and procedures.

Workforce Training and Management

- All workforce members (including volunteers and trainees) must be trained on the entity's privacy policies and procedures.
- Document all training and attendees.

Security Risk Analyses

- Designate a privacy official and document the personnel designation.
- Conduct an accurate and thorough assessment of the potential risks and vulnerabilities of the availability of ePHI annually.
- Review technical safeguards, physical safeguards, and administrative safeguards.

Notice of Privacy Practices

- Provided to patients no later than the first patient visit.
- Posted Notice at the physical location.

Incident Documentation for any Privacy and Security Incidents that Occur

- Implement procedures to regularly review records of activity, such as audit logs, access reports, and security incident tracking reports.
- Mitigate, to the extent practicable, harmful effects of security incidents that are known and document the incident and outcome.

Breach Notification Documentation for any Breach that Occurs

- To an individual:
    - Must be within sixty (60) calendar days after discovery of a breach and written in plain language.
    - A brief description of breach including date of breach and discovery of breach,
    - Description of types of unsecured PHI involved in breach,
    - Any steps individuals should take to protect themselves,
    - A description of what you are doing to investigate the breach, to mitigate harm, and prevent future breaches, and
    - Contact procedures of individuals to ask questions.
- If over 500 residents of a state

    - Within sixty (60) days following the breach, notify prominent media outlets serving the state or jurisdiction.
    - Same information required for notification to individuals.
- Notification to Secretary:
    - Following breach of unsecured PHI you must notify the secretary in accordance with HHS website.

Employee Sanction Documentation

- Maintain documentation of sanctions applied to employees in violation of any policies and procedures.
- Required to mitigate any harmful effect that is known of a use of PHI in violation of any policy or procedure.

Complaint and Resolution Documentation

- Must document all complaints and their disposition (if any).
- A contact person or officer responsible for receiving complaints or further information about matters covered by notice.
- Create a process for individuals to make complaints concerning the covered entity's compliance with its privacy policies and procedures and include in the Privacy Notice.

Business Associate Agreements with Service Providers and Contractors

- You may permit a business associate to create, receive, maintain, or transmit ePHI on your behalf only if you have satisfactory assurances that they will appropriately safeguard the information.
- Document the satisfactory assurances required through a written contract or other arrangement with the business associate through the use of a Business Associate Agreement ("BAA").

Physical Security Maintenance Records

- This record should contain, at a minimum, the name of the person responsible for the item, the location of the item, and any movement of the item.
- Address the final disposition of ePHI and/or hardware on which it is stored.
- Implement/document procedures for removal of ePHI form electronic media before the media are made available for re-use.

Information Systems Activity Reviews, Decisions Made, and Investigations Conducted

- Log records pertaining to views and updates of ePHI.
- Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
- Assign a unique name/or number for identifying and tracking user identity.
- Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
- Implement a mechanism to encrypt and decrypt ePHI.

Contingency Plans/Tests in Effect During the Retention Period

- Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.
- Establish procedures to restore any loss of data.
- Establish procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
- Establish how to obtain necessary ePHI during an emergency.

NO SURPRISES ACT COMPLIANCE

Notify Patients of Availability of a Good Faith Estimate

- In a written document that is clear, understandable, and prominently displayed (in the office, on the provider's website);
- Verbally when the services are scheduled (possibly providing a script for front desk or scheduling staff members; or
- When the patient asks about the cost of the services.

See the attached Good Faith Estimate Notification

Provide Good Faith Estimate in Writing

- A Good Faith Estimate must include the following:
    - Patient's name and date of birth;
    - Clear description of the service and the date the appointment is scheduled for (if applicable);
    - List of all items and services (including those to be provided by co-providers);
    - CPT code, diagnosis code, and charge per item of service;
    - Name, NPI, and TIN of all service providers and the state where the services will be rendered;
    - List of items from other providers that will require separate scheduling;
    - Disclaimer that separate GFEs will be issued upon request for services listed in number 6, and that items in number 4 will be provided in those separate GFEs;
    - Disclaimer that there may be other services required that must be scheduled separately during the course of treatment and are not included in the GFE;
    - Disclaimer that this is only an estimate and actual services, and charges may differ;
    - Disclaimer informing the patient of their rights to a patient-provider dispute resolution process if actual billed charges are substantially above the estimate, as well as where to find information on how to start the dispute process;
    - Disclaimer that GFE is not a contract, and the patient is not required to obtain services from the provider.

A form with all required information can be found at https://www.cms.gov/files/document/good-faith-estimate-example.pdf.

Also see the No Surprises Act Toolkit from Iowa Chiropractic Society