

## INFORMATION TECHNOLOGY (IT) PLANS

### GAIN ABS INFORMATION TECHNOLOGY (IT) PLAN

#### *GAIN ABS Overview of Purpose and History.*

Software supporting the GAIN assessment instruments has been in development for over fourteen years. Its purpose is to provide an electronic platform for computer assisted interviewing (or data entry) for the GAIN and to provide a series of reports that can be used to support diagnosis, placement, treatment planning and outcome monitoring. In recent years there has also been an increasing emphasis on making it handle multiple users, work over the Internet, and to talk to other information systems as well.

Version 1 (FICS) was developed in PC-DOS Fortran in 1993, supported data entry and produced a narrative report. Version 2 (DOMS) was developed in Microsoft Access95 in 1997 and added data synchronization and a statistical summary report. Version 3 (ABSLite) was developed in Microsoft Access97 in 1998 and provided for data export. Version 4 (ABS) was developed in Visual Basic with a Jet database and added the Individual Clinical Profile (ICP) report. Version 5 (ABS) updated version 4 to provide support for HIPAA security configuration, interactive interviews, and the GAIN Recommendation and Referral (GRRS) narrative report.

ABS version 5 is currently in use in over 200 locations and has proven to be effective and easy to use. However, its utility is limited by several things, including its client-server architecture, which requires that software be installed and updated on each individual user's workstation, and its Access/Jet database. Both performance (maximum number of concurrent users) and maximum database size (2 GB, although in practice 500 MB is the practical limit). The GAIN Coordinating Center (GCC) has received requests for a new version with a more robust database platform (such as one of the enterprise-level SQL databases) and a web-based client to minimize demands on local IT support. This new system, GAIN ABS, will be version 6 of the GAIN software.

At the request of CSAT grantees currently using the GAIN ABS system to support their use of the GAIN, we are updating the entire system to make it available as a web-based application using an industry-standard SQL database. This update will make it possible to allow more users at the same time and to make many improvements to the interactive data entry, validation, and review process, thereby making it much easier to ensure that valid data are entered during the interview process, reducing the time required to clean data (see 6.5, "GAIN Data Receipt and Cleaning") and enhancing support for clinical decision-making immediately after the assessment. The GRRS narrative report is also being substantially enhanced, as is the ability to interact with other information systems (e.g., billing, treatment planning, progress reports). Another significant result of the move to a hosted, web-based application is the dramatic reduction in demands that will be made on individual grantees' IT staffs. Most sites will not need to install any special software and will need only an Internet connection and web browsers, which will save a typical site's ABS Administrator 1-2 person-days per month. Sites requiring offline capabilities will need to install software, but maintenance and support will still be

dramatically reduced while security of protected health information (PHI) will be enhanced. The updated system will also greatly simplify the monthly process of sending GAIN.

Planning for the web-enabled, SQL-based GAIN ABS software began in September 2005 with detailed requirement development starting in April, 2006. GAIN ABS went into beta testing in July 2008 and was released for use in production in October 2008.

### **GAIN ABS Maintenance**

GAIN ABS is maintained by the GCC Software Support team. As changes and enhancements are completed by the GCC Software Development team, they are comprehensively tested by the GCC Software Support team before being accepted and moved from the staging server to a beta test server for final acceptance testing. Accepted code changes are then implemented on the production servers, redundant Dell PowerEdge 2950 web servers using Windows Server 2003 Web Edition and Internet Information Server 6.0, and redundant Dell PowerEdge 6850 database servers using Windows Server 2003 and SQL Server 2005. These servers are appropriately configured for security and provided with uninterruptible power backup (battery and diesel generator), and data are backed up in real time to a secure off-site location. Every workday, correct operation of the production servers are verified by a review of the various information logs (web server, operating system, antivirus, firewall, backup system, and database). Patches to system software are routinely applied each Thursday, although critical patches may be applied out of sequence as appropriate. The SQL database is compacted, and tuning operations are performed as appropriate for the level of activity (at least monthly). Contingency plans, such as failover to redundant servers or backup power, are tested on a varying schedule defined in the site policies and procedures.

### **GAIN ABS Support**

GAIN ABS is supported by the GCC Software Support team. Training for end-users is provided in a number of ways, including as part of GAIN training, as a curriculum distributed to GAIN Local Trainers, as a user manual, and as a series of video modules distributed via the Internet or on DVD. The Support Team configures new agency accounts using information provided by the agency's designated contact, including agency preferences, user account creation, user permission configuration, client group creation, and GAIN instrument and template selection. In the event that a custom template or small instrument (trailer) is needed, they are created, tested, and deployed. Agencies are encouraged to have a local GAIN ABS administrator who acts as the primary contact between agency users and the Support team. Requests for support are logged in a helpdesk tracking system, and response is guaranteed within one workday (in practice, response time is typically under 2 hours). System availability is monitored by remote software sensors, and a member of the Support team is notified by pager of any outage.

### **GAIN ABS Requirements**

Functional Requirements: GAIN ABS must provide support for the GAIN family of assessment instruments with appropriate reporting and data management capabilities.

GAIN Family of Instruments: The application will support the full range of GAIN Instruments. Upon initial release it will support:

- GAIN-I version 5.6.0
- GAIN-M90 version 5.6.0
- GAIN-Q version 2.6.0
- GAIN-QM version 2.6.0
- GAIN-TxSI version 1.0.3
- GAIN-SS version 2.0

GAIN Instrument Customization: The application will support the use of named “templates” for all GAIN Instruments. When initiating a new assessment, the clinician will select both an assessment type and a template (e.g., GAIN-I Full where “Full” is the name of the template). These templates will permit defining a subset of questions which will not by default be asked while conducting an interview. These templates may be overridden during conduct of the interactive assessment to permit asking selected “not asked” questions at the discretion of the clinician.

Custom Instrument Support: The application will support development by the GCC Software Development team of additional instruments not directly part of the GAIN family of assessment instruments. This may be done in the form of “trailers” which can be made part of an assessment “template” (inserted between GAIN instrument sections) or as stand-alone instruments.

Conduct Interactive Assessments: The application will support computer-mediated conduct of the assessment interview by displaying individual questions or groups of questions with appropriate controls (text boxes, radio buttons, dropdown lists, etc.) for entering responses. Transition statements, instructions, hints and other supporting text will be displayed as appropriate. A mechanism for coding responses “Refused” (RF) or “Don’t Know” (DK) will be provided, as will a per-question staff notes feature. Responses will be validated by data-type and value and where appropriate compared with other responses and validity conflicts noted.

Data-enter Assessments Conducted Offline: The application will support data-entry of responses conducted offline using printed copies of the assessment. The format of the data-entry screen will be such as to maximize the efficient and accurate data-entry process, and will permit coding responses “Refused” (RF) or “Don’t Know” (DK). A per-question staff notes feature will be available to permit transcribing marginal notes entered by the interviewer. Responses will be validated by data-type and value and where appropriate compared with other responses and validity conflicts noted.

Organize Assessment Data by Client: The application will support creation of client records as members of an agency account’s data set. All GAIN assessments and related reports are linked to a client and grouped by treatment episode. New client records may

be created by authorized staff using the application user interface, by other applications using the application web service, or both.

Generate Printed versions of Instruments: The application will support generating a copy of an assessment/template combination in PDF format suitable for printing locally. This may be a “blank” copy with no responses, suitable for conducting an offline assessment, or an “as conducted” copy of an existing assessment including all questions, transitions, instructions and other related text on the instrument template with responses, and any questions asked which are not listed on the template (optional questions for the template used).

Generate Diagnostic Reports: The application will support generating the complete set of additional scales necessary to create the Individual Clinical Profile (ICP) report and the GAIN Recommendation and Referral Summary (GRRS). The GRRS text will be generated in a series of database fields with a web-based editing interface that will support modifying and adding to the generated descriptive text, the DSM-IV Diagnostic Impressions, the ASAM Placement Recommendations and other GRRS content. Changes to the generated text will be saved separately from the generated text so as to permit referring to, reverting to or comparing with the original text. Upon completion of all editing activities, individual sections of the report may be selected for printing and a PDF format file generated.

Share Data with Other Systems: The application will support a standard WSDL web service interface with appropriate security features (please see the IT Security Plan below) to permit interacting with other clinical information systems.

Other Functional Requirements: GAIN ABS has been designed and implemented to meet the following additional functional requirements:

1. Data Types: Boolean, integer, string, blob;
2. Connection loads: GAIN ABS supports in excess of 100 concurrent assessment activities;
3. User Interface guidelines: GAIN ABS will be accessible using the most commonly available Web Browsers (Microsoft Internet Explorer versions 6-8, Mozilla Firefox 2.x & 3.x and Apple Safari). Please see the Section 508 Compliance plan for additional user interface guidelines;
4. Reliability: GAIN ABS will be expected to be routinely available for end-user access during normal working hours (8-5) in all Continental US time zones Monday through Friday. Routine maintenance will be scheduled when possible outside these hours. GAIN ABS will be hosted at a facility with redundant power and redundant Internet connections. User data will be streamed in real-time over a secure connection to a remote site, and will be backed-up regularly to disk and stored offsite;
5. Security: Please see the IT Security plan.

Technical Requirements: Including details of the server hardware, systems software, application support software, and details of the hosting environment:

Hardware Environment: GAIN ABS is hosted on separate web and database servers. The web host is a Dell PowerEdge 2950 rack-mounted server with two dual-core Xenon 5130 2.0 GHz processors (4 MB cache), 4 GB RAM and redundant 73 GB system drives. The database host is a Dell PowerEdge 6850 rack-mounted server with four dual-core Xenon 7140M processors (16 MB cache), 32 MB RAM and redundant 73 GB system drives. Data storage is provided by a 250 GB SAN employing RAID 5 redundancy and real-time streaming via a dedicated line to a secure remote site.

Systems Software Environment: Web host systems software includes Microsoft Windows Server 2003 Web Edition and Microsoft Internet Information Server 6.0. Database host systems software includes Microsoft Windows Server 2003 and Microsoft SQL Server 2005.

Application Support Software: GAIN ABS was developed using the Microsoft ASP.NET 2.0 framework, the RichTextBox component, and uses the PrinceXML utility to output reports in Portable Document Format (PDF) format.

Hosting Environment: GAIN ABS is hosted at the Trivalent, Inc. Peoria, IL collocation center, which features multiple redundant DS3 connections to the Internet, battery-based and diesel-generator-based UPS, and comprehensive environmental controls and physical and data security (please see the IT Security Plan below). All GCC hardware are located in a dedicated, locked 42U rack with dedicated power. Dual data connections to the firewall-protected Internet are controlled by a Cisco Catalyst 2960 Gigabit switch.

## **INFORMATION TECHNOLOGY (IT) SECURITY PLAN (TASK 6.2A)**

### **Administrative Compliance**

Development of this plan has been guided by OMB Circular A-130, Appendix III, NIST Special Publications 800-12, 800-14, 800-18 Rev. 1 and 800-19, and DHHS IRM Policy 2004-002.001. The person responsible for information security for this project is Mike Vacca ([mvacca@chestnut.org](mailto:mvacca@chestnut.org) 309-451-7769).

### **4.3.2 Administrative Procedures**

The process for developing, implementing, reviewing, and maintaining operational policies and procedures adequate to identify risks to confidentiality, integrity, and availability for both GAIN ABS and RSAF are founded on the longstanding practice of Chestnut Health Systems in implementing IT best practices in the healthcare environment, with a particular focus on the HIPAA Privacy and Security rules. Existing policies and procedures are reviewed for applicability by the manager responsible for both applications, by the lead programmers and the supervisor of the GCC Software Support team. After considering the differences in operating environment and end-users,

and changes are reviewed by Chestnut MIS staff and the Chestnut Health Systems Security Officer before being implemented as policy.

Operating procedures are tested by the GCC Software Support team and, where appropriate are implemented as daily, weekly and monthly activity checklists. Adherence to operations policies is regularly verified and operations staff are encouraged to suggest changes or additions based on their experience. Summaries of operations activities are routinely reported up to supervisors and managers, and unusual events, security incidents or evidence of unexpected application behaviors are immediately reported up, including to the Security Officer if appropriate.

Any unexpected problems will be reported to the GPO within 48 hours and addressed as quickly as possible.

### **4.3.3 Physical Procedures**

Network Availability: The A5, Inc. collocation site has highly redundant fiber connections to the Internet provided by three different sources. Electric power is assured by a 500 Kwh diesel generator and an appropriately scaled battery-based UPS system on the GCC rack.

Redundant Servers: The GAIN ABS application depends on two servers – one web server and one database server. Each server is installed with a second identical server arranged in an appropriate manner to support immediate or very rapid failover in the event that the primary server experiences a hard failure. The likelihood of such hard failure is minimized by adequately scaling these servers and their use of hot-pluggable, redundant power supplies, RAID system drives and SAN data drives, battery- and generator-based UPS and careful attention to the environmental controls at the collocation site. In the event of a hard failure of the web server hardware, the secondary server can be brought into operation in 15-30 minutes with administrative intervention. The database server uses log shipping features of Microsoft SQL Server 2005 to enable rapid transition to the secondary database server in the event of a hard failure of the primary server. The RSAF application is considered less critical and thus does not use a fully redundant second server, although in the event of a hard failure the secondary GAIN ABS web server could be pressed into service by restoring a “Ghosted” image of the RSAF server. All servers and network hardware are covered by the most responsive support option provided by their manufacturers, assuring 24/7 4-hour coverage.

Locks, Alarms, and Sensors: The A5, Inc. collocation site is located in a hardened facility with highly controlled access. It is staffed 24/7 and any after-hours access requires visual identity verification as well as the normal keypad and biometric access control. Environmental controls in the facility monitor temperature, humidity, and the presence of combustion byproducts, particulate matter and liquid water penetration with sensors which are attached to alarms monitored by full-time staff.

Data Integrity, Confidentiality and Availability: In addition to the above mentioned high-availability features and access controls, all data related to GAIN ABS and RSAF are secured and backed-up in an appropriate manner. GAIN ABS data are maintained on a 250 GB SAN with RAID 5 redundancy, and are streamed over a secured line to a secondary site 37 miles away. This secondary site enjoys the same security and availability features as the A5, Inc. Bloomington collocation center. Both RSAF and GAIN ABS data are also backed-up to disk and copies transmitted to Chestnut Health Systems.

#### **4.3.4 Technical Security Services and Mechanisms**

Application Code review and Scanning: All GCC applications are developed using Microsoft ASP.NET, C# and Microsoft SQL Server 2005. Best practices as published by Microsoft and by the Microsoft environment developer community are practiced, including team programming and peer reviews. In addition, both applications are scanned periodically by an outside contractor specializing in security audits and selected by the Chestnut Health Systems Security Officer.

User Identification and Authentication: Access to RSAF requires an active account (created by the GCC Coordinator), a user ID and a password. Passwords are at least 8 characters, a combination of alphabetic, numeric and at least one special character. GAIN ABS user accounts are organized by Agency Account. Each Agency establishes their own password requirements for length, complexity and aging so as to implement their HIPAA security policy. GAIN ABS user IDs are based on a valid email account, and efforts are made to discourage more than one individual using a user ID.

User Account Management: RSAF user accounts are managed by the GCC Coordinator. GAIN ABS user accounts are initially managed by the GCC Software Support team. It is anticipated that at some future date individual GAIN ABS Agency Account holders will be able to identify a GAIN ABS Agency Administrator who will be authorized to deactivate existing user accounts, grant and deny permissions to various functions and to individual clients' and groups of clients' data.

Activity Auditing: For both applications, operating system logging (system, application and security), web server logging and database server logging is active. Both GAIN ABS and RSAF also log significant activities, either to individual log files or as status flags on database records. These logs are monitored regularly by GCC Software Support team members for the purpose of identifying security incidents, levels of activity, evidence of application flaws, and potential hardware or system software issues. Various incidents are reported up to the GCC Software Support team supervisor, the GCC Software Development team supervisor and possibly the Chestnut Health Systems Security Officer.

Firewalls: Both applications are protected by firewall configured to restrict access to the web servers to ports 80 and 443. The GAIN ABS database server is configured to only

accept connections from the web server. Administrative access to all servers is through a proprietary VPN device.

Encryption: Both GAIN ABS and RSAF are only accessible via an 128-bit encrypted Secure Sockets Layer (SSL) connection (HTTPS/Port 443).

Antivirus: All GCC servers and workstations are protected against virus and other malware infections with Symantec's Antivirus products. Antivirus definitions are kept current and status is checked regularly.

Patch Management: It is GCC policy to keep all server software, applications frameworks and components, and other software tools at their current patch level. The GCC Software Support team monitors both manufacturer-hosted and third-party lists for information about vulnerabilities and available patches. Routine patches are tested on an internal instance of the application prior to installation on production servers during a normal weekly service period. In the event of a critical, time-sensitive patch, a decision is made in consultation with the GCC Software Development team, GCC managers and the Chestnut Health Systems MIS staff and the Chestnut Health Systems Security Officer.

Controls Over Access by Other Systems: Access through the web service is controlled by three factors – an identification token, a password, and the agency account that controls the requested information. An agency account must specifically approve a given outside system and define the type of information that it may provide or retrieve before a connection is validated. Connections are only permitted at port 443 (using SSL encryption).

### Compliance

H6. EPA Energy Star Requirements: Any microcomputers, monitors or printers purchased under this statement of work will be in compliance with Executive Order 12845.

H7. Purchase of Information Resource Technology: In the event that the GCC should find the need to purchase Information Resource Technology under this Statement of Work, the Contracting Officer will be provided with appropriate information about the requested purchase not less than 30 days prior to such purchase, which shall not be made without written approval from the Contracting Officer.

H8. Software Implementation: Any software not otherwise specified in the Statement of Work that is not for the internal use of GCC staff will be presented to the Contracting Officer for approval prior to approval.

H9. Virus Protection: All GCC computers (desktop or laptop PC-type as well as all servers) are routinely equipped with Symantec AntiVirus software and policies and procedures are in place to insure that their virus definitions are regularly updated.