



*Delaware Health
And Social Services*

DIVISION OF MANAGEMENT SERVICES

PROCUREMENT

DATE June 15, 2007

PSC#0761

CLINICAL CARE INFORMATION SYSTEM PROJECT
MANAGER

FOR

DIVISION OF SUBSTANCE ABUSE AND MENTAL HEALTH

Date Due: July 13, 2007
11:00 AM

ADDENDUM # 3

PLEASE NOTE CHANGE IN DUE DATE

THE ATTACHED SHEETS HEREBY BECOME A PART OF THE ABOVE
MENTIONED BID.

SANDRA S. SKELLEY, CPPO, CPPB
PROCUREMENT ADMINISTRATOR
(302) 255-9291

DARLENE PLUMMER(302)255-9430

RESPONSES TO QUESTIONS AND ANSWERS SUBMITTED
FOR RFP PSC0761

PLEASE ACCEPT OUR APOLOGIES FOR THE DELAY IN RELEASING THIS
INFORMATION

ALSO NOTE THAT THE DUE DATE FOR SUBMISSIONS HAS BEEN CHANGED
TO ON OR BEFORE 11:00AM ON FRIDAY JULY 13, 2007

1. Information Technology) The stakeholders in this project in this project are the Division of Substance Abuse and Mental Health, the Information Resource Management (IRM) Unit, the Department of Technology and Information (DTI), and possibly certain substance abuse treatment providers that are interested in utilizing this system.
2. How many staff members will be allocated from the Delaware Health and Social Services division or other state entities? The DHSS staff assigned to this project are listed below:
 - IRM Project Leader .5FTE
 - Budgeted Sr Application Support Specialist 1 FTE
 - 2 Sr Application Support Specialist 2 FTE
 - IRM Project Manager .3FTE
 - DSAMH Project Director .3FTE
 - Clinical Subject Matter Experts 3FTE
3. What is the targeted timeframe for vendor selection of the Clinical Care Information System? We are currently in negotiations and anticipate having a contract in July.
4. Following the vendor selection, what is the estimated timeframe for the contract negotiation phase with the system vendor? Will you use technical resources/professional services from the vendor to implement the system?
5. What is the estimated timeframe for the implementation of the system from the signature on the contract to production? Implementation will be one year from the project kickoff.
6. Do you use standard documentation developed by the Delaware Health and Social Services Department for:
 - a. Project Planning/Work Breakdown Structure
 - b. Status Reporting
 - c. Business Requirements/Traceability Matrices
 - d. Functional Requirements
 - e. Technical Specifications
 - f. Change Control
 - g. Risk Management
 - h. Contingency Planning
 - i. Communication Plan
 - j. Disaster RecoveryIf not, is the contractor allowed to propose documentation templates? The contractor is allowed to propose documentation templates.
7. Who will be responsible for determining the functionality requirements for the system? This will be the responsibility of the IRM Project Manager, DSAMH Project

- Director, the IRM Project Leader, the DSAMH Implementation Team, and the Clinical Subject Matter Experts.
8. Who will be responsible for determining the business requirements for the selected system? This will be the responsibility of the IRM Project Manager, DSAMH Project Director, the IRM Project Leader, the DSAMH Implementation Team, and the Clinical Subject Matter Experts.
 9. Attachment 3 Section B #16 refers to Appendices A, B, and C. What is the content of these Appendices? Appendix A is a boilerplate that refers primarily to program service providers. Appendix B will be the negotiated workscope awarded for this project, and Appendix C will be the negotiated budget awarded for this project.
 10. Attachment 3 Section C #2 refers to Appendix C and the contract budget. What is the budget for the project management segment of the project? We do not have a budget.
 11. Attachment 3 Section D #1 refers to the requirements of DHSS Policy Memorandum #46. How do we obtain this memorandum? See attached #1
 12. What is the standard architectural platform for the state? See below
 13. Section 2.1: Is the State seeking full-time on-site presence by the selected project management consultant? Would the State be open to proposals that involve a combination of on-site and off-site services? We would be willing to negotiate
 14. Section 2.1: Is the State seeking a single individual to provide these services or would the State be open to a team approach? The rfp indicates a single individual but you should propose based on your recommendations.
 15. Section 2.1: This section refers to “State Project Managers.” What management-level resources is the State dedicating to this project? Where does the consultant selected for this project fit within the State’s team? (e.g., Will the selected consultant be the lead State project manager for the system implementation or do you envision the selected consultant to fill more of an independent and objective oversight role working in partnership with the State’s management team?) Who will the selected project management consultant report to? See above for state staff listing. It is our intent that the Project Manager will oversee the awarded contractor staff and the state staff and will report to the DSAMH Division Director.
 16. Section 5G states requests bidders to describe “past and present relationships with the bidding entities of the DSAMH CCIS Project.” A list of the vendors attending the pre-proposal conference is posted. Did all of these vendors submit a proposal or is there a separate list naming vendors that submitted proposals? The list of vendors given were those that were able to submit a proposal and our request in Section 5G was to be made aware of any relationships with those vendors.
 17. On page 62 (Section 6.1.5) of the Clinical Care Information System RFP, the schedule indicates that a contract would be finalized on/by January 2, 2007, with a one-year system implementation timeframe. Has a system vendor been selected? If so, can the vendor name be made available to prospective bidders? Also, if a vendor has been selected, have system implementation activities begun? We are currently in final negotiations with a vendor. The name will not be released until a contract has been fully executed.

DHSS Information Technology Environment

Version: May 2007

A. Introduction

The purpose of this document is to outline the information technology (IT) environment at Delaware Health and Social Services (DHSS). The document is intended to serve as a component of RFPs and RFIs for IT procurement. It describes the current and planned environment in sufficient detail that prospective vendors can determine the degree of fit between DHSS' environment and their products.

B. Mainframe Environment

DHSS has a number of applications running on a dual processor IBM z/890 mainframe. The current operating system is z/OS version 1.5. The data communications manager is CICS TS version 2.2. Security management is through ACF2, version 8.3. The CPUs of the mainframe were last upgraded in October 2004 and the mainframe now supports capacity on demand as well.

DHSS also has a number of applications, including Child Support, Employment & Training and Day Care, which have their online components developed in a third generation language, ADS Plus version 11.

Currently, the DBMS on the mainframe is DB2 version 8. Only DB2 is supported for new development. OS/VS COBOL version 1.2, VS COBOL II Version 1.4, COBOL for OS/390 & VM Version 2, and Enterprise COBOL for z/OS and OS/390 Version 3.4 are installed, but only Enterprise COBOL for z/OS is supported for new development.

The operational and technical support for the above environment, which is located in the Biggs Data Center, is provided to DHSS under contract by the Delaware Department of Technology and Information (DTI).

The mainframe production system is not currently supporting 24x7 applications.

C. Client Server Environment

The following development languages are currently in use for the client server environment: Centura Team Developer 1.5.1, 3.1 & 4.2 PowerBuilder 9 & 10, and Borland Delphi 5 & 6. Please note that such client/server languages are considered deprecated for new development and are only currently maintained to continue legacy maintenance support.

The following client server databases are currently in use: Microsoft SQLServer 2000 and 2005. Microsoft SQLServer 2000 and 2005 are the only client/server database manager supported for new development.

D. DHSS currently maintains a clustered Microsoft SQLServer 2000 system that is available 24x7 with fail over and redundancy and a SQLServer 2005 stand alone database server for reporting. DHSS plans is to house all DHSS SQLServer databases on the existing cluster and to upgrade the cluster to 2005 before the end of 2008. This system supports mixed mode authentication. Vendors should be aware that domain authentication is preferred.

E. Hybrid Mainframe/Client Server Environment

In 1998, a new version of DHSS' Delaware Client Information System (DCIS II) was implemented statewide for the Division of Social Services. The interactive component of this application, which runs on a Citrix Metaframe Server, was developed using PowerBuilder. DCIS II utilizes a DB2 database on the IBM mainframe. The client connects to DB2 using Proginet's TransAccess. TransAccess is a middleware product that allows the exchange of information between the personal computer and mainframe platforms by means of CICS Remote Procedure Calls (RPC).

Neon ShadowDirect is a host-based product, which allows ODBC calls to the DB2 database. ShadowDirect enables DB2 access from any standard programming language. This is the DHSS standard method of connectivity for new hybrid application development. DTI is in the process of converting to the new Shadow RTE product which includes upgrades to the ODBC and Zservices connect methods. The mainframe production system is not currently able to support 24x7 hybrid applications.

Hybrid applications of this sort are considered deprecated for new development.

F. Web-Based Environment

Web browser based applications are now considered the only acceptable platform for custom applications development at DHSS. Additionally, in the purchase of any COTS system, web browser based systems will receive preferential treatment.

To support this initiative, DHSS has implemented a series of high-capacity, redundant, and load-balanced web & application servers at the Biggs Data Center. These systems use Microsoft Windows 2003 Enterprise Edition as their operating system and Microsoft Internet Information Server (IIS) 6.x as their web and application server software.

The web server farm at DHSS is protected by a firewall and addresses are NAT'd to an external IP address for access by external users. The internal IP address points to a load-balancing F5 switch running BIGIP which distributes load across the servers in the farm and houses SSL Security Certificates.

The application server farm is configured in a similar manner but is placed behind an additional firewall for further protection.

The application servers can then access databases placed behind yet another firewall for their data stores. Web browser based applications can use either the Microsoft SQL Server cluster described above or the mainframe DB2 database for their data store but the Microsoft database platform is the preferred platform due to its higher availability and failover capacity.

The standard development environment for web browser based applications at DHSS is the Microsoft .NET Framework version 1.1. or 2.0. The standard tool for development in this framework is Microsoft Visual Studio 2005 Enterprise Edition. Other development environments can be considered on a case-by-case basis (please note though that an individual project may make more restrictive determinations concerning development environment).

There are specific standards required for developers working in the .NET environment for DHSS. A comprehensive standards manual can be found at:

<http://www.state.de.us/dhss/dms/irm/files/dhssdotnetmanual.pdf>.

All web pages (whether part of web browser based application or simply part of a standard web site) developed for or by DHSS must conform to departmental and state web standards. These standards include provisions for making web pages accessible to disabled users and address many items required by law for public sector web sites. The standards can be found at:

- o <http://www.state.de.us/dhss/admin/files/pm26.pdf>
- o <http://www.state.de.us/dti/pdfs/State of Delaware Web Guidelines version 2.0.pdf>

Please note that these standards are living documents and subject to revision.

G. Application Deployment

All vendors must supply IRM Application Manger and DHSS Manager of Base Technology detailed instructions for installing and configuring the applications/databases in Both the TEST and PRODUCTION environments. IRM will not deploy any applications without proper documentation.

Network Environment

- A. The DHSS wide area network is built around Verizon's TLS network. Connectivity to 31 of the 46 DHSS Sites is currently supported through 10MB TLS circuits utilizing Cisco routers at the edge. The remaining 15 utilize a mix of DSL, Cable and directly connected fiber for connectivity. Switching technology is used at all remote sites. On the main DHSS campus is housed the Biggs Data Center. Within this data center is the core Cisco switch that is connected to the State network through a 100MB Ethernet connection. The network fully supports TCP/IP. Other communication protocols are currently not supported across the

Wide Area Network.

The larger remote sites have a Windows 2003 file and print server onsite. The campus utilizes an EMC CX500 SAN and multiple Windows 2003 clustered file and print servers for data storage. In addition to the Windows 2003 file and print servers, DHSS operates about three dozen Windows 2000/2003 servers supporting client server databases, web servers, and terminal server/Citrix farms. Authentication is provided by Microsoft Active directory.

As of the date of this document, State of Delaware standards specify dual core based processors as the default choice for workstations. Almost all employee workstations are currently running either Windows 2000 Professional or Windows XP Professional. Windows 2000 Professional workstations are not being upgraded to Windows XP on a regular basis but as new workstations are purchased, the older operating system is phasing out. DHSS' PC inventory as of January 2007 is approximately 3700.

H. Citrix MetaFrame/Terminal Server Environment

DHSS currently supports Metaframe Presentation Server 4 as a standard for allowing remote connectivity to client server applications. Any new client server systems purchased must be tested on and be compatible with the Citrix MetaFrame/Terminal Server environment.

DHSS currently supports Citrix Secure Gateway to expose client server applications to the Internet for non-state network users.

I. Other Environmental Considerations and Standards

1. Master Client Index Requirement

All applications that support the provision of services to DHSS clients must identify individuals by using the unique Master Client Index (MCI) number as a standard identifier across both mainframe and client server systems. The MCI number is a ten digit number assigned by the mainframe MCI system. At a minimum, all software supporting client services must include the MCI number as a mandatory data element.

Use of the MCI system must be integrated with client services applications. If the client services application is not host-based, the integration would involve Neon ShadowDirect ODBC or ZServices access to the DB2 database.. Currently a Client/Server based interface is available and there are plans to create a web service based interface in 2007/2008. The interface involves both demographic data (e.g. name, sex, date of birth, ethnic code, SSN) and program (case history) information (e.g. program identifier, case status, start date, end date).

2. Disaster Recovery

DHSS currently maintains Disaster Recovery plans for all supported production platforms running at the Biggs Data Center. DHSS has contracted with Sunguard Recovery Services for mainframe production system off-site recovery and a project is currently in process to provide similar services for client/server and web browser based systems.

3. System Backups

The mainframe environment has a fully functioning backup system with off-site tape storage contracted through Vital Records Incorporated (VRI). The server-based environments use a mix of standalone tape backup and a Commvault Enterprise backup solution. Off-site tape storage for server-based systems is also handled under contract from VRI. The Commvault backup solution is the required backup solution for all new server-based systems at DHSS.

4. Office Automation Standards

DHSS personal computers are all licensed to run the latest version of both the Microsoft Windows operating system and Microsoft Office Professional. Microsoft Outlook is the standard e-mail package in use at DHSS.

5. Host Terminal Emulation

Currently, Attachmate's Extra Personal Client is the standard DHSS desktop host terminal emulation software. This package supports mainframe communication through 3270 emulation and asynchronous hosts such as UNIX through telnet.

6. HIPAA

The Federal Health Insurance Portability and Accountability Act (HIPAA) standards govern how health related information is handled. These regulations cover transaction and code sets, privacy, security rules and the National Provider Identifier (NPI). All health care related software acquired by DHSS must conform with standards promulgated under HIPAA within the statutory timeframe.

7. Security

DHSS software must provide extensive security features to safeguard data, particularly client related data, from unauthorized access, alteration or damage. There should be levels of protection such that authorized users can execute specific functions in line with their responsibilities. User agencies are responsible for determining and defining any additional security features required by state or federal mandates.

8. Data Integrity

Applications must check for the completeness and accuracy of critical data elements as they are being entered. The system must be able to designate required data elements, so that the user must enter a valid value before the data can be accepted into the database.

9. Reporting

Applications should allow information to be reported both through selection of predefined reports that can accept limited parameters from the users. (Eg: All clients within a specific date range). All reporting in on-line Productions systems should utilize a Reporting database where possible. IRM will deploy the reporting database server and allow replication of Production data for on-line and Ad-Hoc reporting in 2007/2008. .

10. Data Export and Import

Client server and hybrid applications should allow for both the import and export of data using standard file formats. Import and export procedures should be flexible enough to allow users to select specific data elements. As a minimum, systems must support import from and export to Microsoft Excel spreadsheets.

11. Database Archiving

To facilitate database maintenance, when appropriate the software should provide an automated process for the regular archival of inactive records from the database to offline storage. A procedure also should be provided to return archived records to the active database.

12. Database Modeling

Data models and dictionaries are required for any new system. Data models must supply table relationships. Data dictionaries must include detailed description of Tables and table entities. Visio 2003 & 2007 are supported at DHSS for data modeling. Vendors may propose different tools. DHSS will evaluate the tools to determine if they are acceptable for the project. If the proposed tool does not meet with DHSS standards/approval then the vendor will be required to supply the model in MS Visio.

13. Software Escrow

If source code is not surrendered to DHSS as part of a project, vendors will make provisions to escrow applications source language, to be made available to DHSS if for any reason the applications are no longer supported. Each vendor will describe its escrow arrangements.

14. Software Style and Functionality

Applications should be designed in modular fashion, so that modules can be phased into the system, as they are developed. The user interface should be accessible, understandable and customer friendly. Redundant data entry should be avoided. Screens should be clean and uncluttered and should have the same look and feel throughout the application. Applications should be menu driven and menus should have the same format and common menu options across all parts of the system. Context-sensitive help text should be readily available throughout the system.

15. Compliance with Federal Requirements

All software acquired by DHSS must conform to applicable Federal program regulations (e.g. Medicaid, TANF, Food Stamps, Child Support, WIC, Section 508, etc.).

16. Use of Component Services Technology (COM)

Vendors preparing proposals and/or presenting their products to DHSS should be aware that due to a state mandated firewall configuration, there have been significant hurdles to the successful implementation of past projects that make use of Microsoft's Component Services technology (variously referred to as COM, DCOM, COM+, and Enterprise Services in some venues). Some configurations of such technology may prove impossible to implement under the strictures placed by the state authority. Whenever possible, vendors are strongly encouraged to avoid the proposal of use of such technology and instead rely on more modern alternatives like XML Web Services. If a vendor must propose such a technology, the proposal must include a detailed description of why Component Services is required, what impact their use may have on the state firewall configuration (including what ports must be open between various network zones) and how project timelines will be kept up if difficulties are encountered. Vendors should note in particular that port 135 cannot, under any circumstances, be opened between network zones. Utilities do exist to "convert" Component Services objects into XML Web Services but vendors should be aware that DHSS has no experience with such tools and therefore cannot vouch for their abilities. If such a tool is proposed, vendors should address its use in their proposals and account for how the results will be validated.

Related to the use of Component Services are ASP applications (the prior version of ASP.NET). Due to the fact that ASP applications often rely heavily on Component Services, vendors proposing that technology should be aware of these issues as well. Again, whenever possible, vendors are strongly encouraged to make use of more modern alternatives like ASP.NET which is commonly used as DHSS.

As with all technologies not standard at DHSS, the proposed use of Component Services and/or ASP will result in an especially rigorous evaluation of the proposal

by DHSS and vendors must include as much detail as possible so that evaluators can make an informed decision as to the viability of the proposed solution at DHSS.

17. Use of Third-party Products

Proposals must include a detailed outline of all third-party products (not explicitly named as DHSS standards) that will be used during the project contract. This would include, but is not limited to, development languages/products, database platforms, operating systems, middleware, and design tools. The outline must include the product name, the manufacturer/publisher name, the version (when appropriate), and a detailed description of why this product is required for the project and, if a competing product is already standard at DHSS, why that product could not be used instead. Vendors must also detail what purchase requirements will be for DHSS for these products both during the project and ongoing. Products not named in the proposal may be disallowed for use during the project and vendors are encouraged to err on the side of too much detail when listing products being proposed.

Software Quality Acceptance

All proposals for application development and enhancements will be reviewed by the DHSS Division of Management Services (DMS) Information Resource Management (IRM) team comprised of the IRM Applications Manager, Manager of Telecommunications, IRM Security Manager and Manager of Base Technology. DMS IRM will consult with the Biggs DTI Data Center Manager as appropriate. All development of and enhancements to DHSS applications will be measured against IRM Data Center Standards. Final acceptance will be based upon the software meeting the requirements set forth in the standards and will be at the discretion of the IRM Applications Manager. All consultants and/or contract programmers will adhere to data center policies and procedures as follows:

1. All work will be processed through the IRM Applications Manager and an IRM Project Leader using the Helpdesk System and Project Control Procedures for Maintenance request and enhancements. It will be the responsibility of the agency Project Manager to communicate all pertinent information such as; meeting dates, documents, progress reports, problem reports, etc. to the IRM Applications Manager. The IRM Project Leader will be formally responsible for working with the contractual team and will review and approve all deliverables.
2. During the analysis phase, appropriate staff will review and sign-off on storage requirements and projections, scheduling requirements, database and data integrity considerations, and disaster recovery.
3. At an agreed upon time, the contractor will present to IRM data models, critical transaction flows, evaluation and consideration of impact on other data center applications, and screen prototypes. The purpose of this review is to identify areas, which do not meet the DHSS standards and require modification. This should be scheduled so it does not impede the progress of the project.
4. All development and/or enhancements will be fully tested to include stress testing and modeling of transactions to include CPU, Response Time and Storage profiles, documented, accepted and signed-off by the requesting user, DTI and IRM. Program code, documentation

and/or JCL which does not meet standards for acceptance will be returned to the contractor with a statement of deficiencies.

5. IRM staff will be assigned to the project, with the primary purpose of ensuring a smooth transfer of responsibilities after completion of the contractor's work. In addition, the IRM Project Leader is responsible for quality assurance. All analysis, programming and testing performed by the contractor will be worked through the IRM Project Leader. The IRM Project Leader, Divisional Project Lead and the contractor can mutually agree upon assigning work to the IRM staff. It will be the contractor's responsibility to complete all required checklists and documentation before completion and sign-off of the project work.

Additional IRM Data Center Standards are available from the IRM Application Managers.

ATTACHMENT 1



DELAWARE HEALTH AND SOCIAL SERVICES

POLICY MEMORANDUM NUMBER 46 (Replaces 5/27/87)

REVISED 3/11/05

SUBJECT: STANDARDIZED REPORTING AND INVESTIGATION OF SUSPECTED ABUSE, NEGLECT, MISTREATMENT, FINANCIAL EXPLOITATION AND SIGNIFICANT INJURY OF RESIDENTS/CLIENTS RECEIVING SERVICES IN RESIDENTIAL FACILITIES OPERATED BY OR FOR DHSS

I. PURPOSE

- a. To protect the right of residents/clients of Delaware Health and Social Services (DHSS) facilities to be free from abuse, neglect, mistreatment, financial exploitation or significant injury.
- b. To require that each Division that has, or contracts for the operation of, residential facilities establish standardized written procedures for the reporting, investigation and follow-up of all incidents involving suspected resident/client abuse, neglect, mistreatment, financial exploitation, or significant injury.
- c. To require that all DHSS residential facilities comply with The Patient Abuse Law (Title 16, Chapter 11, section 1131, et seq.) and Title 29, Chapter 79, sections 7970 and 7971 (Attachments I and II); and that all Medicaid- and/or Medicare-certified long-term care facilities and Intermediate Care Facilities for Mental Retardation (ICF/MR) comply with the federal regulations (42 CFR) and State Operations Manual for such facilities.
- d. To require that all DHSS residential facilities comply with all applicable state and federal statutes, rules and regulations pertaining to suspected abuse, neglect, mistreatment, financial exploitation, or significant injury.

II. SCOPE

- a. This policy applies to anyone receiving services in any residential facility operated by or for any DHSS Division, excluding any facilities/programs in which the only DHSS contract is with the DHSS Division of Social Services

Medicaid Program.

- b. This policy is not intended to replace additional obligations under federal and/or state laws, rules and regulations.

III. DEFINITIONS

- a. Abuse shall mean:
 - 1. Physical abuse - the unnecessary infliction of pain or injury to a resident or client. This includes, but is not limited to, hitting, kicking, pinching, slapping, pulling hair or any sexual molestation. When any act constituting physical abuse has been proven, the infliction of pain shall be assumed.
 - 2. Emotional abuse – This includes, but is not limited to, ridiculing or demeaning a resident or client, cursing or making derogatory remarks towards a resident or client, or threatening to inflict physical or emotional harm to a resident or client.
- b. Neglect shall mean:
 - 1. Lack of attention to the physical needs of the resident or client including, but not limited to, toileting, bathing, meals, and safety.
 - 2. Failure to report client or resident health problems or changes in health problems or changes in health condition to an immediate supervisor or nurse.
 - 3. Failure to carry out a prescribed treatment plan for a resident or client.
 - 4. A knowing failure to provide adequate staffing (where required) which results in a medical emergency to any patient or resident where there has been documented history of at least 2 prior cited instances of such inadequate staffing within the past 2 years in violation of minimum maintenance of staffing levels as required by statute or regulations promulgated by the department, all so as to evidence a willful pattern of such neglect. (Reference 16 DE Code, §1161-1169)
- c. Mistreatment shall mean the inappropriate use of medications, isolation, or physical or chemical restraints on or of a resident or client.
- d. Financial exploitation shall mean the illegal or improper use or abuse of a client's or resident's resources or financial rights by another person, whether for profit or other advantage.
- e. Significant Injury is one which is life threatening or causes severe disfigurement or significant impairment of bodily organ(s) or functions which cannot be justified on the basis of medical diagnosis or through internal investigation.
- f. Residential Facility shall include any facility operated by or for DHSS which provides supervised residential services, including Long Term Care licensed facilities, group homes, foster homes, and community living arrangements.
- g. Long-Term Care Facility is any facility operated by or for DHSS which provides long-term care residential services and the Delaware Psychiatric Center.
- h. High managerial agent is an officer of a facility or any other agent in a position of comparable authority with respect to the formulation of the policy of the facility or the supervision in a managerial capacity of subordinate employees.

IV. RESPONSIBILITIES

- a. The Director, or his/her designee of each Division within the scope of this policy, is hereby designated as an official DHSS designee under the State Mandatory Patient Abuse Reporting Law.
- b. Each Division will develop written procedures consistent with the standards contained in this policy and which will be activated immediately upon discovery of any suspected abuse, neglect, mistreatment, financial exploitation or significant injury of or to a client of a residential or long-term care facility. These procedures must clearly outline the reporting chain from the witness to the Division Director, and other appropriate parties, to require the expedient relay of information within the required time frames.
- c. These standardized procedures shall also apply when the preliminary inquiry suggests that the significant injury, suspected abuse, neglect, mistreatment or financial exploitation may have been caused by a staff member of the residential facility, whether on or off the grounds of the residential facility. Suspicion of facility/program negligence (including inadequate supervision resulting in client-client altercations) and incidents involving abuse by persons who are not staff members of the residential facility shall also be reported.
- d. The standardized procedures shall be approved by the appropriate Division Director prior to implementation. The Division Director or designee shall forward a copy of the approved procedures to the Chief Policy Advisor, Office of the Secretary, and other appropriate agencies.
- e. Each Division will require that the standards established in this policy are incorporated in all residential operational procedures and all residential contracts. Each Division shall require that all residents and providers of these programs be informed of their specific rights and responsibilities as defined in the Division's written procedures.
- f. Each Division shall require that all levels of management understand their responsibilities and obligations for taking and documenting appropriate corrective action.
- g. Each Division shall require appropriate training of all staff and contract providers in the PM 46 policy and procedures. Such training shall also include the laws prohibiting intimidation of witnesses and victims (11 Del. C., sections 3532 through 3534) and tampering with a witness or physical evidence (11 Del. C., sections 1261 through 1263 and section 1269).
- h. Each Division shall develop quality assurance/improvement mechanisms to monitor and oversee the implementation of the PM 46 policy and procedures.
- i. Each Division must ensure that all employees of, or contractors for, residential facilities shall fully cooperate with PM 46 investigations.

V. STANDARDS/PROCEDURES

Standard and consistent implementation of this Department policy is required. Each Division's written procedures shall include the following:

- a. Employee(s) of the residential facility, or anyone who provides services to residents/clients of the facility, who have reasonable cause to believe that a resident/client has been abused, mistreated, neglected, subjected to financial exploitation, or has received a significant injury shall:
 1. Take actions to assure that the residents/client(s) will receive all necessary medical attention immediately.
 2. Take actions to protect the residents/client(s) from further harm.
 3. Report immediately to the Division of Long Term Care Residents Protection (if the incident occurred in a long-term care facility or if the client was a resident of a long-term care facility); and to the Department of Services for Children, Youth and Their Families/Division of Family Services (if the client is a minor, as required under 16 Del. C., section 903). It is essential that the reporting person ensure that the report be made to the appropriate division designee immediately.
 4. Report immediately to the facility/program director and the Division's designated recipient(s) of PM 46 reports.

5. Follow up the verbal report with a written initial incident report to the persons/agencies named in (a) 3 and (a) 4 (above) within 48 hours.
- b. In addition to the above named persons, any other person may make a report to a staff person of the facility or to the Division director or his/her designee. Such a report shall trigger activities under V(a), items 1 through 5.
- c. Each written initial report of suspected abuse, neglect, mistreatment, financial exploitation, or significant injury (completed by the reporting employee) must include:
 1. The name and gender of the resident or client.
 2. The age of the resident or client, if known.
 3. Name and address of the reporter and where the reporter can be contacted.
 4. Any information relative to the nature and extent of the abuse, neglect, mistreatment, financial exploitation or significant injury.
 5. The circumstances under which the reporter became aware of the abuse, neglect, mistreatment, financial exploitation or significant injury.
 6. The action taken, if any, to treat or otherwise assist the resident or client.
 7. Any other information that the reporter believes to be relevant in establishing the cause of such abuse, neglect, mistreatment, financial exploitation or significant injury.
 8. A statement relative to the reporter's opinion of the perceived cause of the abuse, neglect, mistreatment, financial exploitation or significant injury (whether a staff member or facility program negligence).
- d. The Division's designated recipient of PM 46 reports shall report all allegations of abuse, neglect, mistreatment, financial exploitation and significant injury, to the Office of the Secretary; the Office of the Attorney General/Medicaid Fraud Control Unit (for Medicaid- and/or Medicare-certified long-term care facilities); the appropriate state licensing agency for the program, if applicable; and the Division Director or designee, within 24 hours of receiving notification of such.
- e. In instances where there is immediate danger to the health or safety of a resident/client from further abuse, mistreatment or neglect; if criminal action is suspected; or if a resident/client has

died because of suspected abuse, mistreatment, neglect or significant injury, the Division Director or his/her designee shall immediately notify the appropriate police agency. The Division of Long Term Care Residents Protection, and the Office of the Secretary, shall be notified if the police were contacted. Further, the Division Director or his/her designee shall notify the Office of the Attorney General/Medicaid Fraud Control Unit, the Office of the Secretary, and the Chief Medical Examiner, if a

resident/client has died because of suspected abuse, mistreatment, neglect, significant injury, or as a result of any cause identified by 29 Del. C., section 4706.

- f. The Division Director or his/her designee shall review the initial incident report and initiate an investigation into the allegations contained in the report. The investigation, with a written report, shall be made within 24 hours, if the Division has reasonable cause to believe that the resident's/client's health or safety is in immediate danger from further abuse, neglect or mistreatment. Otherwise, the investigation and written Investigative Report, up to and including the Division Director's or designee's signed review of the report, shall be made to the Division of Long Term Care Residents Protection (DLTCRP) within 10 days. This timeframe may be extended by DLTCRP if extenuating facts warrant a longer time to complete the investigation. If the facility is a Medicaid-Medicare certified long-term care facility, or an ICF/MR facility, the report of suspected abuse, neglect, mistreatment, financial exploitation or significant injury shall be sent to the appropriate authorities, as required in the respective regulations under 42 CFR, within 5 working days of the incident.
- g. The investigative process shall be confidential and not subject to disclosure both pursuant to 24 Del. C., section 1768 and because it is privileged under the governmental privilege for investigative files. Each Investigative Report shall be labeled as confidential and privileged, pursuant to 24 Del. C., section 1768. Each investigation shall include the following:
 - 1. A visit to the facility or other site of incident.
 - 2. A private interview with the resident or client allegedly abused, neglected, mistreated, whose finances were exploited or whose injury was significant.
 - 3. Interviews with witnesses and other appropriate individuals.
 - 4. A determination of the nature, extent and cause of injuries, or in the case of exploited finances, the nature and value of the property.
 - 5. The identity of the person or persons responsible.
 - 6. All other pertinent facts.
 - 7. An evaluation of the potential risk of any physical or emotional injury to any other resident or client of that facility, if appropriate.
- h. A written report (Investigative Report) containing the information identified in V (g) shall be completed within the time frames identified in V (f) and shall include a summary of the facts resulting from the investigation. (Attachment 3)
- i. The Investigative Report shall be sent to the facility director and to the Division Director or designee. The Facility Director and the Division Director or designee shall review the report. If the incident is serious, the Division Director must review the incident with the Department Secretary prior to the completion of the report. The Facility Director and the Division Director or designee shall indicate in writing their concurrence or non-concurrence with the report. If the facts show that there is a reasonable cause to believe that a resident/client has died as a result of the abuse, neglect, mistreatment, or significant injury, the Division Director or designee shall immediately report the matter to the Office of the Attorney

General/Medicaid Fraud Control Unit, the Division of Long Term Care Residents Protection, and the Office of the Secretary.

- j. All Investigative Reports shall be forwarded by the reporting division, forthwith, to the Division of Long Term Care Residents Protection. The Division of Long Term Care Residents Protection shall complete the investigation by making a determination of findings and documenting their conclusions.
- k. If a determination is made at the Division level (upon consultation with the Division of Management Services, Human Resources office) that discipline is appropriate, the Investigative Report shall be forwarded to the Human Resources office. Human Resources shall determine the appropriate level of discipline, forward their recommendations to the Office of the Secretary and to the originating division for implementation, and proceed as appropriate.
- l. The Office of the Secretary shall be informed by the Division of Long Term Care Residents Protection, in writing, of the results of the investigation, including the findings and recommendations, within 5 days following the completion of the investigation.
- m. The Division Director or designee shall notify the appropriate licensing or registration board, if the incident involved a licensed or registered professional, and the appropriate state or federal agency, including the appropriate state licensing agency of the program, if applicable, upon a finding of: 1) abuse, mistreatment, neglect, financial exploitation, or significant injury; 2) failure to report such instances by a licensed or registered professional; or 3) failure by a member of a board of directors or high managerial agent to promptly take corrective action.
- n. The Division Director or designee shall notify the employee, resident/client, the guardian of the resident/client, if applicable, and the incident reporter of the results of the facility-based case resolution, unless otherwise prohibited by law. They shall also advise the parties of the fact that there is a further level of review that will occur through the Division of Long Term Care Residents Protection and/or the Office of the Attorney General/Medicaid Fraud Control Unit.
- o. The Division of Long Term Care Residents Protection shall, at the conclusion of their review of the case, notify the DHSS employee (or the agency director for contract providers), the resident/client, or the guardian of the resident/client, if applicable, and the originating Division Director or designee, of the substantiated or unsubstantiated status of the case, unless otherwise prohibited by law. The

Division of Long Term Care Residents Protection shall also notify the Office of the Attorney General/Medicaid Fraud Control Unit of all substantiated cases.

VI. IMPLEMENTATION

- a. This policy shall be effective immediately (upon the completion of mandatory departmental training).
- b. In carrying out this policy, all parties must protect the confidentiality of records and persons involved in the case, and may not disclose any Investigative Report except in accordance with this policy.

VII EXHIBITS

- a. Attachment 1 – Delaware Code, Title 16, Chapter 11, Sections 1131-1140.
- b. Attachment 2 – Delaware Code, Title 29, Chapter 79, Sections 7970-7971.
- c. Attachment 3 – Investigative Report form

Vincent P. Meconi

Vincent P. Meconi
Secretary