



---

## **The Virginia Community-Based Coordinated Services System: GetCare Standards for Data Security**

---

RTZ Associates  
150 Grand Avenue  
Oakland, CA 94612  
(510) 986-6700  
Rick@getcare.com



Technology Partners Who Can

**Prepared by:**

**Rick Zawadski, Ph.D. & Susan Maxwell  
RTZ Associates, Inc.  
January 2006**

# **The Virginia Community-Based Coordinated Services System: GetCare Standards for Data Security**

---

## **Introduction**

---

The State of Virginia is embarking on an innovative new pilot project that will enable consumers and service providers to coordinate long-term care services across multiple programs. This enhanced coordination will improve the efficiency of service delivery and the quality of care and reduce administrative burden, in addition to providing pivotal planning and outcomes information to service funders. To accomplish this coordination, electronic consumer data will be shared within agencies, across agencies, and between agencies and funders. It has long been recognized that information sharing among service providers is necessary and has traditionally taken place over the phone or through hard-copy exchange.

In fact, there is considerable national momentum for the implementation of interoperable electronic health and case management records. Since 2001, the Department of Health and Human Services (HHS) has been promoting the standardized development and use of electronic consumer information and health records. From a consumer perspective, integrated records reduce error, increase quality clinical communication between agencies as well as consumer safety and health. Increasing safety and health is particularly important for long-term care consumers, many of whom suffer from impairments in physical, cognitive, and social functioning that make them more vulnerable to health and safety threats.

In order to protect consumer data integrated in a centralized database with multiple views, the Community-Based Coordinated Services pilot project will function under stringent data security policies. Sensitive, confidential and protected consumer data will be shared only with the consent of the consumer, only with appropriate individuals, and only through technologically secure means. This paper describes the policies and the system features that will enable the

project to maximize the benefits of data sharing while also maximizing consumer protection and confidentiality.

## **Background**

---

Healthcare in the United States is witnessing an information systems revolution as consumer health information is stored electronically and shared as part of an increasingly integrated data network. By 2007, over 70 percent of healthcare organizations in the United States will move from silos of information and will begin the creation of consolidated views of patient medical record applications in order to streamline service delivery and billing. This move toward multi-agency access to integrated databases will improve the efficiency and quality of care, benefiting consumers and providers alike. One of the most important issues facing those long-term care providers shifting to integrated databases is compliance with data security guidelines under Federal and State regulations.

This paper provides background on the benefits and challenges of integrated databases and summarizes the data security requirements of the State of Virginia and the Health Insurance Portability and Accountability Act (HIPAA). The paper also provides an overview of GetCare security standards and data structures. Building on this background, the authors describe GetCare's specific access and accountability controls and the data release and restriction options the system provides to consumers. Finally, the paper illustrates several data sharing scenarios, provides a list of policy questions, and offers recommendations on data security procedures for Virginia stakeholders.

## **The Benefits of an Integrated Data Set**

---

*An integrated data set serves as a centralized database for consumer information and services, as well as management.*

The current long-term care service climate makes it imperative that identification information and clinical data reside in one common system, accessible by different caregivers and from different locations. The array of benefits resulting from an integrated data set is well documented. First and foremost, data integration facilitates the coordination of services, which becomes increasingly significant as the nation shifts away from institutional care and toward consumer-driven home and community-based care. Secondly, an integrated system reduces the burden on the consumer of repeated data collection by multiple providers. Thirdly, an integrated system creates a multi-service database for service management. Finally, an integrated system enables community-wide data exchange to measure and improve service delivery and clinical outcomes. Measuring outcomes facilitates the documentation of service gaps and statewide analysis and program planning across the state.

## **The Challenges of an Integrated Data Set**

---

*Two key challenges in data integration are regulating user access and formulating consumer data sharing options.*

While there are many benefits to an integrated data set, there are also complex challenges. Navigating federal and State compliance guidelines for data sharing can be arduous. For example, Virginia has several State departments that put forth regulatory standards; these standards may be conflicting or confusing when examined as a whole. In addition, the HIPAA Security Rules can most accurately be described as a set of best practices. They do not provide specific instructions, test cases or methods for meeting security requirements. The two major data security issues to be tackled are 1) how to regulate user access to information in the integrated database to maintain consumer privacy, and 2) how to design, track and comply with consumer consent policies on data sharing.

## Federal HIPAA Data Security Guidelines

---

*There are five major data security requirements mandated by HIPAA to maintain the privacy of protected health information.*

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates significant changes in the legal and regulatory environments governing the provision of health benefits, the delivery and payment of healthcare services, and the security and confidentiality of individually identifiable protected health information (PHI). A sizable percentage of the initial HIPAA regulations pertain to maintaining the privacy of PHI. Protected health information is any information in the medical record or designated record set that can be used to identify an individual and that was created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. Data that is person-identifiable because it includes personal identifiers such as name and address *is not* considered to be PHI because the data are not associated with or derived from a healthcare service event

As spelled out in the General Rules section of HIPAA, there are five primary requirements for compliance:

- 1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.**
- 2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.**
- 3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted.**
- 4. Ensure compliance with these requirements by the workforce.**
- 5. Maintain security of physical facilities.**

## Virginia Data Confidentiality Policies

---

*Commonwealth of Virginia data security regulations mainly adhere to the broad standards put forth by HIPAA.*

In addition to HIPAA standards, the Virginia Department of Aging, the Virginia Information Technologies Agency, Virginia's Department of Medical Assistance Services, and Virginia's Department of Social Services all have standards for data security. Security standards of these organizations

are generally less stringent than HIPAA standards, and/or refer back to HIPAA as a guideline.

**The Virginia Department of Aging (VDA)** and related organizations provide broad guidelines on the use of health information. The policy of the Commonwealth is that all personal information collected is private, and will not be sold or reused. Consumers must sign a consent form to enable transmittal of their personal data across agencies. Consumers have the right to inspect, copy and amend, to request restrictions on information disclosure, and to request confidential communications on personal health matters.

Health information collected from consumers must be used and disclosed only for specific purposes. This information can be disclosed to determine service eligibility, to provide services, to provide medical treatment, to track service and insurance payment, to provide treatment alternatives, to friends or family involved in the consumer's care, when required to do so by law, to avert serious threat to a consumer's health and safety, if a consumer does not speak English. Disclosures may be made under other circumstances; however, a consumer's written and revocable permission is required.

**The Virginia Information Technologies Agency (VITA)** has a well documented policy regarding general security practices. This security policy has 13 components, all of which contain measures as to how sensitive information is to be protected internally as well as externally. Data security and systems interoperability security are the two most relevant of the 13 main components. They are described as:

- **Data security:** owners are responsible for determining appropriate levels of data security; IT staff must protect stored data and remove data from hardware and software before disposal or reuse by other agencies.
- **Systems interoperability security:** If agencies share data, they must develop formal agreements on safeguarding the information.

VITA also has specific requirements concerning password length, maximum age, logon hour restrictions, number of attempts before lockout, password complexity enabling, and password confidentiality practices.

**Virginia's Department of Medical Assistance Services (DMAS)** strives to protect and enhance the rights of consumers by providing them access to their health information and controlling the inappropriate use of that information. Privacy regulation requires that any dissemination of information must have the consent of the consumer. HIPAA compliance requires an integrated and comprehensive approach that ensures security measures are at the highest standards. In order to maintain Protected Health Information (PHI), security measures are required to protect against unauthorized disclosure of information. However, it is also DMAS' position that PHI data may be shared for the purposes of delivery and billing of Medicaid services.

**Virginia's Department of Social Services (DSS)** requires that the Business Associate, or entity that performs functions or activities that involve the use or disclosure of PHI, may not use or disclose PHI for any other purpose other than the purpose expressly stated in the Agreement. The Business Associate also may not use or disclose PHI in a manner that would violate HIPAA regulations. The Business Associate will implement and maintain safeguards that are necessary to ensure that PHI is secure. The Business Associate will outline those safeguards that are implemented and maintained to prevent the unauthorized use or disclosure of PHI.

The Business Associate will not transmit PHI over the Internet in an insecure or open communication channel unless such information is encrypted or otherwise safeguarded using procedures no less stringent than those prescribed by HIPAA. If transmissions are performed in an encrypted form, the Business Associate shall provide the Covered Entity with the key or keys to unlock such information.

## **AN INTRODUCTION TO GETCARE SYSTEM SECURITY**

---

*HIPAA provides standards for the confidentiality and integrity of data, protection against security hazards, protection against unauthorized system use, ensuring workforce compliance, and physical facility security. GetCare's up-to-date measures comply with and exceed HIPAA stipulations.*

RTZ has been designing and managing integrated databases that maintain consumers' privacy since 1977. The GetCare database is structured for maximum compliance with consumer privacy rights and minimum data duplication, which occurs when multiple agencies create multiple records for the same client. Below is an overview of GetCare system

security features organized according to the five main security requirements of HIPAA.

### **Confidentiality and Integrity of Data**

---

GetCare provides secure, confidential and HIPAA compliant maintenance, tracking and transmittal of data. HIPAA compliance is ensured in the following ways: 1. The system only stores encrypted Social Security numbers. 2. During data transfer, data is encrypted through a Secure Socket Layer and is not decoded until it is confirmed that the correct recipient machine has received the data. 3. Data is protected by a three-tier architecture. 4. After 5 errant password logins, a lockout function is activated. 5. A firewall physically limits access to the core data set.

### **Protection Against Threats or Hazards**

---

In order to protect against security hazards, RTZ Associates' hardware staff perform an internal risk assessment and audit every six months. The company also reviews overall risk plans on a periodic basis and performs external reviews of system security.

### **Protecting Against Unauthorized Use or Disclosure**

---

The GetCare database accomplishes this through a streamlined user permission system that grants access through a series of user IDs and passwords, protected with a 64-bit encryption technology. The system accommodates several hundred permutations of user permissions and enables system administrators to limit access of users at the module level. Each of the modules in the system allows the administrator to assign the following access levels: administrative, full, read only and none. For example, local AAAs performing NAPIS reporting can view/edit their own client and aggregate data but give the state access to only aggregate data from all regions.

### **Ensuring Workforce Compliance**

---

RTZ maintains Business Associate Agreements with all customers to maintain the privacy of participant data. In turn, our customers maintain agreements with subcontractors and

staff for the protection of participant confidentiality. The Business Associates Agreements include stipulations for the responsibilities of the parties with respect to protected health information, mutual covenants between the parties and terms for termination between the parties.

GetCare also maintains audit trails historically and displays the most current changes on the lower right-hand side of most screens. The system tracks who made the last change and when that change was made. In the overall GetCare system, audit trails are tracked at the level of screens. In addition, in the Listing Maintenance tool used to manage provider listings in the service directory, the audit trail is tracked at the level of field. All data is archived in multiple locations. Databases are dumped nightly to a local and a remote hard drive. On a monthly basis, data is archived to DVD and tape.

### **Facility Physical Access Security**

---

Web-based services are provided through a secure service environment with redundant T-3 connections to ensure 24/7 system operation and availability. The server co-location sites provide a secure environment with restricted access through a sophisticated handprint identification system.

### **AN INTRODUCTION TO THE GETCARE DATA STRUCTURE**

---

*Service Directory listings, Unique Client Identification Information, and Client Contact and Basic Demographic Data are not protected health information, as defined by HIPAA.*

*In contrast, Client Service Enrollment and Case Management data are protected health information.*

GetCare is an integrated, multi-service, multi-agency database that tracks a broad array of services, client information and costs. GetCare collects and maintains different types of data, some of which is considered protected health information and some of which is not. As discussed earlier, the purpose of an integrated data system is the elimination of data duplication. GetCare provides multiple windows onto this integrated system, which are controlled on a need-to-know basis. The following section describes **1) the major data types found in the system; 2) the uses of those data types; and 3) mechanisms to control access to those data types.**

## Data Types

---

There are four basic types of data tracked and transmitted through GetCare. Data types possess varying levels of sensitive, confidential, and protected health information. GetCare is committed to the maintaining the privacy of sensitive and confidential information, in addition to protected health information.

1. **Unique Client Identification Information** (*Sensitive Information*)
  - a) Name
  - b) Date of birth
  - c) Encrypted and abbreviated Social Security numbers
  - d) Program-specific identification numbers which can be used in place of Social Security numbers
2. **Client Contact and Demographic Data** (*Sensitive Information*)
  - a) Client Contact Information, such as address and phone number
  - b) Basic Demographic Information
  - c) Contact Information and instructions, and client needs in case of emergency situations
3. **Client Service Enrollment and Recording Data** (*Confidential Information*)
  - a) Basic Assessments
  - b) Service Enrollments
  - c) Program and Service Costs
  - d) Internal/External Referral Information
  - e) Follow-up Summaries
4. **In-Depth Case Management Data** (*Both Confidential and Protected Health Information*)
  - a) Expanded Assessments
  - b) Client health status and health/nutritional risks
  - c) Medications Tracking

- d) Service scheduling, authorization and recording
- e) Care Plans
- f) Multi-Agency electronic Progress Notes

## Uses of Data

---

GetCare records varying levels of sensitive and non-sensitive data. Data are used by different agencies and staff for a range of purposes, listed below.

- 1) **Unique Identification:** to eliminate data duplication and thereby maximize operational and analytic effectiveness.
- 2) **Program Operations:** to provide operational support to long-term care service staff responsible for the delivery of services.
- 3) **Service Management:** to track, record and schedule the delivery of services
- 4) **Accountability:** to enable organizations to report activities and outcomes to funders
- 5) **Care Coordination:** to organize cross-program service coordination and high-level clinical functions across all agencies delivering services to a client
- 6) **Research & Planning:** to provide service use, service gap and service outcomes information on the local, regional, state and national level

## Structural Controls for Data Security: Access & Accountability

---

*GetCare restricts access on a need-to-know principle regulated through agency and user permissions.*

GetCare controls access to its single integrated database on a need-to-know basis. Access to data is controlled at the agency and the user level. This means that screens accessible to an information and referral agent providing service referrals will differ greatly from the screens accessible to a clinical supervisor overseeing client services for an agency.

**Access to data is determined at the agency level by:**

- 1) **The agency's target population**
- 2) **Services provided by the agency**

**Access to data at the user level is determined by individual staff roles and generally falls into six categories:**

- 1) Information & Referral Agents**
- 2) Operations Staff**
- 3) Clinical Staff**
- 4) Case managers who only see clients**
- 5) Teams who see all data on shared clients**
- 6) Supervisors who see all clients in the system**

Staff access to data is always limited to the authority of their agency, which means that staff members only have access to a subset of their agencies' data. The data subset accessed by staff is limited to the information they need to perform their role.

In addition, data access is typically controlled through each consumer's Agency of Record. Because consumers are served through multiple agencies, it is useful to designate a lead agency to maintain a consumer's core information as well as data release agreements. Typically, the Agency of Record is either the first agency to serve a consumer or the agency that provides the most in-depth services to a consumer.

Every agency incorporates user controls, such as passwords. User access is set by the agency and the passwords can be set by either the agency administrator or the user. Passwords in GetCare have variable parameters, and are designed to conform to VITA password guidelines on the number and type of password characters, maximum password age before expiration, and lockout and update procedures.

### **Methods of Access Control in GetCare**

---

While in theory it is possible to control access at the level of every variable, for operational and developmental efficiency GetCare controls access at the level of 1) system function buttons, which can include one or more screens and reports, and 2) individual screens. For example, the function button "Client Service Recording," which contains multiple screens, is only available to specific user IDs within an agency authorized to track service enrollments in the system. Controlling at the level of function button and screen enables

GetCare to provide as many standard screens as possible and to limit screen permutations for a simpler system.

GetCare's system buttons can also be organized according to types of data protected at a higher level under Virginia regulations. For example, Substance Abuse or Mental Health PHI can be consolidated under one function button requiring a higher level of access.

### **Consumer Control Over Information Access**

---

*Consumers can choose to provide partial or no data in addition to choosing if and how they want their data to be shared.*

Security regulations built into the GetCare system ensure that consumer data is accessible to agencies and staff on a need-to-know basis only. Consumers also have additional options for controlling their own information: 1) they can choose to provide partial or no data and 2) they can choose if and how they want their data to be shared. Consumers have five major options for limiting access to their information. They can achieve these options either by choosing what data they provide in the first place or through stipulating their confidentiality wishes on a data-sharing agreement.

In practice, the level of control available to a consumer varies depending on which services a consumer uses. For example, a consumer can receive a service referral whether or not they choose to give any identification information. However, a consumer enrolling in a Medicaid-funded service is required to give their actual social security number to receive services.

*During data collection by agency staff, consumers have the following three options for providing non-identifiable data:*

- 1) Non-Provision of Data:** Consumers served through GetCare's Information & Referral system may receive service information and referrals without giving any information about themselves.
- 2) Anonymous Response:** Consumers may also choose to provide personal information, such as demographics, but no identification information, such as name, social security number, etc. This method is viable for some service enrollments, such as Legal Services, but not Medicaid-funded services.
- 3) Non-Identifiable/Pseudonym Response:** Consumers may choose to provide personal information linked to a pseudonym. The advantage of

this method is that an individual's information can be tracked over time without identifying the person.

*If consumers do provide identifiable data, they have the following options for managing access to that data:*

**4) Identifiable Response:** Consumers who provide identifying and protected health information will sign a release form, stipulating how they want their data to be managed. Consumers will choose from three preferences for data sharing:

- i. **Data Release** enables consumer information to be shared with agencies delivering or managing services for the consumer. ***Data release does not mean that all agencies have access to a consumer's data.*** A consumer must be either referred to or enrolled in an agency's program in order for that agency to access his/her contact, demographic, enrollment and case management data. The only data accessible system-wide are unique identifiers with encryptions. In addition, information is always restricted within agencies to only the staff who need to know that information, as described in the sections above.
- ii. **Service-Specific Release** functions through a **Consumer Key**, which is an alpha or numeric code consumers choose when they enter the system. The Consumer Key is a password used to unlock an individual's data. Consumers control who sees their data by granting access only to those agencies they approve.
- iii. **Restricted Data** stipulates that a consumers' data not be shared across agencies. In cases of data restriction, GetCare can create separate parallel records for use by different agencies. However, the total restriction of data inhibits coordination and can hamper the quality of care. For example, if a case manager cannot make a service referral directly, the client is required to self-refer and to provide assessment and personal information multiple

times. If service providers cannot coordinate a care plan for a client, they cannot as effectively build upon their knowledge of that client's needs and capacities.

## **Consumer Key Policies and Procedures**

---

For the Community-Based Coordinated Services pilot in Virginia, we anticipate that most people will choose to automatically share their data with those agencies serving them and that only about 10%-15% of all the consumers will choose to use the Consumer Key. Similar data sharing concepts were tested through the San Francisco Department of Health's coordinated, standardized client registration system (REGGIE) for HIV-related services. The REGGIE project found that over 90% of all clients chose to grant cross-agency access to their data. Although the concept of consumer control may have slightly more limited application among the senior population, the data sharing options presented here provide a wide range of choice to Virginia's consumers.

The Consumer Key represents a level of data security that exceeds HIPAA requirements and operationalizes RTZ's commitment to consumer direction. For those consumers using the Key, the most significant procedural question is what to do in cases of lost and forgotten key codes. At their Agency of Record, a consumer is first entered into the database and given their alpha or numeric key code. When authorizing and activating their Key, each consumer also answers a set of security questions, such as "what is your mother's maiden name" or "what is your pet's name." These questions can be designed to query 1) for information not normally available in the GetCare client database, or 2) for "standard" CARE tool data, such as demographics or personal contact information.

When a consumer contacts a new service agency, he/she gives the code to the intake staff member, who uses it to unlock the consumer's data. If the consumer does not have their Key, the system displays a screen informing the staff member that the consumer's data is not accessible. The screen also displays the set of security questions originally answered by the consumer during Key authorization. The consumer or his/her guardian then provides the answers for the staff member to enter into the system. By answering the

security questions, the consumer authorizes data sharing and the agency gains access to the consumer's record.

### **Data Sharing Scenarios**

---

The following data sharing scenarios illustrate operational possibilities and challenges that will arise in the course of service provision.

**Scenario 1:** A consumer calls an information and referral service and wishes to not provide any data about him/herself. In that case, the agent will simply record in the database what contact event took place, i.e. a referral was given to a transportation program.

**Scenario 2:** A consumer calls an information and referral agency and is willing to provide data. To expedite operations, the agent collects unique identifying information so the consumer's record can be retrieved in the future. To enhance program research and planning, the agent collects demographic and basic service needs information.

**Scenario 3:** A consumer completes an intake at Program X, the Agency of Record, and later enrolls in Program Y. If the consumer wishes to share his/her information with Program Y, there are three possible scenarios depending on the consumer's original data sharing authorizations on file with Program Y. *(In all of the following scenarios, Program Y will have access to that consumer's Unique Identification information.)*

- a) If the consumer agreed to share his/her data between agencies, Program Y enrolls the consumer and automatically gains access to the consumers' data. **The consumer must be referred to or be enrolled in Program Y's services for Program Y to access his/her data.**
- b) If the consumer has a Consumer Key, the consumer gives Program Y his/her key identifier to unlock data.
- c) If the consumer stipulated no sharing of data, s/he can either repeat intake data collection with Program Y or sign a new release form with Program Y in order to authorize the sharing of data.

**Scenario 4:** Data security policies around sharing Electronic Progress Notes are especially important due to the sensitive nature of notes. Some notes, such as those recording shifts in service scheduling or changes in functional status, need to be shared. Some notes, such as those recording personal psychosocial information disclosed by the client, need not be shared. RTZ has performed pilot studies on different methods of sharing Progress Notes, and recommends that notes be coded at four levels: **Private Draft, Final Private, Final Shareable within Agency, and Final Shareable Across Agencies.** Notes coded as Draft can be updated and edited. Notes coded as Final are date and time stamped and cannot be changed. Notes coded as Private are only accessible to the staff member entering them, and, if policy allows, the staff supervisor. Notes coded as “shareable” can either be shared within the agency or across agencies.

### **Policy Questions**

---

Data security and sharing technology practices raise an array of implementation and policy questions to be discussed by Virginia stakeholders. The following is a partial list of those questions.

1. When is a Consumer Key necessary? What data may be accessible regardless of Key authorization?

2. When is a written authorization required for data sharing and when does verbal consent suffice?

3. What is the best way to ensure consumers receive the services they need if they wish to refrain from sharing data?

4. What are the additional technological and operational costs of ensuring possibilities for data restriction?

5. What operational steps should be taken when consumers require guardians to help them make data sharing decisions?

6. How will a consumer's Agency of Record be determined? Who will make that determination? How will the Agency of Record be changed, if necessary?

7. Are there situations in which Progress Note privacy codes should be overridden?

8. What kind of consumer service and health data, i.e. substance abuse and mental health information, should be protected at a higher level than other PHI data? How should segregation of this data be accomplished?

9. In cases of multiple parallel records, which record should be used for outcomes study in program research and planning?

10. Should Client Contact and Basic Demographic data be shared system-wide on a need-to-know basis?

## Recommendations

---

*An integrated database of non-duplicated consumer information is pivotal for the delivery of quality care across services and agencies.*

Because sharing data makes it easier for consumers to apply for and receive services, RTZ's overall recommendation is to share as much data as safely as possible. An integrated database of non-duplicated consumer information is pivotal for increasing access to services and for the delivery of quality care across services and agencies. While data sharing risks do exist, the GetCare system successfully minimizes those risks. Although less often highlighted, the health risks and service impacts resulting from *not* sharing data are perhaps more critical to the consumer.

Keeping this in mind, it is the responsibility of the community and agency to explain the importance of data sharing decisions to each consumer. The consumer must understand and appreciate what will happen as a result of releasing or not releasing data. If consumers wish to restrict their data, they must deal with each agency individually to obtain needed information, and/or agencies may not be able to provide services.

## **Data Sharing Best Practices**

---

### **Unique Client Identification Information**

**Data Sharing Recommendation:** To create a usable, non-duplicated database, it is necessary to share this minimum data set across agencies. Unique identifiers do not disclose protected health information or sensitive identification information, such as social security numbers. In addition, GetCare can also be adapted so that agency users will only see unique identification information for their regional service level, as opposed to statewide.

### **Client Contact and Basic Demographic Information**

**Data Sharing Recommendation:** The sharing of client contact and emergency information across agencies is very useful, especially in emergency situations. In San Francisco and Southwest Arkansas, agencies share this information as common practice. RTZ recommends sharing this data to better ensure the health and welfare of consumers.

### **Client Service Enrollment and Recording Information**

**Data Sharing Recommendation:** The sharing of Client Service Enrollment and Recording Data requires consumer authorization. Even with consumer authorization, only approximately 60% of agencies and staff users will require access to this data.

### **In-Depth Case Management Information**

**Data Sharing Recommendation:** The sharing of In-Depth Case Management Data requires consumer authorization. Even with consumer authorization, only approximately 20% of agencies and users will require access to this data.

### **Progress Notes**

**Data Sharing Recommendation:** RTZ recommends the coding of Progress Notes on four levels: **Private Draft, Final Private, Final Shareable within Agency, and Final**

**Shareable Across Agencies.** Coding notes on multiple levels gives staff the range of confidentiality options they need to document work with clients and to improve care coordination across agencies.

## **Research & Planning Recommendations**

---

If consumers choose to restrict their data, separate parallel records will be created for that consumer by different agencies. The creation of separate parallel records, and therefore multiple UAIs, will have consequences for the research and planning of programs. Policy concerning which UAI to be used during outcomes research will need to be determined. Some research options are 1) using the most recent assessment 2) using the assessment completed by the staff member with the most clinical training, or 3) using the assessment completed by the Agency of Record.

In addition, RTZ recommends a comparative study of service provision, cost, clinical, and quality of life outcomes between consumers with multiple records and consumers with integrated records. This analysis will indicate the impacts of data sharing on consumers and reveal what factors are likely to inhibit or promote consumer data sharing.

## **Summary**

---

The Virginia Community-Based Coordinated Services System has two main objectives: 1) to deliver to Virginia consumers and service providers the considerable benefits that accrue from the multi-agency exchange of data, and 2) to ensure that data is shared safely and appropriately.

RTZ Associates, the designers of GetCare, have been maintaining long-term care data security since 1977. The integrated GetCare database is structured for maximum protection of sensitive, confidential, and protected information with minimum data duplication. In addition, policies and systems of data security will evolve during the pilot project, and the technology for protecting confidential information will also evolve, providing even more comprehensive systems and security for the future.

## Appendix 1: Data Security Matrix

The following table shows a matrix of the five data types in the system, the uses of each of those data types and the levels of consumer control and security that can be applied to each.

**Table 1: GetCare Data Security Matrix**

Data Type	Use of Data	Options for Consumer Control of Data					
		Non-Provision	Anonymous	Non-Identifiable/ Pseudonym	General Release	Service-Specific Release: Consumer Key	Data Restriction
Service Directory Provider Listings	Research & Planning	NA	NA	NA	NA	NA	NA
Unique Client Identification Information	Unique Identification	✓	✓	✓	✓	✓	
Client Contact and Basic Demographic Data	Program Operation				✓	✓	(Determined By Policy)
	Service Mgmt						
	Research & Planning						
Client Service Enrollment and Recording Data	Program Operation				✓	✓	✓
	Service Mgmt						
	Research & Planning						
In-Depth Case Management Data	Care Coordination				✓	✓	✓
	Research & Planning						

## Appendix 2: DATA SHARING AGREEMENT

---

*I understand that different agencies provide different services and benefits. Each agency must have specific information about me to provide services and benefits. By signing this form, I am specifying whether or not I want my confidential information to be shared between agencies for the purpose of service delivery.*

I, \_\_\_\_\_, am signing this form for  
*(FULL PRINTED NAME OF CONSENTING PERSON OR PERSONS)*

\_\_\_\_\_  
*(FULL PRINTED NAME OF CLIENT)*

\_\_\_\_\_  
*(CLIENT'S ADDRESS)*

\_\_\_\_\_  
*(CLIENT'S BIRTHDATE)*

\_\_\_\_\_  
*(CLIENT'S SSN - OPTIONAL)*

My relationship to the client is:  Self    Parent    Power of Attorney    Guardian  
 Other Legally Authorized Representative

---

### Different Kinds of Data Agencies May Collect & Share:

1. **Your Unique Identification Information** (name, encrypted ssn)
2. **Your Contact and Demographic Data** (address, emergency contacts, age, gender and other demographic information)
3. **Your Service Enrollment Data** (service referral, enrollment, and follow-up information)
4. **Your Case Management Data** (assessment, medications and service scheduling information)

### Options for Data Sharing:

**General Release:** I wish my confidential information to be shared with all agencies whose services I am enrolled in or referred to. I understand that only those staff members who need access to my data to serve me will be given my information. I understand that exchanging certain information will make it easier for agencies to work together effectively to provide or coordinate my services or benefits.

**Service-Specific Release:** I wish to share my data only with those agencies I personally authorize. I understand that I will be given an authorization code called a

Consumer Key, and that I will be responsible for sharing that code with agencies I authorize to have access to my data.

**Data Restriction:** I **do not** wish to share my data across agencies. I understand that choosing this option means that I will need to personally supply my information to each agency individually. I also understand that I may not be able to receive certain services that require data sharing.

---

**This agreement is good until:**  My service case is closed.  Other: \_\_\_\_\_

*DECLARATION OF CONSENT*

I can change this agreement at any time by telling the referring agency, also called my Agency of Record. I have the right to know what information about me has been shared, and why, when, and with whom it was shared. If I ask, each agency will show me this information. I want all the agencies to accept a copy of this form as a valid consent to share information.

Signature(s): \_\_\_\_\_ Date: \_\_\_\_\_  
*(CONSENTING PERSON OR PERSONS)*

Person Explaining Form: \_\_\_\_\_