

HIPAA Auditing Tool

Department:

Site Location:

Visit Date:

Auditor:

Staff Interviewed:

Notice of Privacy Practice §164.520(c)	A covered entity must make the notice required by this section available on request to any person...A covered health care provider that has a direct treatment relationship with an individual must provide the notice no later than the date of the first service delivery...If a covered health care provider maintains a physical service delivery site, the notice must be posted in a clear and prominent location and be available by request for individuals to take with them.
--	--

Department Efforts	Compliant (yes or no)	Findings/Recommendations
NPP prominently posted		
NPP current version supply on site		
Acknowledgement supply on site		
Acknowledgement in client's chart		
Staff Interview confirms understanding of NPP distribution requirement		
Staff Interview confirms understanding of NPP content		

Administrative, Physical and Technical Safeguards § 164.530(c)	A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information
--	--

Department Efforts	Compliant (yes or no)	Findings / Recommendations
County P & Ps on site		
Designated Departmental Privacy Officer or HIPAA contact person		
Record of employee training available		
County & Dept. training material “		
Business Associate Agreements are used when necessary		

Administrative, Physical and Technical Safeguards § 164.530(c)	A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information
--	--

Department Efforts	Compliant (yes or no)	Findings / Recommendations
Client sign-in sheets and schedules contain only limited information		
Documents containing PHI are in closed folders or turned face down on desks, counters		
Sufficient locking file cabinets available		
Client charts or reports are locked in drawer or cabinet at end of work day		
Documents containing PHI are shredded prior to disposal		
Voices are low when discussing PHI		
Doors are closed when speaking on the telephone		
Private rooms are used when possible		
Clients /unauthorized personnel are escorted to and from reception area		
Restricted areas clearly identified		
Staff mail boxes are not readily accessible to clients / or visitors		
Only authorized staff have access to confidential client information and they access and use only the minimum amount necessary to accomplish their duties		
There are departmental procedures for storage and check out of client charts and sufficient documentation to locate checked-out charts		

Administrative, Physical and Technical Safeguards § 164.530(c)	A covered entity must have in place appropriate administrative, technical and physical safeguards to protect the privacy of protected health information
--	--

Department Efforts	Compliant (yes or no)	Findings / Recommendations
Staff do not discuss confidential client information among themselves in public areas or within earshot of clients, visitors or unauthorized staff		
Staff interviews confirm understanding of "minimum necessary" rule		
Client information redacted from invoices before claim submitted to auditor		
Computer monitors are turned away from view of public or unauthorized personnel		
Printers, copiers and faxes are located in secure areas		
Fax numbers are confirmed prior to sending		
Computers are locked from unauthorized access when unattended		
Passwords are changed regularly and kept confidential		
Staff interviews confirm an awareness of appropriate physical safeguards		
Staff interviews confirm an awareness of appropriate technical safeguards		

HIPAA Forms and Documentation: Authorization §164.508(c)(1)&(2) Minimum Necessary § 164.502(b) & §164.514(d) Accounting of Disclosures § 164.528	<p>A covered entity may not use or disclose protected health information except as permitted or required...and in compliance with an authorization that complies with § 164.508...</p> <p>When using, disclosing, or requesting protected health information, a covered entity must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure or request...</p> <p>An individual has a right to receive an accounting of disclosures of protected health information made by a covered entity</p>
---	--

Department Efforts	Compliant (yes or no)	Findings/Recommendations
Staff using HIPAA valid authorization		
Authorization form in clients' charts		
Department has clearly defined "minimum necessary" standards for each job category		
Department has P & P addressing routine and non-routine uses and disclosures		
Staff interviews confirm an understanding of minimum necessary standard		
Disclosure log in client's chart		
Staff interviews confirm an understanding of what disclosures need to be tracked / logged		

Complaint Process §164.530(d) Refraining from Intimidating or Retaliatory Acts §164.503(g)	<p>A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures...a covered entity must document all complaints received, and their disposition, if any.</p> <p>A covered entity must not intimidate, threaten, coerce, discriminate against or take other retaliatory actions against any individual who exercises their right to complain...testifies, assists or participates in an investigation...or opposes any act or practice made unlawful by this...</p>
---	--

Department Efforts	Compliant (yes or no)	Findings / Recommendations
Department has a process for handling issues before they are complaints		
Staff know where to get Complaint forms		
Documentation exists supporting Department efforts to resolve client issues		
Staff interviews confirm an understanding of individual's right to complain		
Staff interviews confirm an understanding of the non-retaliation policy		

Reminder: Please return all pages to County Privacy Officer when complete. **Please print legibly.**