HIPAA PRIVACY RULE AND HITECH ACT AUDIT TOOL

DEPARTMENT AND/OR FACILITY/PROGRAM: _____

ADDRESS: _____

DATE OF AUDIT: _____

CONTACT INFORMATION: _____

AUDITOR: _____

Notice of Privacy Practices (45. C.F.R. §164.520) A covered health care provider that has a direct treatment relationship with an individual must provide the Notice of Privacy Practices to the individual no later than the date of the first service delivery. If the health care provider maintains a physical site, the notice must be posted in a clear and prominent location(s) and be available for individuals to take with them.

The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Notice of Privacy Practices is/are posted in prominent patient locations, such as waiting areas and lobbies.	❑	❑	❑
The current version of the Notice of Privacy Practices is available upon request.	❑	❑	❑
The Notice of Privacy Practices is provided to the patient/client on the date of first service delivery.	❑	❑	❑
The Notice of Privacy Practices Acknowledgement of Receipt Form is in clients' charts.	❑	❑	❑
Staff interviews confirm an understanding of the Notice of Privacy Practices.	❑	❑	❑
Staff interviews confirm an understanding of patients' privacy rights described in the Notice of Privacy Practices.	❑	❑	❑
The Department and/or facility have policies and procedures for the Notice of Privacy Practices' requirements.	❑	❑	❑
Staff is aware that the Notice of Privacy Practices and the Acknowledgement of Receipt form are two separate documents.	❑	❑	❑

NOTES:

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

Administrative Requirements (45 C.F.R. §164.530) A covered entity must have in place policies and procedures that address appropriate administrative safeguards to protect the privacy of protected health information, train its workforce on those safeguards, establish sanctions for noncompliance, and establish a complaint process.			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department and/or facility designated a privacy officer or privacy coordinator to oversee ongoing activities related to the development, implementation and maintenance of the department's HIPAA and HITECH requirements.	❑	❑	❑
The Department and/or facility have an organizational chart for reporting to the Department's Privacy Officer.	❑	❑	❑
The Department has a process in place for reporting to the Chief HIPAA Privacy Officer.	❑	❑	❑
The Department has designated an individual/office to oversee the training of its workforce members on HIPAA regulations.	❑	❑	❑
The Department has designated an individual/office to establish sanctions for its workforce members who are not in compliance with the HIPAA regulations.	❑	❑	❑
The Department has a process for individuals to file a HIPAA complaint. (See additional requirements below)	❑	❑	❑
NOTES:			

Complaint Process (45. C.F.R. §164.530) A covered entity must develop and implement policies and procedures whereby individuals may file complaints concerning the entity's failure to comply with one or more of the requirements.			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department and/or facility have policies and procedures on how individuals may file a complaint.	❑	❑	❑
All HIPAA complaint forms are made available to all individuals upon request.	❑	❑	❑
The Department and/or facility have identified a contact person to receive any complaints, such as the Department's Privacy Officer and/or the facility's Compliance Officer.	❑	❑	❑
Staff interviews confirm an understanding of the policies and procedures for which an individual may file a complaint.	❑	❑	❑
The Department/facility has established reasonable timelines to investigate a complaint.	❑	❑	❑
The Department and/or facility have methods in place for notifying the individual of the complaint's disposition and any actions taken.	❑	❑	❑
The Department and/or facility have documentation to support its efforts to resolve complaints.	❑	❑	❑
The facility has a process in place to report complaints to the Chief HIPAA Privacy Officer quarterly.	❑	❑	❑
The facility logs all HIPAA complaints and maintains the log for a minimum of six years.	❑	❑	❑

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

NOTES:			
Refraining From Intimidating or Retaliatory Acts (45 C.F.R. §164.530(g)) A covered entity must not intimidate, threaten, coerce, discriminate against or take other retaliatory actions against any individual who exercises their right to complain, testify, assist, or participate in an investigation.			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department and/or facility have policies that address the process individuals can take to complain about threatening, discriminating or retaliatory actions against individuals for filing a complaint against the Department or any other agency, such as the Office for Civil Rights.	❑	❑	❑
The Department/facility has policies that sanction workforce members who retaliate against whistleblowers.	❑	❑	❑
NOTES:			
Training Workforce Members (45 C.F.R. §164.530(b)) A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information as necessary and appropriate for the members of the workforce to carry out their function within the covered entity.			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department/facility has policies that require workforce members who have access to protected health information to take HIPAA/HITECH Act training.	❑	❑	❑
The Department's training materials cover general awareness of HIPAA/HITECH Act privacy and security requirements and the Department's and facility's policies and procedures on safeguarding protected health information.	❑	❑	❑
The Department's training materials inform workforce members of individual rights regarding the use and disclosure and access to protected health information.	❑	❑	❑
The Department/facility maintains documentation that its workforce members received training in accordance with its policies and procedures on training.	❑	❑	❑
The Department/facility maintains copies of HIPAA training for a minimum of six years.	❑	❑	❑
The Department/facility workforce members know where to find the training materials, (i.e., online or in binders accessible to all workforce members).	❑	❑	❑
The Department has trained its workforce members on its sanctions' policy.	❑	❑	❑
Does the Department or facility conduct role-based training?	❑	❑	❑

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

• If your answer is yes to the above question, please answer the following question. How does the Department and/or facility conduct role-based training?			
Does the Department or facility have the ability to run a report on whether staff has received HIPAA/HITECH training? • Please provide a list of employees who have completed the training. • Please provide a list of employees who have not completed the training.	❑	❑	❑
• How often does the Department or facility run a report to ensure workforce members have completed the training prior to gaining access to PHI?			
NOTES:			

Uses and Disclosures for which an Authorization is Required (45 C.F.R. §164.508) Except as otherwise permitted or required by law, a covered entity may not use or disclose protected health information without an authorization that is valid under this section.

The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department has policies and procedures that inform workforce members regarding the uses and disclosures of protected health information that require an authorization.	❑	❑	❑
The Department and/or facility have written patient authorization forms with the required HIPAA language (e.g., date, signature, and expiration date of the authorization.)	❑	❑	❑
Copies of the authorization(s) are located in patients' medical charts.	❑	❑	❑
Copies of any revocation of the authorization are located in patients' medical charts.	❑	❑	❑
The audit review shows that staff knows to obtain written authorization when sharing patient PHI that is not for treatment, payment, health care operations, or required or permitted by law.	❑	❑	❑
The Department retains all authorizations for a minimum of six years.	❑	❑	❑
NOTES:			

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

Uses and Disclosures for which an Authorization is not Required (45 C.F.R. §164.506, §164.512) Except as otherwise permitted or required by law, a covered entity may use or disclose protected health information without a written authorization of the individual that is valid under this section. (Please note §164.510, i.e., opportunity for individual to agree or object applies.)			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department has policies and procedures that inform workforce members of the circumstances for which a use and/or disclosure of patients' protected health information are permitted without an authorization.	❑	❑	❑
Interviews with the Department's and/or facility's privacy/compliance officer or designated individual shows an understanding that protected health information may be disclosed to the individual for which the PHI is about and for treatment, payment and healthcare operations (with some exceptions, e.g., psychotherapy notes, HIV, and substance abuse, drug and alcohol).	❑	❑	❑
Interviews with the Department and/or facility staff show an understanding that protected health information can be shared for treatment, payment, and health care operations.	❑	❑	❑
Interviews with the Department and/or facility staff show an understanding the certain protected health information can be shared for coordination of care.	❑	❑	❑
NOTES:			

Minimum Necessary Use and Disclosure (45 C.F.R. §164.502 (b)) When using or disclosing protected health information or when requesting protected health information from another covered entity, 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.			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department and/or facility have policies with written guidelines that inform workforce members of the minimum necessary standards.	❑	❑	❑
The Department and/or facility or program has defined minimum necessary standards for role-based access or category of persons who need access to protected health information to carry out their job duties.	❑	❑	❑
NOTES:			

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

Accounting of Disclosures (45 C.F.R. §164.528) Individuals have a right to receive an accounting of disclosures of protected health information made by the covered entity, except to carry out treatment, payment and health care operations. (See additional exceptions under §164.502, §164.510, §164.512.)			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department has policies that inform workforce members of an individual's right to receive an accounting of disclosures protected health information.	❑	❑	❑
The Department has policies that address routine and non-routine uses and disclosures and inform staff which disclosures require documentation in patients' medical record under the Accounting of Disclosures' log.	❑	❑	❑
The Accounting of Disclosures' log has sections requesting a date, brief statement of the purpose of the disclosure, and the person/office that released the information.	❑	❑	❑
The Accounting of Disclosures' log is maintained in the patients' medical chart.	❑	❑	❑
Patients' Accounting of Disclosures' log is maintained for a minimum of six years.	❑	❑	❑
NOTES:			

Administrative, Physical, and Technical Safeguards (45 C.F.R. §164.530(c)) A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.			
The audit provides evidence of the following:	**YES**	**NO**	**N/A**
Medical Records' Room			
Medical Records' Room is equipped with technical safeguards.	❑	❑	❑
▪ The clinic has a tracking system for chart accounting.	❑	❑	❑
• Only assigned staff have access to Medical Records' rooms, file cabinets, etc.	❑	❑	❑
• All charts are returned each day. If not, please explain procedure for tracking charts not returned.	❑	❑	❑
When a drop-box is used, staff checks for incoming charts prior to checking out charts.	❑	❑	❑
NOTES:			

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

Workplace Physical Safeguards	YES	NO	N/A
Client sign-in sheets contain only limited information.	❑	❑	❑
Incidental disclosures are minimized by program staff, (i.e., voices kept low, client cases are discussed where appropriate).	❑	❑	❑
Workforce members practice Department's faxing policy and procedures.	❑	❑	❑
Caseload listings are secured each day or end of business hours.	❑	❑	❑
Clients, visitors, and other non-authorized individual are escorted in and out of non-public hospital or clinical areas.	❑	❑	❑
Clients, visitors, and other non-authorized individual are not able to access areas that contain sensitive information, unless they are escorted by facility staff.	❑	❑	❑
Fax machines, copiers, printers maintained in secure area (inaccessible by clients/visitors).	❑	❑	❑
Documents from printers are picked up without unreasonable delay.	❑	❑	❑
File cabinets, desk drawers, and shelving units containing PHI have locking mechanisms and are locked at the end of the business day or when unattended.	❑	❑	❑
Medical records and other documents containing PHI are removed from sight when clients/visitors are in clinician offices or financial offices.	❑	❑	❑
Computer screens are equipped with privacy screens or positioned to avoid unauthorized viewing by clients/visitors.	❑	❑	❑
Documents containing PHI are turned face down or put away when they are unattended.	❑	❑	❑
Documents containing PHI are locked up at the close of business.	❑	❑	❑
When meeting with patients, private rooms are used when possible.	❑	❑	❑
Staff mailboxes are not readily accessible to clients/visitors.	❑	❑	❑
NOTES:			

Technical Safeguards	YES	NO	N/A
Computers are locked from unauthorized access when unattended.	❑	❑	❑
Passwords are changed regularly and kept confidential.	❑	❑	❑
Can the system administrator enforce the Department's password policy?	❑	❑	❑
Does the system application automatically log a user off after a predefined period of inactivity?	❑	❑	❑
Is access to ePHI based upon the user's job role? (Role-based Access Controls)	❑	❑	❑
In an emergency situation, does the system application allow access by staff to a patient's electronic health information that is not included within their standard access privileges?	❑	❑	❑
• If yes to the above question, does the application capture and retain details pertain to this action for review?	❑	❑	❑
Interviews with staff confirm awareness of Department's and facility's HIPAA/HITECH IT policies and procedures.	❑	❑	❑

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

PHI is blocked from being stored on hard drives.	❑	❑	❑
Mobile devices containing sensitive information are encrypted.	❑	❑	❑
Confidential information is not saved on portable devices unless encrypted.	❑	❑	❑
Does the Department have policies that require confidential data to be encrypted before storing it on portable devices such as back-up tapes, CDs, DVDs, or devices such as laptops, hard disk drives?	❑	❑	❑
Application systems' activity logs, audit trails, and access controls are documented.	❑	❑	❑
System managers can create a retrievable, exact copy of electronic PHI when needed.	❑	❑	❑
Department and/or facility have established procedures to create and maintain retrievable exact copies of electronic protected health information.	❑	❑	❑
Department has established procedures to enable continuation of critical business process for protection of the security of electronic protected health information while operating in emergency mode. §164.308.	❑	❑	❑
Department and/or facility have established procedures to restore any lost data.	❑	❑	❑
Computers and mobile devices are sanitized upon termination of staff.	❑	❑	❑
NOTES:			
Medical Chart Review:	**YES**	**NO**	**N/A**
Notice of Privacy Practices §164.520			
Signed Acknowledgement of Receipt of Notice of Privacy Practices is retained in client's record.	❑	❑	❑
Workforce members are aware that the NPP and the Acknowledgement of Receipt are two separate documents.	❑	❑	❑
NOTES:			
Authorization for Request or Use/Disclosure of Protected Health Information (PHI) §164.508			
HIPAA – Compliant authorization form retained in client's record	❑	❑	❑
For Authorization Form, required elements present:			
▪ Identity of recipient	❑	❑	❑
▪ Identity of disclosing party	❑	❑	❑
▪ Description of PHI	❑	❑	❑
▪ Purpose of Use or Disclosure	❑	❑	❑
▪ Expiration date	❑	❑	❑
▪ Dated signature of client/personal representative	❑	❑	❑

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

NOTES:			
Right of Access §164.524			
Clients submit request to see or to get a copy of their record in writing.	❑	❑	❑
▪ If yes, staff responds to the request with appropriate form	❑	❑	❑
▪ The requests always honored in a timely manner	❑	❑	❑
Were any requests denied (in whole or partial)?	❑	❑	❑
▪ If yes, did client submit request for review of denial of access?	❑	❑	❑
▪ If client submitted the request for denial, did Program Manager follow the procedures for review of denial?	❑	❑	❑
NOTES:			
Chart Review: Clients' Rights	**YES**	**NO**	**N/A**
Right to Amend §164.526			
Clients submit request to amend their record in writing.	❑	❑	❑
▪ If yes, staff responds to the request with form.	❑	❑	❑
▪ The requests are always honored in a timely manner	❑	❑	❑
▪ Notification Letter for Amendment of PHI.	❑	❑	❑
▪ Statement of Disagreement	❑	❑	❑
Right to Special Restrictions §164.522(a)	❑	❑	❑
Clients submit request in writing.	❑	❑	❑
Documentation that the Department or facility agreed to the request.	❑	❑	❑
Right to confidential communications §164.522(b)			
Clients submit request for confidential communication in writing.	❑	❑	❑
Letter of Denial Regarding Client's Request for Confidential Communications.	❑	❑	❑
Right to Accounting of Disclosure §164.528			
Facility uses Accounting of Disclosures Tracking Sheet or Log.	❑	❑	❑
Clients submit request for Accounting of Disclosures in writing.	❑	❑	❑
Letter Responding to Client's Request for Accounting of Disclosures is in patient file.	❑	❑	❑

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

Right to Complain §164.530(d)			
Department or facility documents receipt of patient complaint in patient file.	❑	❑	❑
Disposition of complaint is documented in patient file.	❑	❑	❑
Management notified of HIPAA complaint is documented in patient file.	❑	❑	❑
NOTES:			

Breach Notification (45 C.F.R §164.404, and §13402 of the HITECH Act) A covered entity that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHI shall, in the case of a breach of such information that is discovered by the covered entity, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered entity to have been, accessed, acquired, or disclosed as a result of such breach.

The audit provides evidence of the following:	**YES**	**NO**	**N/A**
Department/facility has a policy that addresses the HITECH Act breach notification requirements.	❑	❑	❑
Breaches of PHI and/or ePHI are logged and documented.	❑	❑	❑
Facility has assigned an individual to record/document any information regarding a breach of PHI.	❑	❑	❑
Facility has trained their workforce members on the breach notification requirements.	❑	❑	❑
Workforce members are aware of the procedures in which to report a potential breach or actual breach of PHI or ePHI.	❑	❑	❑
Management is aware of the procedures to report a potential or actual breach to the department's designated privacy and/or security officer.	❑	❑	❑
The Privacy and/or Security Officer utilize the Risk Assessment Tool to determine whether the breach is unsecured or secured.	❑	❑	❑
Do you have another tool that you use with the required HITECH elements describing an unsecured breach?	❑	❑	❑
The Privacy and/or Security Officer(s) are aware of the circumstances to notify the individual of the breach.	❑	❑	❑
The Privacy and/or Security Officer(s) are aware that the Chief HIPAA Privacy Officer must be notified immediately if the breach involves more than 500 individuals.	❑	❑	❑
The Department provides the Chief HIPAA Privacy Officer a quarterly report of all the department's HIPAA breaches.	❑	❑	❑
The Department provides the Chief HIPAA Privacy Officer an annual report of the department's unsecured PHI or ePHI breaches.	❑	❑	❑
The Department is aware of the information to be included in the breach notification letter to the individual.	❑	❑	❑
NOTES:			

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

Mitigation (45 C.F.R. §164.530(f)) A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associates.

The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department has policies and procedures that address mitigation of a breach of PHI and/or ePHI.	❑	❑	❑
The Department is aware of the required elements to be included in the breach notification letter to the individual, (e.g., explain what happened, what the Department is doing to mitigate the breach, steps individuals can take to protect themselves from identity theft such as providing information about the three major national credit bureaus).	❑	❑	❑

NOTES:

Business Associate Agreements (45 C.F.R §164.504, §164.314, §13408 of the HITECH Act) Each organization, with respect to a covered entity, that provides data transmission of protected health information to such entity or its business associate and requires access on a routine basis to such protected health information is required to enter into a written contract.

The audit provides evidence of the following:	**YES**	**NO**	**N/A**
The Department has identified all business associates according to the HIPAA/HITECH definition of a business associate.	❑	❑	❑
The Department has entered into a written contract with its business associates.	❑	❑	❑
The appropriate sections of the contract have been updated or rewritten to include HIPAA/HITECH Act requirements.	❑	❑	❑
The Department has determined what protected health information is provided to which business associates, and the quality and quantity of information is appropriate for the business purposes.	❑	❑	❑
The contract between the department and business associate provides that the business associate will report to the designated person(s) any privacy or security incident that contains protected health information.	❑	❑	❑
The business associate contract ensures that any agent, including a subcontractor, to whom it provides protected health information agrees to implement reasonable and appropriate safeguards to protect such information; such assurances is pursuant to a written contract.	❑	❑	❑

NOTES:

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.

Summary of Other HIPAA Compliance Requirements			
Management retains a binder/electronic folder with policies and procedures.	❑	❑	❑
All staff (including volunteers, interns, and contractors) that have access to protected health information is HIPAA trained within a reasonable time, but no later than 90 days from their start date.	❑	❑	❑
All staff receive basic HIPAA awareness training prior to given access to PHI.	❑	❑	❑
Hard copies of HIPAA related policies and procedures are available for employees that do not have access to the Department's Intranet.	❑	❑	❑
HIPAA policies are available to staff online through the Department's and/or facility's website.	❑	❑	❑
The Department has a process to audit its facilities and clinics for HIPAA compliance.	❑	❑	❑
The Department has dedicated resources to investigate and respond to complaints and audit findings.	❑	❑	❑
The Department has dedicated resources for ongoing oversight, implementation, and maintenance of the HIPAA/HITECH Privacy Rule to remain in compliance with the regulations.	❑	❑	❑
NOTES:			

Note: This tool was modified for the 23rd National HIPAA Summit presentation and is not a comprehensive HIPAA audit tool.