Cook Hearing & BALANCE

PATIENT INFORMATION

Today's Date: _____

Last Name _____ First Name _____M.I._____

Preferred Name (Nickname) _____ Gender: Male ☐ Female ☐

Date of Birth: ___/___/____ Home Phone # ___-___-____ Cell Phone # ___-___-____

Social Security # _____ Social Security # of guardian (if minor) _____

Address _____ City _____ State _____ Zip Code _____

Email address _____

Employer _____ Occupation _____

Spouse's name _____ Spouse's phone # ___-___-____

Emergency Contact: _____ Relationship _____

Phone # _____

Primary Care Physician _____ Phone # ___-___-____

How did you hear about our office? _____

INSURANCE INFORMATION

Primary Insurance Company _____

Insurance ID # _____ Insurance Group # _____

Name of Policy Holder _____ Policy Holder's DOB _____

Secondary Insurance Company _____

Insurance ID # _____ Insurance Group #_____

I understand and agree that (regardless of my insurance status), I am ultimately responsible for the balance on my account due for any professional services rendered. I have read all the information on this sheet and certify that this information is correct to the best of my knowledge. I will notify Cook Hearing & Balance of any changes in my health status or in the above information.

Signature: _____ Date: _____

Parent Signature (if minor): _____ Date: _____

Cook Hearing & BALANCE

Patient Name: Last: _____First: _____M.I.____

Medical History:

Yes	No	(Please check yes/no)
☐	☐	Have you seen a doctor specializing in diseases of the ear?
☐	☐	Have you ever had your hearing tested? If yes, please give date_____ by whom_____
☐	☐	Have you ever had any type of ear surgery? If yes, what type of surgery _____
☐	☐	Do you take medicine every day? _____ If yes, for what condition(s)? _____ _____
☐	☐	Do you have any other medical conditions that have affected your hearing? If yes, please explain _____
☐	☐	Have you ever had a serious illness in the past that may have affected your hearing? (i.e., scarlet fever, meningitis, mumps, etc.) _____
☐	☐	Have you been exposed to high levels of sound? (i.e., farm equipment, power tools, lawn mowers, chain saws, firearms)_____ If yes, was hearing protection used? Yes ☐ No ☐ Sometimes ☐

About Your Ears:

(Please check all that apply)

- ☐ Deformity of the ear
- ☐ Drainage from the ear
- ☐ Sudden or rapid loss of hearing in the past 90 days
- ☐ Acute or chronic dizziness
- ☐ Have you seen a doctor for wax removal?
- ☐ Do you ever have pain in your ears?
- ☐ Do you ever experience ringing or noises in your ears?

If yes: Left ☐ Right ☐ or Both ☐ If yes, is the sound: Constant ☐ or Intermittent ☐

About Your Hearing: Do you experience difficulty with the following?

Yes	No	
☐	☐	Understanding conversations
☐	☐	Hearing in a crowd
☐	☐	Hearing by telephone

How long have you had difficulty in communicating? _____

☐	☐	Is one ear stronger than other? If yes: Left ☐ or Right ☐
☐	☐	Has anyone else in your family been diagnosed with hearing loss? If yes, who? _____
☐	☐	Do you now or have you ever worn a hearing aid? If in the past, when? _____

Signature: _____ **Date:** _____

Cook Hearing & BALANCE

Patient Authorization of Disclosure

In general, the HIPAA Privacy Rule gives individuals the right to request a restriction on uses and disclosures of their protected health information (PHI). The individual is also provided the right to request confidential communications of PHI be made by alternative means, such as sending correspondence to the individual's office instead of the individual's home. The patient may revoke or change this authorization at any time with a written request.

I wish to be contacted in the following manner (check all that apply):

Home Telephone:

☐ OK to leave a message with detailed information

☐ Leave message with call-back number only

Written Communication:

☐ OK to mail to my home address

☐ OK to send to my email address

Other: _____

Signature: _____ Date: _____

In an effort to protect your health information and the confidentiality of your healthcare, we ask that you designate below to whom the staff at Cook Hearing and Balance may discuss your healthcare and scheduling needs as well as billing issues that may arise.

☐ Only disclose information to myself

Name: _____ Relationship: _____ Phone: _____

Name: _____ Relationship: _____ Phone: _____

Acknowledgement of Receipt of Notice

I hereby acknowledge that I have read this medical Practice's attached "HIPAA Security Policy"

Signature: _____ Date: _____

If not signed by the patient please indicate relationship:

☐ Parent or guardian if patient is a minor

☐ Guardian or conservator of an incompetent patient

☐ Beneficiary or personal representative of deceased patient

HIPAA SECURITY POLICY
COOK HEARING AND BALANCE
1603 Medical Parkway, #200
Cedar Park, TX 78613

The Health Insurance Portability and Accountability Act (HIP AA), Public Law was enacted in August 1996 to administer and process health data in an industry-wide set standard. Cook Hearing, by law, must enact HIP AA policies to protect the confidentiality, integrity, availability and security of health information that is transmitted or stored electronically.

1. ADMINISTRATION SAFEGUARDS

1.1 Risk Analysis: Covered entity will perform a yearly risk analysis, which will provide an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of "electronic Protected Health Information (ePHI) managed by the covered entity. HIPAA Section 164.308(a)(l).

1.2 Risk Management: Covered entity will implement measures to reduce computer risks and vulnerabilities, including identifying and documenting potential risks and vulnerabilities that could impact systems managing ePHI; performing annual technical security assessments of systems managing ePHI in order to identify and remedy detected security vulnerabilities. HIPAA Section 164.308.(a)(l).

1.3 Sanctions: Cook Hearing and Balance, contractors, and BA's will adhere to the sanctions statement found in this policy, found under ENFORCEMENT. HIP AA Section 164.308(a)(l).

1.4 Information System Activity Review: Covered entity will periodically review information system activity records, including audit logs, access reports, and security incident tracking reports, to ensure that implemented security controls are effective and that ePHI has not been potentially compromised. HIPAA Section 164.308(a)(l).
Measures should include:
1.4.1 Enabling logging on computer systems managing ePHI.
1.4.2 Developing a process for the review of exception reports and/or logs.
1.4.3 Developing and documenting procedures for the retention of monitoring data. Log information should be maintained for up to six years, either locally on a protected server or through the use of protected and encrypted backup devices.
1.4.4 Periodically reviewing compliance to HIPAA, HITECH and Department of OCR.

1.5 Assigned Security Responsibility: Cook Hearing and Balance will identify a local Privacy/Security Officer and/or a backup. The officer is responsible for the adherence to this policy and to the implementation of procedures required to protect the confidentiality, integrity and availability of ePHI. HIPAA Security 164.208(a)(2).

1.6 Workforce Security: Covered entity will establish procedures that ensure only authorized personnel have access to systems that manage ePHI. HIP AA Section 164.308(a)(3). Measures that each covered entity should address include:
1.6.1 Establishing a procedure that requires managerial approval before any person is granted access to systems managing ePHI.
1.6.2 Performing appropriate background check, where appropriate, before any person is granted access to systems managing ePHI.
1.6.3 Limiting authorized persons access to ePHI to the extent that access to this information achieves the requirements of the person's job responsibilities.
1.6.4 Implementing procedures for terminating access to ePHI when the employment of a person ends or the job responsibility of the person no longer warrants access to ePHI.
1.6.5 Periodically reviewing the accounts on systems managing ePHI to ensure only current authorized persons have access.

1.7 Information Access Management: Covered entity will establish procedures in compliance with HIP AA, HITECH and Department of OCR that ensure that systems that manage ePHI have authorization controls that allow only authorized personnel access. HIPAA Section 164.308(a)(4).

1.8 Security Awareness and Training: Covered entity will ensure that their local security personnel receive periodic security updates and all BAA's and employees receive HIP AA security rule and awareness training. HIPAA Section 164.308(a)(5).

1.9 Password Management: Covered entity will implement Policies and Procedures regarding passwords on systems managing ePHI to ensure they comply with HIP AA requirements. The policy on password management is that all passwords must be renewed/changed every 90 days and must be changed immediately if compromised. HIPAA Section l64.308(a)(5).

1.10 Security Incident Procedures: Covered entity will log and document when a system managing ePHI is involved in a security incident (examples include: virus or worms, accounts compromised, and servers damaged from a denial of service attack). HIP AA Section 164.308(a)(6) .

1.11 Contingency Plan: Covered entity will have procedures in place to respond to an emergency or other occurrence that damages systems managing ePHI, HIP AA section 164.308(a)(7). Measures that each covered entity should address include having procedures for creating and maintaining backups of ePHI adequate to both restore ePHI and the systems maintaining this data; establishing procedures to restore any loss of data due to a disaster, and develop an emergency-mode operation plan that enables continuation of critical process to assure access to ePHI and provide for adequate protection of the security of ePHI while operating in emergency mode in the event an at-risk system is identified or a failure occurs.

1.12 Evaluation: Covered entity will perform an annual review to demonstrate its compliance with HIPAA, HITECH and OCR guidelines. HIPAA Section 164.308(a)(8).

2. Physical Safeguards

2.1 Facility Access Controls: Covered entity will ensure that systems that manage ePHI are kept in areas with physical security controls that restrict access. RIP AA Section 164.310(a)(1).

2.2 Workstation Use: Covered entity will ensure that only designated workstations possessing appropriate security controls will be sued to access and manage ePHI, and that these workstations are not used in publicly accessible areas nor used by multiple users not authorized to access ePHI. This security measure extends to the use of laptops and home machines. HIPAA Section 164.310(b).

2.3 Workstation Security: Covered entity will ensure that physical safeguards are in place to protect workstations that access and manage ePHI consistent with Cook Hearing and Balance Information Security Policy and RIPAA guidelines. HIPAA Section 164.310(c).

2.4 Device and Media Controls: Covered entity will ensure that procedures are in place to govern the receipt and removal of hardware and electronic media that contains ePHI into and out of the offices, and the movement within these facilities. Media can include: hard disk, tapes, floppy disks, CD ROMs, optical disks, thumb drives, and other means of storing computer data. HIPAA Section 164.31 0(d)(1). Measures should address include disposing of media with ePHI when it is discarded or reused using means that prevent its recovery and ensuring that backups of ePHI are created before systems managing ePHI are moved.

3. Technical Safeguards

3.1 Access Control: Covered entity will ensure that security controls are in place to protect the integrity and confidentiality of ePHI residing on computer systems, including applications, databases, workstations, servers and network equipment using procedures associated with HIPAA, HITECH and OCR. RIPAA Section 164.312(a)(1).

3.2 Audit Controls: Covered entity should implement an audit control from an independent reviewer to review system activity. HIP AA Section 164.312(b).

3.3 Integrity: Covered entity will ensure all systems and applications managing ePHI have the capability to maintain data integrity at all time. HIP AA Section 164 .312(c)(1).

3.4 Person or Entity Authentication: Covered entity should have controls in place that verify that a person seeking access to ePHI is the one claimed. HIP AA Section 164.312(d).

3.5 Transmission Security: Covered entity will have controls in place that ensure the integrity of ePHI is maintained when in transit. Secure transmission mechanisms that encrypt ePHI as well as confirms that data integrity has been maintained should be used. The use of e-mail for transmitting ePHI should be avoided; if required, e-mails with ePHI should be encrypted. HIPAA section 164.312(e)(1).

ENFORCEMENT:
Each employee of Cook Hearing and Balance is a covered entity under the HIP AA privacy rule. Every employee, BA's and contractors with access to ePHI is required to adhere to all HIP AA mandates. Violations of this policy may result in disciplinary action up to and including termination of employment or services. Under Federal law, violation of the HIP AA privacy rule may result in civil monetary penalties of up to $250,000 per year and criminal sanctions including fines and imprisonment. HIP AA Section 164.308(a)(1).

RESOURCE(S):

HIP AA Privacy Policy
S & S Computing
HITECH Act
Georgetown University Information Security HIPAA Policies

ACKNOWLEDGEMENTS:
Cook Hearing and Balances HIP AA Security Policy is adapted, with permission, from Georgetown University offices of Security and IT.

Erin Fogarty, University Information Security Office, Georgetown University, (202)687-2633, email: ref52@georgetown.edu.

Effective: 12/16/2019

Approved: Elizabeth Sperino

Title: Audiologist/Owner

Date: 12/16/2019