

## Information Systems Audit Tool (ISAT) Overview & Instructions

### **PURPOSE of the Information Systems Audit tool (ISAT)**

Knowledge of the capabilities of a Mental Health Organization (referred to as the Contractor) information system is essential to evaluate effectively and efficiently the Contractor's capacity to manage the health care of its beneficiaries. The purpose of this assessment is to specify the desired capabilities of the Contractor's information system and to pose standard questions to be used to assess the strength of a Contractor with respect to these capabilities.

This will assist GCBH to assess the extent to which a Contractor's information system is capable of producing valid encounter data, performance measures, and other data necessary to support quality assessment and improvement, as well as managing the care delivered to its beneficiaries.

### **OVERVIEW of the Assessment Process**

Assessment of the Contractor's information system is a process of four consecutive activities.

Step one involves the collection of standard information about the Contractor's information system. This is accomplished by having the Contractor complete the Information Systems Audit Tool (ISAT). The ISAT is an information collection tool provided to the Contractor by GCBH. Data will be recorded on the tool by the Contractor. Documents from the Contractor are also requested and are summarized on the checklist at the end of this document.

Step two involves a review of the completed ISAT by GCBH reviewers. Materials submitted by the Contractor will be reviewed in advance of a site visit.

Step three involves a series of onsite and telephone interviews, and discussion with key Contractor staff members who completed the ISAT as well as other knowledgeable Contractor's staff members. These discussions will focus on various elements of the ISAT. The purpose of the interviews is to gather additional information to assess the integrity of the Contractor's information system.

Step four will produce an analysis of the findings from the ISAT and interviews/discussions with the Contractor staff. A summary report of the interviews, as well as the completed ISAT document, will be included in an audit report. The report will discuss the ability of the Contractor to use its information system to meet contractual obligations.

### **INSTRUCTIONS**

The ISAT, Document A, is provided in a format that allows the Contractor to complete and return this document electronically to GCBH via the VPN. For any questions that you believe do not apply to your organization, please mark the item as "n/a". Do not leave any questions unanswered. It is recommended to review the entire document before completing the questionnaire.

You may also attach existing documents which provide an answer to an item in the questionnaire. For example, if you have current policy and procedure documents that address a particular item, you may attach and reference these materials.

Documents B–SC should be sent to GCBH electronically, if possible, via the VPN. Note: You are **not** required to create new documentation; send only documentation that already exists. Also, you are not limited to providing only the documents listed below. We encourage you to



provide any additional documents that may help clarify an answer or eliminate the need for a lengthy response.

All documents must be labeled according to the checklist below and if needed, may be submitted multiple times. Documents must be received by the RSN at least 21 days prior to the site visit. If you have questions please contact John Bartholomew at (509) 735-8681 [johnb@gcbh.org](mailto:johnb@gcbh.org).

**Checklist for Requested Documents**

Docu ment Label	Regulation Reference	Document Title	Description
A	42 CFR 438.242 MG Contract: IS Security & Protection of Confidential Information 16.c	Information Systems Audit Tool (ISAT)	Questionnaire.
B	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Technical Safeguards 164.312(a)(2)(i) Unique User Identification (R) MG Contract: IS Security & Protection of Confidential Information 16.c	Organizational Chart	Documentation that clearly identifies the relationship among key individuals/departments responsible for information management and claims and encounter data that are reported to the RSN.
C	42 CFR 438.242, BBA: D MG Contract: IS Security & Protection of Confidential Information 16.c	Data Flow Chart	Documentation that clearly identifies how all encounter and demographic data are acquired, processed, audited, and submitted.
E	42 CFR 438.242 BBA: D	Contractor Encounter Edits	Please attach a list of specific edits performed on encounter data as the encounters are adjudicated. Note whether the edits are manual or automated functions.
G	HIPAA: 45 C.F.R. § Physical Safeguards 164.310(d)(2)(iv) Data Backup and Storage (A), Administrative Safeguard Data Backup Plan 4.308(a)(7)(ii)(A) MG Contract: IS Security & Protection of Confidential Information 16.c	Rotation Schedule and Backup and Restoration Policy	Documentation that describes backup frequency of and retention schedule for data.

AC	<p>HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Polices &amp; Procedures and Documentation Requirements 164.316(b)(2)(iii) Updates (R), Administrative Safeguards IS Review 164.308(a)(1)(ii)(D), Physical Safeguards 164.310(a)(2)(iii) Access Control and Validation Procedures (A) MG Contract: IS Security &amp; Protection of Confidential Information 16.c</p>	Access Control	<p>Documentation that describes identifying, reporting, and correcting information and information system flaws in a timely manner; providing protection from malicious code at appropriate locations within CONTRACTOR information systems; and monitoring information system security alerts and advisories and taking appropriate actions in response.</p>
AT	<p>HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: 164.308(a)(5) Security Awareness and Training, Polices &amp; Procedures and Documentation Requirements 164.316(b)(2)(ii) Documentation Availability (R), Administrative Safeguards Risk Management 164.308(a)(1)(ii)(B), Polices &amp; Procedures and Documentation Requirements 164.316(b)(1)(ii), IS System Security &amp; Protection of Confidential Information 14.3.5 MG Contract: IS Security &amp; Protection of Confidential Information 16.c GCBH P&amp;P: IS704.01.III.A.2.a</p>	Security Awareness and Training	<p>Documentation that describes how managers and users of CONTRACTOR information systems are made aware of the security risks associated with their activities and of the applicable directives, policies, standards, or regulations related to the security of CONTRACTOR information systems; and how CONTRACTOR personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.</p>
AU	<p>HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: § Physical Safeguards 164.310(d)(2)(iii)</p>	Audit and Accountability	<p>Documentation that describes how information system audit records are created, protected, and maintained to the extent needed to enable the monitoring, analysis,</p>

	<p>Accountability (A), Administrative Safeguard Access Establishment and Modification (A) 164.308(a)(4)(ii)(c), Administrative Safeguards Workforce Clearance Procedure (A) 164.308(a)(3)(ii)(B), Administrative Safeguards Workforce Security 164.308(a)(3)(i), Administrative Safeguards Sanction Policy 164.308(a)(1)(ii)(c) MG Contract: IS Security &amp; Protection of Confidential Information 16.c</p>		<p>investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity, and how the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.</p>
CA	<p>HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Security standard MG Contract: IS Security &amp; Protection of Confidential Information 16.c</p>	Security Assessment	<p>Documentation that describes how security controls are assessed in CONTRACTOR information systems to determine if the controls are effective in their application.</p>
CM	<p>HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164 &amp; NIST SP 800-64, Security Considerations in the Information System Development Life Cycle, Technical Safeguards 164.312(b) Audit Controls (R) MG Contract: IS Security &amp; Protection of Confidential Information 16.c</p>	Configuration Management	<p>Documentation that describes baseline configurations and inventories of CONTRACTOR information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and security configuration settings for information technology products employed in CONTRACTOR information systems.</p>
CP	<p>HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Physical Safeguards 164.310(a)(2)(i) Contingency Operations (A), Administrative Safeguard</p>	Contingency Planning	<p>Documentation that describes plans for emergency response, backup operations, and post-disaster recovery for CONTRACTOR information systems in emergency situations.</p>

	Contingency Plan 164.308(a)(7)(i) MG Contract: Business Continuity & Disaster Recovery 16.b		
IA	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: 164.308(1)(ii)(D)Information System Activity Review, Technical Safeguards 164.312(d) Person or Entity Authentication (R) MG Contract: IS Security & Protection of Confidential Information 16.c	Identification and Authentication	Documentation that describes how CONTRACTOR identifies information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to CONTRACTOR information systems.
IR	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: 164.310(c)(1) Integrity Controls , Technical Safeguards 164.312(e)(2)(i) Integrity Controls (A) MG Contract: IS Security & Protection of Confidential Information 16.c	Incident Response	Documentation that describes incident handling capability for CONTRACTOR information systems that includes detection, analysis, containment, recovery, user response activities, and reporting.
MA	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Administrative Safeguard Security Reminders (A) 164.308(a)(5)(ii)(A) MG Contract: IS Security & Protection of Confidential Information 16.c	System Maintenance	Documentation that describes organization-defined maintenance on CONTRACTOR information systems.
MP	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Safeguards 164.310(d)(1) Device and Media Controls (R); Physical Safeguards 4.310(d)(2)(ii)	Media Protection	Documentation that describes how information system media, both paper and digital is protected, accessed, and destroyed.

	Media Re-Use (R), 164.310(d)(2)(i) Disposal (R) Security & Protection of Confidential Information MG Contract: IS Security & Protection of Confidential Information 16.c GCBH P&P: IS702.02.II.I		
PE	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Physical Safeguards 164.310(c) Workstation Security (R), Physical Safeguards 164.310(b) Workstation Use (R), Physical Safeguards 164.310(a)(1) Facility Access Controls (R) MG Contract:14.3.1	Physical and Environmental Protection	Documentation that describes physical access to information systems, equipment, and the respective operating environments to authorized individuals; and protection against environmental hazards.
PL	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b) MG Contract: IS Security & Protection of Confidential Information 16.c	Security Planning	Documentation that describes the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
SA	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: MG Contract: IS Security & Protection of Confidential Information 16.c GCBH P&P: IS704.01.III.A.2.f, IS704.01.III.A.2.g, IS704.01.III.A.2.h, IS704.01.III.A.2.j	System and Service Acquisition	Documentation that describes allocating sufficient resources to adequately protect CONTRACTOR information systems; employing software usage and installation restrictions; and ensuring that third- party providers employ adequate security measures to protect information, applications, and/or services outsourced from the CONTRACTOR.
SI	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: 164.308(a)(8)	System and Information Integrity	Documentation that describes how information and information system flaws are identified and corrected in a timely manner; protected from

	MG Contract: IS Security & Protection of Confidential Information 16.c		malicious code; and monitored for system security alerts and advisories.
SC	HIPAA of 1996, codified in 42 USC §1320(d) et.seq. and CFR Parts 160, 162 and 164: Administrative Safeguard Log-in Monitoring (A) 164.308(a)(5)(ii)(c), Physical Safeguards 164.310(a)(2)(ii) Facility Security Plan (A) MG Contract: IS Security & Protection of Confidential Information 16.c	System and Communications	Documentation that describes protecting CONTRACTOR communications (i.e. information transmitted or received by CONTRACTOR information systems) at the external boundaries and key internal boundaries of the information systems.