



Perry Johnson & Associates, Inc.,  
Technical Responses  
RFP 170007304 Transcription Services

## Executive Summary

Perry Johnson & Associates, Inc. is a privately owned and operated U.S. company delivering business value through services in medical transcription, billing & coding, transcription platform services, Teleradiology, and EMR. PJ&A provide each client with quality services based on a combination of domain expertise relevant technologies, and a reliable service delivery model. PJ&A helps clients increase their satisfaction levels through effective utilization of transcription expertise and superior customer service, as well as IT and customer support 24/7, 365 days a year.

As of 2015, PJ&A is the largest privately held Medical Transcription Company within the United States. The PJ&A portfolio of clients includes some of the following groups: Dartmouth-Hitchcock Medical Center, Henry Ford Health, Northwell Health New York, PSY, Inc., The Medical Centers in Kentucky, Humana/Concentra, and North Kansas City Hospital, just to name a few. Each of these systems encompasses a multitude of healthcare providers and facilities. PJ&A prides itself on ensuring that quantity never affects quality, no matter the size of the client.

PJ&A's management team has over 30 years' experience handling the implementation, go-live, and post-live day-to-day operations of clients of all sizes. Through proven implementation strategies and project analysis and planning, a seamless transition is the only acceptable outcome for each new client. Each implementation is handled by a multi-faceted approach that begins with the PJ&A project management team performing a thorough on-site evaluation of the facility to determine the exact scope of the project.

PJ&A has the capabilities both in technology and staffing to meet the requirements of this RFP. PJ&A developed a dictation and transcription group of software applications that were developed to solve many of the problems physicians and hospital staff encounter on a day-to-day basis. Easy to use dictation lines that are customizable down to the voice recording make the task of dictation much simpler for the physicians. This is imperative as this is most often the physicians' first experience with the PJ&A system and first impressions are everything.

The document management system GEMS efficiently stores all dictation audio and transcribed reports in a secured, searchable database. Within GEMS, users are able to listen to dictation audio, edit reports, view usage statistics, eSign reports, print, fax, send messages to the PJ&A Quality and Transcription teams, mark jobs as STAT, monitor job status and progress, along with many other included options to help productivity and improve efficiencies and speed of care for patients.

PJ&A's Transcription, Quality, and IT teams all have the experience and expertise in their respective field to provide the utmost confidence to both the Lead State and Participating States.

The PJ&A Transcription team is staffed by transcriptionists who have a minimum of 5 years' experience in medical transcription. Through this experience comes the knowledge of a multitude of areas of medical terminology. PJ&A only hires the best of the best, and each transcriptionist is required to go through a vigorous hiring process that includes multiple interviews, a skills verification exam and background check.

PJ&A's Quality and IT teams are fully available 24 hours, 7 days a week, including all holidays. No matter the scale of the issue or question, there will always be someone available to help. All staff are located within the U.S. and are made familiar with any new accounts that begin service. This allows a timely response without further delaying patient care or physician time.

## Section 4: Administrative and Technical Response Requirements

### 4.1 Mandatory Minimum Administrative Proposal Requirements

Perry Johnson & Associates, Inc., has been providing dictation and transcription services for over 30 years. In this span, PJ&A has accrued a client portfolio ranging from hospitals and healthcare systems, to law offices and court reporting, along with general transcription services such as typing out the minutes from publicly held meetings.

Over the years, PJ&A has built a client base that not only stretches into all fifty states (including multiple Alaskan clients), but also to the United Kingdom and Guam. Having such a strong network of clients has provided for an extensive history and background in numerous facets of the transcription industry, and provided a rich and full background.

As a major part of PJ&A's transcription business, medical transcriptionists are well versed in the numerous areas this discipline requires such as behavior health, pathology, radiology, ambulatory, sleep studies, vascular, among many others.

For this RFP, the primary point of contact will be Jeffrey Hubbard, who is the President and CEO of PJ&A.

Jeffrey Hubbard began his career with Perry Johnson & Associates, Inc. in 2006. As the president, Mr. Hubbard oversees all employees and is responsible for all day-to-day Global Operations and Departments. Mr. Hubbard brings over 17 years of upper-management experience to PJ&A and its clients. Jeffrey earned his master's degree in Financial Management along with a B.A.A. in Business, and Marketing.

Jeffrey Hubbard  
(800) 803-6330  
[jhubbard@pjats.com](mailto:jhubbard@pjats.com)  
Fax: (248) 247-3460  
755 W. Big Beaver Rd STE 1300  
Troy, MI 48084

As previously mentioned, PJ&A has clients across numerous time zones, with many requiring service 24 hours a day, 7 days a week. It's for this reason, PJ&A will have around the services, transcription and customer/IT support without any downtime. PJ&A support will be available via email and phone, with emailed responses coming within 20 minutes of initial email receipt.

As PJ&A already has numerous clients located within the state of Alaska, a copy of PJ&A's valid business license has been included with this proposal.

### 4.2 NASPO ValuePoint Master Agreement Statement of Compliance

Please accept this as PJ&A's statement of acceptance to all terms and conditions found within the Master Agreement of this RFP (Attachment A).

#### 4.2.1 Insurance

All requirement insurance has been included in this RFP response. Please see the attached proof of insurance for all details of the PJ&A policy that meet the minimum requirement guidelines set forth; Commercial general liability covering premises operations, independent Contractor's, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than \$1 million per occurrence/\$2 million general aggregate.

#### 4.2.2 NASPO ValuePoint Administrative Fee and Reporting Requirements

PJ&A has factored in all necessary fees and expenses into the final proposed cost for this project. This includes the administrative fee of .25%.

PJ&A also agrees to provide to the Lead State and NASPO the required sales reports, on the required timeframes, with the required information. Although this RFP is providing a service and not a product, which may not necessarily be relevant, if and when the instance does become necessary both at the reporting periods and the quarterly marks.

Executive summaries will also be provided to the designated coordinator quarterly.

#### 4.2.3 NASPO ValuePoint eMarket Center

PJ&A agrees to make services offered available through this channel.

#### 4.3 Lead State Terms and Conditions

PJ&A has read through the terms and conditions set forth by the Lead State, in this case Alaska, and fully agrees to adhere and follow all requirements without issue.

#### 4.4 Participating State Terms and Conditions

PJ&A fully understands that under the scope of this project, multiple state entities will be involved. For this reason, special circumstances may arise that require additional terms and conditions to be set through a negotiation and compromise period. PJ&A is willing to make concessions to adhere to these special terms and conditions if deemed necessary to meet the original scope of work laid out in this proposal.

#### 4.5 Technical Requirements

Please refer to section 4.5.1 for the precise technical specifications PJ&A will be utilizing for this proposal.

##### 4.5.1 Experience and Capabilities

Perry Johnson & Associates, Inc. is a privately owned and operated U.S. company that has global healthcare operations, delivering business value through services in medical transcription, billing & coding, transcription platform services, e-signature, Teleradiology, and EMR. PJ&A strives to provide each client with industry-leading quality standards based on a combination of domain expertise relevant technologies, and a reliable service delivery model. PJ&A provides the service and tools to each and every client to increase their satisfaction levels through effective utilization of transcription expertise and superior customer service, as well as IT and customer support 24 hours a day, 7 days a week.

As of 2015, PJ&A is currently the largest privately held Medical Transcription Company within the United States. The PJ&A portfolio of clients includes some of the following groups: Dartmouth-Hitchcock Medical Center, Henry Ford Health, Ernest Health, North Shore-LIJ Health System, PSY, Inc., The Medical Centers in Kentucky, Humana/ Concentra, Cook County Illinois, Sitka Hospital and North Kansas City Hospital, just to name a few. Each of these systems encompasses a multitude of healthcare providers and facilities. PJ&A employees pride themselves on ensuring that quantity never affects quality, no matter the size of the client.

PJ&A's management team has over 50 years' experience handling the implementation, go-live, and post-live day-to-day operations of clients of all sizes. Through proven implementation strategies and project analysis and planning, a seamless transition is the only acceptable outcome. Each implementation is handled by a multi-faceted approach that includes an experienced project management team starting with a thorough on-site evaluations of each client facility to determine the exact scope of the project.

#### Offeror Profile

- a. Perry Johnson & Associates, Inc.
- b. 755 W. Big Beaver Rd STE 1300 Troy, MI 48084 (Corporate Office)
- c. PJ&A is a privately owned, zero debt, C-Corporation with a headquarters in Henderson, Nevada.
- d. Key personnel are listed below:

##### **Jeffrey R. Hubbard, President/CEO:**

Jeffrey Hubbard began his career with Perry Johnson & Associates, Inc. in 2006. As the president, Mr. Hubbard oversees 10,860 employees and is responsible for all day to day Global Operations and Departments. Mr. Hubbard brings over 15 years of upper-management experience to PJ&A and its clients. Jeffrey earned his masters degree in Financial Management along with a B.A.A. in Business, and Marketing.

##### **James Nowak, Director of IT and CS Development:**

With over 20 years of progressive information systems responsibilities, starting at entry level and advancing to senior systems analyst, Jim Nowak started with PJ&A in October of 2006. Jim possesses expertise in information systems technologies including, but not limited to: server builds, computer automation, application support, customer support, internet/intranet technology, documentation, disaster recovery, HIPAA compliancy, network security and topology.

##### **David Campbell, Vice President of Technology & Development:**

David has worked with Perry Johnson & Associates, Inc. since February 2005. He specializes in HL7 Interfaces, Imaging Systems, Chart Completion Systems, and Lotus Notes. His Programming Languages Include C, C++, Perl, and Java. He has worked in the health field for the 16 years and has worked with thousands of customers.

##### **Nadya Zolotaya, CFO:**

Nadya has been with Perry Johnson & Associates, Inc. since January, 1996. She is the companies CFO and works directly with Mr. Hubbard.

**Sunil Kumar, Director of Medical Transcription:**

Sunil has been with Perry Johnson & Associates, Inc. since February 2004. He has also worked as a director in this field for the past 18 years with two of our direct competitors. Mr. Kumar reports directly to the company President and works with all members of the Perry Johnson & Associates, Inc team.

**Scott Meesseman, Director of IT and CS Development:**

Scott has worked with Perry Johnson & Associates since January 2013. He has been in the IT field for the past 21 years. He has a vast knowledge of all current health systems and information systems and is the lead developer on many PJ&A projects including the mobile dictation app Crystal and the front-end speech application Jewel.

**Ryan Dungs, Senior Network Engineer:**

Ryan has been an employee with Perry Johnson & Associates, Inc. since earning his degree from Lawrence Technical Institute in 2008. His responsibilities include implementing network security, network/internet routing engineering, deployment of VOIP systems. In addition, Ryan also manages PJ&A's help desk ticketing system and processes.

**Scott Bogart, Network Engineer:**

Scott has earned a Bachelor's of Information Technologies and Securities Degree from Baker College. For the last 2.5 years, Scott has been responsible for system and network administration which includes maintaining server infrastructure, Active Directory, Exchange, and Database administration, patch management, system backups, as well as top level technical support.

**Brett Robertson, CS and IT Account Manger:**

Eric has worked with Perry Johnson & Associates, Inc. since March 2010. He specializes in system troubleshooting and is a valuable asset to CS and IT Account Management due to his skills and abilities and past experience as a medical transcriptionist.

**Bryan Newby, CS/IT Support Staff:**

Bryan has earned a Bachelor of Science from Central Michigan University with a major in Information Technology and a minor in Media Design, Production and Technology. Bryan supports 100+ clients remotely with technical support, user training, and customer setup. Joining Perry Johnson & Associates, Inc. in 2016, he is also responsible for monitoring, maintaining and installing PC desktops, laptops, printers, scanners and servers. He configures hardware and software of new systems and upgrade existing systems as needed for security and stability. This includes the daily monitoring and configuration of our dictation servers and applications. Some of Tim's top qualities include customer service, technical support, inventory control, security policies/procedures, documentation and network administration.

**Vitaliy Kucherenko, CS/IT Support Staff:**

For the last 5 years, Vitaliy has been responsible for system administration which includes maintaining server infrastructure, coordinating customer setup, top level technical support, after hours' customer service and technical support.

**Katheryn Somers, Corporate Customer Support Manager:**

In March of 20010 Katheryn joined the team at Perry Johnson & Associates, Inc. A graduate of Wayne State University with a bachelor's degree in business, Katheryn deals directly with the customers' staff during the facilities on-site set up as well as working at our headquarters and managing the customer service team.

**Teeya Brow, CS Support Staff:**

Teeya is entering her third year of being a part of the team at Perry Johnson & Associates, Inc., and is a critical member whose attention to detail and communication skills help to ensure the clients satisfaction. Teeya works at our Troy, MI corporate office.

**Joy Vanbuskirk, CS Support Staff:**

A former home medical coder and transcriptionist with multiple degrees from Grand Valley State University, Joy started at PJ&A in February of 2016. Joy assists across all clients with the day-to-day operations and troubleshooting should any issues arise.

**Rachel Rottman, Accounts Payable:**

Rachel has been with Perry Johnson & Associates, Inc. since January, 2004. She is responsible for all Accounts Payable entry and reimbursement and vendor reconciliation.

**William Robinson, Accounts Receivable/Billing:**

William has been a diligent force with the Accounting Department for the past 15 years. He excels at his daily duties of banking, billing and collections for Perry Johnson & Associates.

**Jason Millbrand, Corporate Marketing Materials Manager:**

In May of 2005 Jason joined Perry Johnson & Associates, Inc. Having a strong background as well as certification in corporate marketing and computer design, Jason is responsible for keeping our staff and clients up to date with the services PJ & A has to offer and creating the marketing and training materials for our sales team and for our new clients.

- e. PJ&A currently employs 1,100 employees across the United States.
- f. [www.pjats.com](http://www.pjats.com)
- g. For all additional sales, Jeffrey Hubbard will be the main point of contract for this agreement.
- h. PJ&A has a 100% client retention rate over the last 3 years.
- i. PJ&A was founded in 1982, performing services in medical transcription.
- j. PJ&A has seen record growth not only the last 3 years, but the past 5 years, with figures of around 40% uptick in sales annually.



- k. PJ&A is able to service all states specified in this contract. Already providing transcription services to clients in all fifty states, PJ&A will be able to step in as-needed, outside of the Lead State.

#### Customer Service

- a. PJ&A services and customer/IT support are available 24 hours a day, 7 days a week at no additional charge to the client. Key personnel are available during regular business hours, with exceptions made for critical issues related to the success of the project.
- b. If at any time an issue presents itself, PJ&A will ensure the appropriate team member is alerted. The project management for the project will then assign the appropriate resources to ensure timely resolution of the issue. If the problem cannot be remedied within an hour, progress will be tracked and reported to all applicable contacts on the client side until resolution is achieved. This will be achieved through both email and phone calls. Upon final resolution, the issue will then be written up as a case study to be stored on file by PJ&A to prevent the issue from happening again.
- c. PJ&A has a workforce that is fully capable of handling both the Lead State and any additional Participating States that may arise through the life of this contract. Team leads will be assigned to each Participating State, with open lines of communication established between these teams to promote efficiency and best practices. Although each Participating State may have differing terms and conditions, it is the belief of PJ&A that a unified approach be taken with all to create standards and practices.

Teams will meet regularly to discuss common correspondences and how each handles them, and which methods were most effective. This will include the various types of transcription needs received. Cross-organization trainings and meetings will be held regularly to ensure all PJ&A teams are on the same page and have a general understanding of each Participating States account.

Teams will all be required to have a firm understanding of the Lead States terms and conditions, along with the scope of work required within the Master Agreement. The PJ&A project manager will be the responsible party to coordinate this communication.

- d. Once transcription errors are notified to PJ &A, a detailed correction analysis is conducted by QA personnel by going through the complete voice file. Following the analysis, a one-on-one session is held with the MT and editor through whom the errors had passed and explanation is sought for the error as well as constructive feedback provided in order to avoid recurrence of errors. The team working on the account will then be briefed about the identified errors so they will not make the same mistakes. Regular random auditing is conducted on the erroneous editor/MT that has direct upload privilege in order to keep a check on the quality of the jobs being delivered to the client.

PJ&A will provide a 98% accuracy rate with a 3% credit on the work at hand that falls below 98%. This will only be provided if the accuracy is affected due to PJ&A MT errors. Errors due to health system related issues or poor audio quality do not qualify for credit.

PJ&A will monitor and enforce the specific policies, and rules set by the Lead and Participating States. PJ&A will request this information prior to the Go-Live and PJ&A will train its team members and management on every issue. PJ&A will also hold weekly meetings with the transcriptionists to make sure all polices, rules and procedures are being followed to the agreed upon guidelines.

PJ&A will continue weekly meetings until the project is up and running at 100%. The meetings will be moved to a bi-weekly schedule for the duration of the agreement. If the Lead State does not provide PJ&A with such information the PJ&A team will utilize its standard policies, rules and procedures for the duration of the agreement. The scheduled meeting guide will also stay in effect.

**Issue Tracking:**

Anyone on the project team can raise an issue by contacting the project manager. The process is as follows:

- The project manager and the client contact discuss the issue and decide whether the issue will be tracked. The project manager adds the issue to the issue spreadsheet with a state of Open.
- The project manager works with PJ&A, Inc. and the Lead State resources to identify a course of action and responsible resources for the issue. The project manager adds the action items and other information to the issue spreadsheet and changes the state to In Progress.
- The project manager includes the open issues in the regular status report.
- When the assigned resources notify the project manager that the issue is resolved, the project manager changes the state to Closed.

ID	Status	Issue Description	Status/Last Action/Next Action	Assigned To	ID Date	Target Completion Date
1	Open					
2						
3						
4						
5						
6						
7						

- e. Customer satisfaction is determined through multiple steps. The first is through the accuracy and TAT scores on transcribed reports. This measuring tool is the easiest way to gauge tertiary customer satisfaction. Accurate, on-time reports are the primary goal of this project.

The second gauge are through monthly phone calls between the PJ&A project manager and key personnel at the Lead State. These phone calls are utilized to focus specifically on how PJ&A is handling workflow and to check on the satisfaction with reports and the PJ&A system.

Takeaways from these monthly phone calls will then be addressed with the team and improvements to processes will be implemented to ensure any shortcomings are immediately addressed.

- f. Please see the attached document labeled PJ&A Quality Policy.
- g. This question will be addressed to speak to unexpected increases in volumes from the Lead State, the Participating States, or both.

PJ&A currently has the capacity to handle an additional 840,000,000 VBC of transcription volume per month. In addition, PJ&A currently has in place the hiring, training, quality assurance processes and technology infrastructure scalability processes, IT support and customer service established to increase capacity by 30%-35% within 30 business days.

## Technology

- a. PJ&A's platform utilizes the power of the Internet and the latest proven technologies to offer a scalable, fully integrated, comprehensive solution for dictation, transcription, document management. PJ&A's system allows authorized personnel including transcriptionists, physicians, HIM directors, quality assurance editors and clinicians access needed transcripts and patient information remotely from the browser (Internet Explorer 7.0 or higher) or from a networked connection. All transactions are secured using approved data encryption methods and SSL (Secure Socket Layer) technology.

As this technology is scalable, PJ&A has the capabilities to setup and configure the system to accept dictations from an infinite number of sources, each that can be stored as its own entity, or a sub-domain of a parent enterprise. This will be determined after the award of the contract during scoping and evaluation.

The PJ&A model of service varies depending on the client's needs. PJ&A can provide a toll free voice dictation line for dictating directly onto our systems. A physician would dial into the dictation system and dictate. Additionally, PJ&A can accept digital voice files generated in another system or DVR and import these voice file into the PJ&A system. Physical copies such as USB drives, CDs, or cassette tapes can also be uploaded into the PJ&A platform for transcription. File formats of digital audio that are acceptable include .mp3, .WAV, .WMV, and .AVI.

PJ&A establish a VPN between our site and the client facility. Two or more interfaces are built to transfer ADT, voice files, completed transcriptions, HL7 feeds, etc.

Once the interfaces and VPN are established, PJ&A is able to feed the dictations and ADT information into our systems giving the medical transcriptionists access to start typing.

The documents are typed and submitted to quality review for proofing, editing and grading.

Once the completed documents go through a standard review process, the completed transcription is marked complete and the interface returns the transcription to the client site. PJ&A can either stream into an EMR via interface or a folder drop of the completed transcription can be performed.

#### PJ&A WEB-BASED PORTAL

Transcription reports can be accessed via the PJ&A web portal GEMS. The web portal gives the ability to access, view, modify, print or e-sign depending on the user rights assigned to the individual users.

#### SOFTWARE

- OPERATING SYSTEM
- Windows XP Pro with SP2
- INTERNET BROWSER
- Microsoft Internet Explorer 7.0+

#### INTERNET EXPLORER SETTINGS

- Advanced Tab – Disable script debugging (Internet Explorer) and (Other)
- General Tab – Temporary Internet Files – Settings – Check for new versions of stored pages: Every visit to the page
- PJ&A URL is required to be in the trusted sites
- Automatic prompting for ActiveX controls – Enable
- Binary and script behaviors – Enable
- Download signed ActiveX controls – Enable
- Download unsigned ActiveX controls – Prompt
- Initialize and script ActiveX controls not marked as safe – Prompt
- Run ActiveX controls and plug-ins – Enable
- Security Tab – Trusted Sites -
- Custom Level - Script ActiveX controls marked safe for scripting – Enabled

- b. Please see the above response.
- c. Please see the above response.

#### 4.5.2 Data Security & Confidentiality

- a. Please see the attached HIPAA Security Policies and Procedures document.
- b. Please see the attached HIPAA Security Incident Response Procedures document.

- c. Please see the attached HIPAA Security Policies and Procedures document.

#### 4.5.3 References

- a. Please see Attachment D.

#### 4.5.4 Scope of Work

- a. In this section, each item from the scope of work outlined in Attachment B will be addressed individually, or if deemed appropriate, address in conjunction with other items or items already addressed previous in this response document.

**\*\*\*Please refer to attached document labeled Attachment B Responses.**

#### 4.5.5 Marketing of the NASPO ValuePoint Master Agreement

- a. At this time, PJ&A does not anticipate any promotion of the Master Services agreement. However, it may be asked to be used in the future to further additional business developments through the experience garnered. If this occurs, PJ&A will work closely with the Lead State and NASPO to ensure all proper channels are addressed.
- b. If at any time PJ&A plans to leverage this contract in its marketing and sales strategy, PJ&A will take no action without first contacting the proper team at NASPO to determine the scale and scope of publicity that may be utilized. Only after there is approval and sign-off, will PJ&A then move forward with any marketing of this agreement.
- c. With the scope of work thoroughly laid out in this agreement, it will not be a problem to analyze and evaluate any requests that may come through as a result of this agreement, and determine if the request falls within the scope of the original RFP. This will be decision that will come down from multiple communications between PJ&A and the necessary entities from NASPO and the States involved.
- d. The due dates for fees and reporting will be handled by the project manager and the accounting team at PJ&A.
- e. PJ&A's Marketing team is fully capable of cooperation with NASPO and does not foresee any challenges in this arrangement. Strong lines of communication will be established to ensure items aren't left hanging. PJ&A will also require any team member to be knowledgeable and fluent in the requirements of NASPO's marketing and branding strategies.

## Authorized Signature Page

March 17, 2017

Perry Johnson & Associates, Inc.  
Primary Contact:  
Jeffrey R. Hubbard, President/CEO  
Office phone: (800) 803-6330  
Fax: (248) 247-3465  
755 W. Big Beaver Road, Suite 1300  
Troy, MI 48084  
jhubbard@pjats.com

To Whom It May Concern,

Perry Johnson & Associates (PJ&A) is pleased to submit our response for RFP 170007304.

Please accept this letter as well as my signature as a binding agreement for all statements and pricing quoted within this RFP response, Attachment B responses, along with all attachments included with this response.

Please contact us if you have any questions while reviewing our responses.

Regards,

A handwritten signature in black ink, appearing to read 'J. Hubbard', with a long horizontal flourish extending to the right.

Jeffrey R. Hubbard  
President, Perry Johnson & Associates, Inc.



Perry Johnson & Associates, Inc.  
Technical Responses to Attachment B  
RFP 170007304 Transcription Services

## A.1. General Transcription Services

1. PJ&A will provide transcription services as illustrated and detailed in the scope of work.
2. All required hardware and software is the sole responsibility of PJ&A and should the need for any additional to be provided, PJ&A will handle all costs and fees associated with meeting this requirement.
3. PJ&A has the capabilities to transcribe both audio and video files to a text document.
4. In accordance with the PJ&A Quality Policy, all transcribed documents will be reviewed by an editor before being returned to the Lead State or any Participating States. Please see the exact policies and procedures detailed in the attached PJ&A Quality Policy.
5. PJ&A complies with the requirement to establish a secured file transfer protocol, and would propose the use of the web-based audio and document management tool GEMS to fulfill this requirement. If this does not meet this requirement on its own, PJ&A will develop a process that satisfies this requirement to the exact specifications of the Lead State or Participating States.
6. The PJ&A solution contains the capabilities to handle both electronic transfer of audio and video files along with the capabilities to handle physical files as well. All costs associated with this will be taken on PJ&A and have been factored into the proposed cost included in the proposal for services.
7. Through PJ&A's web solution GEMS, authorized users will be able to review both the audio files and the transcribed documents. Permissions can be granted on a per user basis that allow users to listen, view, print, edit, fax and send messages to the PJ&A Transcription Team regarding additional corrections or edits required. These user permissions will be determined by the Lead State and Participating States, and each approved user will be given a unique username and password.

Any required corrections will be made and the updated report available within 12 hours of notification.

- a. PJ&A has internal benchmarks in place that require all documents be transcribed with a minimum of 98.7% accuracy. Failure to do so will result in the implementation of the quality improvement plan mentioned previously.
8. PJ&A will work with the Lead State and Participating States to determine the required turnaround times for each type of document needing to be transcribed. These turnaround times will then be the benchmark for all reports through the life of the contract, and will be included as part of the signed contract.



9. PJ&A maintains all audio and transcribed documents securely stored within GEMS for any amount of time, as determined by the Lead or Participating State. Individual requirements can be set for each. Within GEMS, audit trails are kept that log the following activities:
- o User(s) who accessed a report
  - o Timestamp of when they accessed the report
  - o Edits done to the document
  - o Versioning of documents so if changes were made in error, the previous document can be restored
  - o Playback of audio
- a. PJ&A maintains strict audit trails of all transcription files.
- b. All reports will be generate at the request of the Lead or Participating States and can be delivered at the express consent and requirement of either entity.
10. If at any point throughout the life of the contract, there are policy changes, legislative changes, or administrative rule changes, PJ&A will adapt and follow new policies to ensure they are compliant.
11. All PJ&A offices and data centers are focused on data security and implement industry standard protocols and measures to ensure the utmost confidence of each and every client. This includes badge entry on any and all areas that may contain sensitive data, security parameters on all computers that disables the use of external peripheral devices such as USB drives and plug and play CD/DVD burners. Along with office security, the security at each data center is also taken very serious.

#### **Peak 10 Data Centers**

Peak 10 owns and operates multiple world-class data centers supported by highly skilled technical personnel 24 hours a day, seven days a week. All Peak 10 data centers are engineered with multiple levels of security, uninterruptible power, redundant HVAC systems, fire suppression and around-the-clock monitoring and management.

#### **Security**

Each Peak 10 facility is engineered with a minimum of five levels of security:

- Level 1: Proximity card access with PIN is required to enter the building. You are not yet in the data center.
- Level 2: Proximity card access with Biometric (fingerprint) scan is required to enter the data center.
- Level 3: All hardware is secured in a locked cage or steel mesh cabinets fitted with combination locks.
- Level 4: Video surveillance cameras are placed throughout the facility.
- Level 5: Staffed 24x7x365.

#### **Uninterruptible Power**

Each Peak 10 data center is engineered with an uninterruptible power system and backup generator to deliver seamless power. In the event of a commercial power failure, our isolated UPS system will provide immediate backup power until our diesel generators take over the load and continue operation of the center.

### **Redundant HVAC**

Peak 10 utilizes best-in-class environmental units to control and monitor the temperature and humidity in each data center facility. Our redundant HVAC system keeps the average temperature in each data center at 70 degrees Fahrenheit to ensure a consistent operating atmosphere for your mission critical technology infrastructure.

### **Fire Suppression**

Peak 10 data centers utilize dry-fire suppression systems that can be deployed manually, or by a sequence of three failures anywhere in a data center zone. Each Peak 10 facility is also fully equipped with smoke and heat detection sensors as well as fire doors and handheld gas-based fire extinguishers.

### **Other Facility Facts**

- Custom-sized Private Cages, Single or Half Cabinets
- AC Power (20-100A 110-208V, Multi-Phase, Custom)
- 24x7 Customer Access with 24 hour staff and security
- Customer Work Stations with Phone and Internet Access
- All Peak 10 data centers are **SAS70 Type II certified**

In addition to Peak 10, we also host servers at two of our PJ&A office locations, Southfield, MI, and Grand Rapids, MI. The two locations in Michigan are secured data centers with HVAC and fire suppression systems and redundant internet connectivity across multiple carriers. In the case of a system crash, PJ&A has the capability to mitigate system wide outages by transferring work between our Peak 10 data center located in North Carolina, or our internal data centers located in Michigan.

12. PJ&A complies with this requirement.
13. PJ&A offers toll-free dictation lines that are available 24 hours a day, 7 days a week. Multiple numbers can be utilized to be facility specific, or a main line can be utilized, with users being prompted to enter a facility code after dialing the main line.
  - a. PJ&A also supports the use of hand-held DVRs, which the audio can be uploaded using software created by PJ&A developers called Emerald. This software application allows users to dock their device, and with the Emerald window open, the files will automatically download to the user's computer and then upload directly into GEMS to be transcribed.

Speechmikes, with or without barcode scanners, can also be utilized, and paired with PJ&A's software Diamond, allow users to quickly and easily pull patient information from the barcode and into the software application Diamond, which will then upload all information into GEMS.

PJ&A also offers users the use of a mobile dictation application that can be used on any iOS or Android device. The audio is captured on the device, encrypted, and then sent

over-the-air to GEMS through secured HTTPS connection either through cellular data or Wi-Fi.

All dictation options allow for the quick and easy marking of a dictation high priority through a simple prompt which will alert the PJ&A transcription team that the audio needs to be transcribed in an expedited manner.

- b. PJ&A also has the capability within its system to capture multiple dictators and have that audio combined into a single report.
- 14. PJ&A's solution includes all standard audio controls including fast forward, rewind, pause, editing, omit, replace, and insert audio.
- 15. PJ&A's solution can store both the audio and the document file for any discriminate amount of time, deemed necessary by the Lead State or the Participating State. These times are specific to the file type, and can be customized by the entity as well.
- 16. All PJ&A transcriptionists are U.S. based and operated and speak English as a first language. Therefore, proper speech, grammar, speech, and punctuation will not be an issue.
- 17. Please see the attached PJ&A Quality Policy for more information on this requirement.  
  
Once the specifications for reports and billing reports are established, PJ&A will have no problem matching these exactly.
- 18. PJ&A complies with this requirement.
- 19. Please see the attached documents labeled Security Policies and Procedures, and Security Incident Response Procedures for full, detailed plans of action following these requirements.
- 20. PJ&A complies with this requirement.
- 21. PJ&A will only utilize transcriptionists located within the U.S.

## A.2. Medical Transcription Services

- 22. PJ&A complies with this requirement.
- 23. PJ&A complies and can accommodate any formatting requirements.
- 24. PJ&A complies with this requirement.
- 25. PJ&A complies with this requirement.
- 26. PJ&A complies with this requirement.

27. PJ&A complies with this requirement.

28. All PJ&A transcriptionists have a minimum of 5 years' experience in the industry, and all are required to carry medical transcriptionist certification.

29. PJ&A complies with this requirement.

### A.3. Legal Transcription Services

30. PJ&A complies with this requirement.

### A.3. Optional Transcription Services

31. PJ&A complies with this requirement.



# QUALITY POLICY

Revised: March 01, 2017

## **INTRODUCTION and OVERVIEW:**

The Quality Policy set forth below is the standard reference document regarding quality in Perry Johnson & Associates, Inc. It is clearly understood that this policy may undergo changes from time to time in order to better meet customer needs.

PJ&A commits to its ultimate clients that it will provide transcribed files that achieve a score of 99% (for accuracy) on the standard set out by the American Association of Medical Transcription. To achieve this level of accuracy, PJ&A will review the transcribed work using a 6-point measure:

- Reports have all essential components and all required and relevant information.
- Reports are consistent both within themselves and externally, with the other parts of the patient record, should that be made available to PJ&A. Discrepancies are flagged for the dictator.
- Reports have the proper structure, format, content, spelling and grammar.
- Reports are transcribed to accurately reflect the meaning intended by the dictator, yet may be interpreted and edited by the transcriptionist in accordance with the particular client requirements.
- The patient's right to confidentiality is strictly guarded.
- Reports are timely in their completion and submission.

## **PROCEDURE:**

- Each transcriptionist and editor utilizes both American-English and Medical spellcheckers and dictionaries. Spell check is run on each file prior to saving it.
- Reports are verified by a format specialist to verify correct formatting.
- Transcribed files should follow the guidelines established in the AAMT Book of Style, unless the client specifies otherwise.
- Abbreviations should be spelled out where necessary in accordance with JCAHO guidelines.

## **ERROR CATEGORIES**

When beginning a new account, 100% of the work will be edited until grades reflect 99% or above for the first 2,000 lines. Edited files will be graded based on the following 5 broad error categories:

### **Major Errors = 1 point**

The following errors are considered Major errors:

Demographic error, Creative transcription/Inserted Text, Drug Error, Major Medical Errors, Major English Error, Comprehension Error, Wrong Template usage, and Spelling error.

**Demographic error:** Any error in the header or footer of the file (Patient name, MRN, Speaker Name etc.).

**Creative transcription/ Inserted Text:** This refers to fabricating or "making up" dictation (words and/or phrases) when what is dictated is not clear or varies significantly from what was dictated.

**Drug Error:** Wrong drug name keyed in.

**Major Medical Errors:** This refers to wrong medical word in the file which affects the patient's condition and hence is not acceptable.

i.e.:

Dictated: Anti-CCP level is positive.

Transcribed: NCCP level is positive.

In this example, this error is a medical major error as this will affect the patient care.

**Major English Errors:** This refers to wrong English words in the file which affects the patient care and hence is not acceptable.

i.e.:

Dictated: Dermoscopy showed discrete lesions.

Transcribed: Dermoscopy showed discreet lesions.

**Comprehension Errors:** This refers to errors caused due to lack of comprehension.

i.e.:

Dictated: Asteatotic dermatitis of lower legs.

Transcribed: As she had contact dermatitis of lower legs.

**Spelling Error:** This error category refers to the misspelling of any words, including both medical and English words. This category also includes the use of an incorrect form of a medical word, failure to use correct combining forms, and incorrect entries from the macro expander. Errors would include not capitalizing trade drugs, capitalizing generic drugs, improper capitalization in abbreviations.

**Wrong Template:** Using the wrong template or not using the updated template.

**Minor Error = 0.50 points**

**English Minor and Medical Minor**

**English Minor:** This refers to minor English errors in the file which is an error but will not affect the patient care and are precisely simple grammatical errors.

i.e.:

Dictated: It does rub against his shoulder pads at which time it hurts him more. It has not bled.

Transcribed: It is rubbing at the shoulder pads at which time it hurts him the more. It does not bled.

**Medical Minor:** This refers to minor medical errors in the file which is an error but will not affect the patient care.

i.e.:

Dictated: The patient has Behcet syndrome.

Transcribed: The patient has Behcet disease.

Omitted: Words dictated but not keyed.

i.e.:

Dictated: Side effects including bleeding, pain, infection, scarring, need for further treatment, written consent was obtained.

Transcribed: Side effects including bleeding, infection, scarring, need for further treatment, written consent was obtained.

**Typographical:** This refers to errors caused in keying in the word.

Dictated: being

Transcribed: bieng.

#### **Formatting Error --- 0.50 points**

This error category refers to certain information within the attribute page that the transcriptionist could have verified by using accessible references. This includes errors in the page setup, client specifications, and template instructions.

#### **Grammar Error -- 0.25 points**

This category identifies errors committed due to wrong usage or lack of basics of English grammar - subject-verb agreement, abbreviation use, use of proper speech (lay vs. lie), use of nouns and adjectives, use of proper singular or plural nouns, positioning modifiers, correct verb tense, etc.



**Inappropriate Blanks -- 0.10 points**

This error category refers to a blank that was easily understood by the evaluator. The help of another transcriptionist or helper in the department must be sought and/or other efforts exhausted before leaving a blank.

***Perry Johnson & Associates***  
***Quality Check Sheet***

Transcriptionist: \_\_\_\_\_ Date: \_\_\_\_\_

Quality Associate: \_\_\_\_\_

<u>Error#</u>	<u>Description</u>	<u>Occurrences</u>	<u>Value</u>	<u>Total Error Value</u>
1.	Major Error	_____	X 1.0 =	_____
2.	Minor Error	_____	X .50 =	_____
3.	Format Error	_____	X .50 =	_____
4.	Grammar Error	_____	X 0.25 =	_____
5.	Inappropriate Blanks	_____	X 0.10 =	_____
<b><u>Total Error Value:</u></b>				_____

**Error percentage = [(Total Error value) / (Number of lines)] x 100**

**Accuracy = 100 – Error percentage**

**The accounts for Perry Johnson & Associates, Inc. fall under two categories—Full-edit account and No-edit account.**

- **Full-edit accounts:** All new dictators are by default begun on Full-edit status. These files are fully edited by PJ&A QA's and feedback will be provided on these files so that the transcriptionists can learn quickly.
- **No-edit accounts:** A dictator moves into no-edit status, as soon as the MT begins delivering 99% + accuracy on a consistent basis for 2,000 lines. PJ&A expects that the MTs will make all efforts to move a new account to No-edit status by reaching the desired quality level in 2,000 lines. Moving an account from full edit status to no edit status is done based on the discretion of the PJ&A Quality Assurance Team.

Once an account moves to no-edit status, this category of files will be randomly edited. If the quality is poor on three (3) consecutive uploads for an account that is in no-edit status, the account will be either be moved to no-pay status until 99% accuracy is attained on a consistent basis for 2,000 lines or can be moved out from the MT.

The responsibility of the no-edit files is on the MT. In general, once an MT reaches No-Edit status for a specific client, they will retain that status provided the required quality is maintained on the daily random edit of documents and no client complaints are received.

**Format Audit:**

A format audit will also be done on a weekly basis and files that do not comply with the format requirements will be graded.

Following are the format error categories:

- Incorrect/old template used.
- Incorrect second page format information.
- Excessive space at the end of a page.
- Demographic information mismatch or missing.
- Incorrect format of salutation.
- Not adhering to client specifics.

**Difficult Dictators:**

If the quality of the voice files is bad for a consistent period of time, then this has to be brought to the notice of the Quality Assurance team. They will review the audio files from 2 different perspectives: a) Poor audio quality b) Poor dictation quality. If the audio files fall under "poor audio quality" category, then the Quality Assurance will take up the issue with

the IT team who in turn will work the client to improve the audio quality of files. If the audio files fall under "poor dictation quality," then the Quality Assurance team will bring it to the notice of Customer Service representatives who will then pursue the matter with the concerned clients/dictators on improving the dictation quality. The Customer Service team will also make sure that enough samples are available for tough dictators.

If the voice quality of one (1) particular file is bad, then the concerned MT/Proof Reader will need to bring this to the notice of Quality Assurance team. They will review this file and put a note to client saying "Poor Audio Quality."



**DISASTER RECOVERY PLAN**  
**Perry Johnson & Associates, Inc.**

Revised: January 14, 2017



## TABLE OF CONTENTS

Table of Contents .....	2
Overview .....	3
System Architecture and Topology .....	4
Southfield Data Center.....	5
Grand Rapids Data Center .....	6
Data Backup.....	8
Intrusion Protection.....	8
Data Center Fault Tolerance Components.....	9
Server .....	9
Storage Area Network (SAN).....	9
Oracle Database .....	9
Applications .....	9
Web Servers.....	9
Name Resolution.....	10
Definition of Customer Services.....	11
Telephone Dictation.....	11
GEMS .....	11
Patient Demographic Data Interface.....	11
Document Delivery Interface.....	11
Customer Service Disruption Thresholds .....	12
Telephone Dictation.....	13
GEMS .....	13
Patient Demographic Data Interface.....	13
Document Delivery Interface.....	13
Definition of 'Disaster' Conditions .....	15
Actions Performed for Disaster Recovery .....	16
Telephone Number Reroute.....	16
Verify Virtual Private Network (VPN).....	16
Modify patient demographic data Interfaces .....	16
Modify Document Delivery Interface.....	17
Communication.....	18



## OVERVIEW

This document provides the complete disaster recovery (DR) agreement between the customer and Perry Johnson & Associates, Inc. (PJA).

Disaster Recovery (DR) is one of the most important aspects of system design and operation. A well designed system can survive a range of failures; from small component failures to large scale natural disasters. It is important to understand how the system will survive each type of failure; this document provides specific details about the specific actions that will be taken for each type of failure.

Within this document, the term 'Disaster Recovery' includes the following:

- System Architecture and Topology
- Data Center Fault Tolerance Components
- Definition of Customer Services
- Customer Service Disruption Thresholds
- Definition of 'Disaster' Conditions
- Actions Performed for Disaster Recovery
- Communication

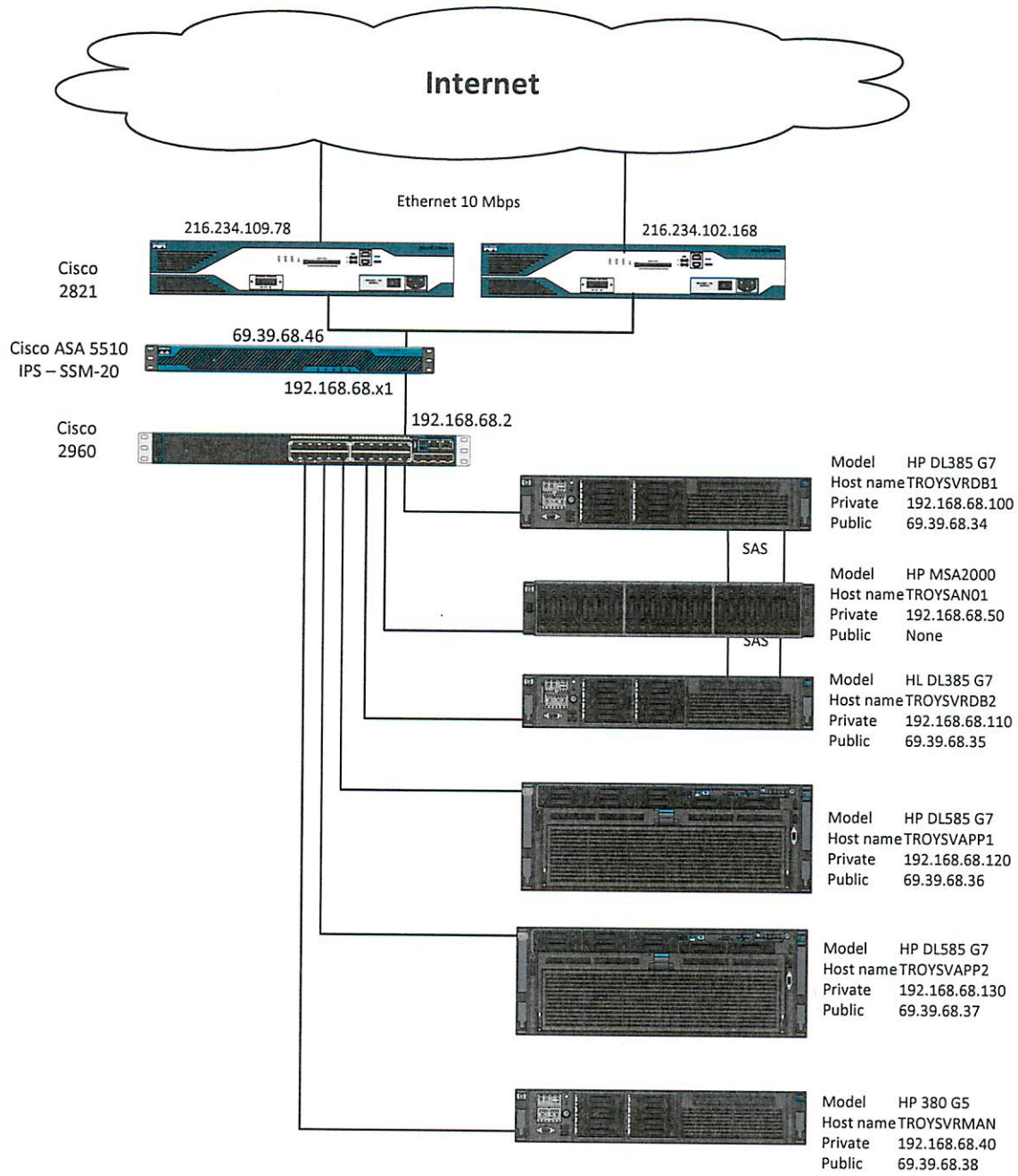


## SYSTEM ARCHITECTURE AND TOPOLOGY

The diagrams on the following pages illustrate the equipment installed at the data centers.



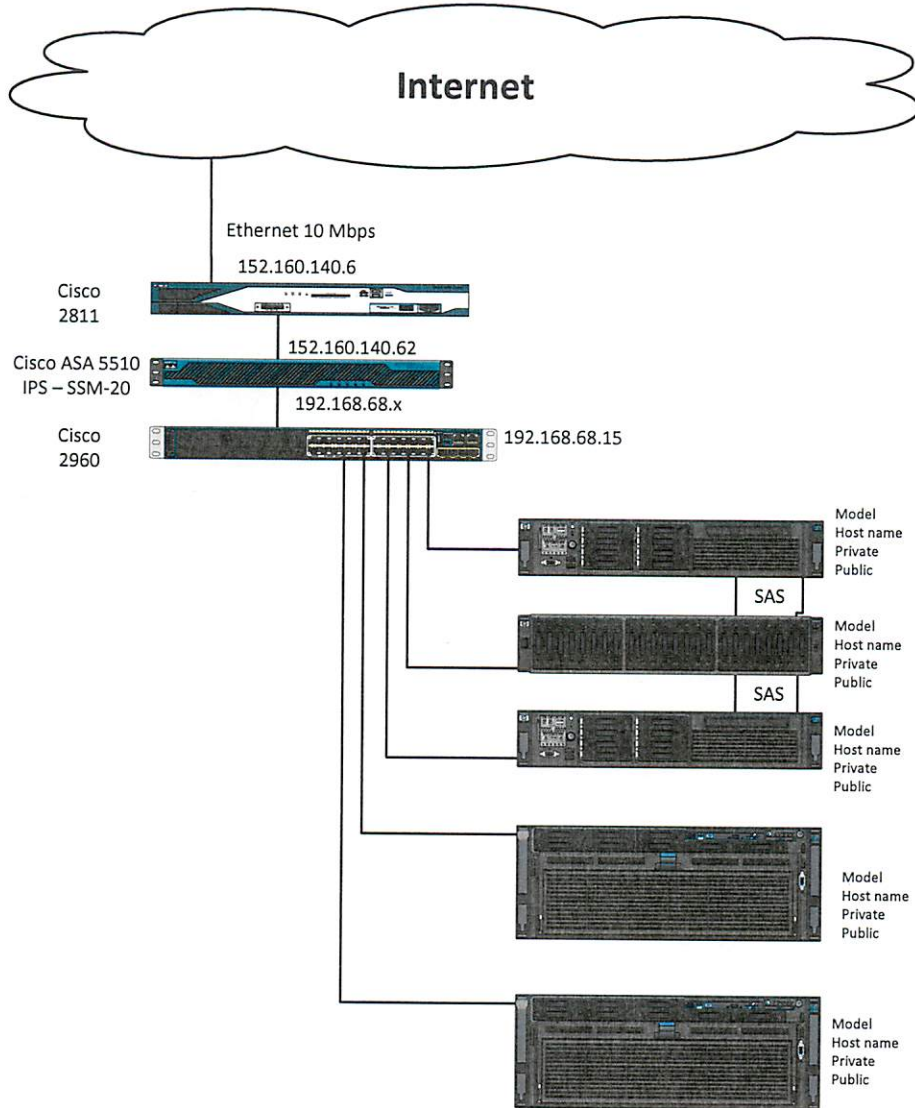
# SOUTHFIELD DATA CENTER







# GRAND RAPIDS DATA CENTER





The equipment at both data centers are installed at a hosted data center. These centers provide the following:

- Backup utility power provided by a 750 kVA diesel generator
- Dual Internet connection circuits; these circuits are provided by separate providers and enter the data center in separate locations using separate fiber
- Physical security is provided with keyless entry systems with video monitoring for all entry doors
- Integrated fire suppression
- Metro Ethernet connectivity for inter data center connectivity

During normal operation, all Oracle data is replicated from one data center to the other. This replication is not synchronous; each transaction is queued and replicated. Replication is performed every 30 seconds.

Applications are deployed as shown below:

<b>Server</b>	TROYSVRDB1 and GRSVRDB1
<b>Applications Installed</b>	Oracle Real Application Clusters Database Server Web Server Name Resolution Server
<b>Server</b>	TROYSVRDB2 and GRSVRDB2
<b>Applications Installed</b>	Oracle Real Application Clusters Database Server Web Server Name Resolution Server
<b>Server</b>	TROYSVRAPP1 and GRSVRAPP1
<b>Applications Installed</b>	Telephone Dictation Server Job Import Server Job Allocation and Workflow Server Document Distribution Server HL7 Interface Server
<b>Server</b>	TROYSVRAPP2 and GRSVRAPP2



### **Applications Installed**

Telephone Dictation Server  
Job Import Server  
Job Allocation and Workflow Server  
Document Distribution Server

### **DATA BACKUP**

All Oracle data is backed up using 'Recovery Manager' (RMAN). These backups include the following:

- Server Parameter File (SPFILE)
- Control File
- Data Files
- Archived Redo Log Files

A level '0' backup is performed at 2:00 am on Saturday.

A level '1' cumulative backup is performed at 2:00 am on Sunday, Monday, Tuesday, Wednesday, Thursday and Friday. By using RMAN as a backup method, the database does not need to be shut down to make full backups. These backup sets are physically stored in the Troy office data center.

PJA utilizes a multilevel incremental backup scheme. A full backup is a level '0' backup. A level '1' backup will back up everything that has changed since the most recent level '0' backup.

### **INTRUSION PROTECTION**

Intrusion protection is provided by an IPS-SSM-20 module located in the Cisco ASA at each data center.



## **DATA CENTER FAULT TOLERANCE COMPONENTS**

The system is designed to function within a single data center. To achieve this goal, each component within each data center includes redundant features. Each of these features is described below:

### **SERVER**

- Each server includes redundant hot swappable power supplies. Each power supply is connected to a separate electrical circuit.
- Each server includes fault tolerant disk storage. All storage volumes implement either RAID 1 or RAID 5. All disk drives are hot swappable.
- The application servers include a hot swappable PCI bus. This allows digital dictation adapters to be replaced while the server is running.

### **STORAGE AREA NETWORK (SAN)**

- A SAN is used for all database data. The SAN includes dual controllers; if either controller fails, the other controller survives without any loss of performance or functionality. This SAN includes redundant hot swappable power supplies.

### **ORACLE DATABASE**

- The Oracle database is deployed on a two-node cluster; the physical data is stored within the SAN. Each node in the cluster uses two physical connections to the SAN; if either connection fails, the other connection continues to provide connectivity without any loss of performance or functionality.

### **APPLICATIONS**

- All applications are configured to connect to the oracle cluster. The connection is dynamic; the Oracle grid software will dynamically allocate the connection to the server with the smallest workload. If either database server fails, the applications will automatically connect to the other server without any loss of functionality. Performance will be reduced in this scenario.

### **WEB SERVERS**

- The web servers are deployed on two servers. The web application is clustered on the two web servers. The web session ID is replicated between the two servers; if either



server fails, the other server will continue to service the web session without any disruption to the client.

### **NAME RESOLUTION**

- Name resolution is provided by BIND. This application is installed on 3 servers within the data center. A single server is configured as the primary server and the other two servers are configured as secondary servers. If name resolution fails on a server, the client application will connect to one of the other servers for uninterrupted service.



## **DEFINITION OF CUSTOMER SERVICES**

The customer interacts with the PJA system using the following services:

### **TELEPHONE DICTATION**

This service enables the physicians and other clinicians the ability to dictate using a telephone. All hospitals share the same dictation applications.

### **GEMS**

This application enables customers to monitor all aspects of the system. It provides the ability to check the status of a job, change the priority of a job, print a transcript and view a transcript. A separate web URL, i.e. <https://hospital.pjats.com>, is implemented for each hospital.

### **PATIENT DEMOGRAPHIC DATA INTERFACE**

This delivers patient encounter data from the customer to PJA. A separate interface is implemented for each hospital.

### **DOCUMENT DELIVERY INTERFACE**

This delivers the completed transcript from PJA to the customer. A separate interface is implemented for each hospital.



## CUSTOMER SERVICE DISRUPTION THRESHOLDS

The previous section defined the following customer services:

- Telephone Dictation
- GEMS
- Patient Demographic Data Interface
- Document Delivery Interface

Disruption of these services cause different impacts to the customer.

- Telephone Dictation

If this service is disrupted, this directly affects physicians. This impacts their ability to provide timely patient information. This will also affect other clinicians who depend on the dictation and the transcript.

Disruption Threshold : 0 minutes

- GEMS

If access to GEMS is disrupted, this directly affects health information management (HIM) personnel. This will impact their ability to verify dictation for a specific encounter, view the status of a transcript and view the transcript.

Disruption Threshold : 30 minutes

- Patient Demographic Data Interface

This service delivers patient data for each encounter to PJA. This patient data is needed for automatic inclusion in the transcript.

Disruption Threshold : 60 minutes

- Document Delivery Interface

This service delivers the completed document from PJA to the customer. The completed document is delivered to CHARMS or HPF. Disruption of this service would impact physicians, clinicians and billing staff.



Disruption Threshold : 120 minutes

Each service depends on one or more hardware and software components. These components are defined below:

### **TELEPHONE DICTATION**

1. Multiple PRI communication circuits from telephone company
2. Cisco Ethernet switch
3. Hardware server : TROYSVRAPP1 or TROYSVRAPP2
4. Digital dictation adapter (Dialogic)
5. Telephone dictation capture application
6. Oracle database running on : TROYSVRDB1 and TROYSVRDB2
7. Name resolution running on : TROYSVRDB1 and TROYSVRDB2

### **GEMS**

1. Internet connectivity circuits
2. Cisco 2821 router
3. Cisco Ethernet switch
4. Hardware server : TROYSVRAPP1 or TROYSVRAPP2
5. Name resolution running on : TROYSVRDB1 and TROYSVRDB2
6. Web server running on : TROYSVRDB1 and TROYSVRDB2
7. Oracle database running on : TROYSVRDB1 and TROYSVRDB2

### **PATIENT DEMOGRAPHIC DATA INTERFACE**

1. Internet connectivity circuits
2. Cisco 2821 router
3. Virtual Private Network (VPN) from Client to Southfield data center
4. Cisco Ethernet switch
5. Hardware server : TROYSVRAPP1
6. Name resolution running on : TROYSVRDB1 and TROYSVRDB2
7. HL7 interface application running on TROYSVRAPP1
8. Oracle database running on : TROYSVRDB1 and TROYSVRDB2

### **DOCUMENT DELIVERY INTERFACE**

1. Internet connectivity circuits
2. Cisco 2821 router
3. Virtual Private Network (VPN) from Client to Southfield data center
4. Cisco Ethernet switch
5. Hardware server : TROYSVRAPP1





6. Name resolution running on : TROYSVRDB1 and TROYSVRDB2
7. Document distribution application running on TROYSVRAPP1
8. Oracle database running on : TROYSVRDB1 and TROYSVRDB2



## **DEFINITION OF 'DISASTER' CONDITIONS**

Any condition which causes the service disruption threshold values to be exceeded will be considered a disaster. Once a disaster has been declared, operation will shift from the current data center to the backup data center.



## **ACTIONS PERFORMED FOR DISASTER RECOVERY**

When a disaster has been declared, it is crucial that the actions required are documented completely and the staff trained to complete these actions. The following actions will be performed:

### **TELEPHONE NUMBER REROUTE**

**Resource** Perry Johnson & Associates, Inc.

**Description** The telephone companies will be contacted; they will be instructed to modify call delivery for the specified dictation telephone numbers. Call delivery will be changed from the circuits at the failing data center to the circuits at the surviving data center. PJA staff will verify that job import application is running at surviving data center.

### **VERIFY VIRTUAL PRIVATE NETWORK (VPN)**

**Resource** Perry Johnson & Associates, Inc.  
Customer

**Description** Both resources will verify that the VPN to the surviving data center is active. No action should be required; this VPN is expected to be active at all times.

### **MODIFY PATIENT DEMOGRAPHIC DATA INTERFACES**

**Resource** Perry Johnson & Associates, Inc.  
Customer

**Description** The customer will be responsible for changing the target IP address and port number for each HL7 interface.

Perry Johnson & Associates, Inc. will be responsible for starting the HL7 interface applications on the servers at the surviving data center

Both resources will verify connectivity and verify that patient data is being received by PJA.



## MODIFY DOCUMENT DELIVERY INTERFACE

**Resource**      Customer

**Description**      The customer will be responsible for modifying the document delivery interface to retrieve documents from a different location. The new location will be the server IP address and server share name within the surviving data center.



## COMMUNICATION

When any type of disruption of services has been detected, it is critical that communication to facility staff occurs immediately following the instance and following the diagnosis of the disruption.

At time of disruption, PJA will communicate such disruption to the defined Client staff via email notification of affected systems, what measures are currently taking place to diagnose and correct and an estimated time for resolution.

If at any time PJA requires assistance from the facility IT support staff, PJA will contact the appropriate team members. Examples of this would be restarting interfaces, VPN redirection and telephony support.

During any extended outage, recurrent updates will occur at regular intervals stating the current status, steps taken and time lines for resolution.

If deemed necessary, conference calls will occur for open discussion and Q&A.

A follow up meeting will be scheduled after resolution to discuss what happened, how the problem was resolved and how we plan to mitigate future occurrences.



## HIPAA SECURITY POLICIES AND PROCEDURES

Effective Date: February 23, 2017



## **GENERAL POLICY**

Perry Johnson & Associates, Inc., ("Business Associate") performs certain functions, activities, or services for, or on behalf of, one or more covered entities (each, a "Covered Entity") whereby it may create, receive, maintain, or transmit for, or on behalf of, the Covered Entity certain protected health information ("PHI") related to persons who are the subject of PHI and, as such, is a "business associate" of the Covered Entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

On January 25, 2013, the Office of Civil Rights of the U.S. Department of Health and Human Services ("HHS") released a final rule (the "Final Rule") implementing changes to the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules, many of which are required by the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act").

Business Associate is committed to meet the requirements of HIPAA, and as of the Effective Date has implemented these HIPAA Security Policies and Procedures to comply with the Final Rule, the applicable requirements of Security Standards for the Protection of Electronic Protected Health Information (the "Security Rule"), 45 CFR 164 subpart C, and with our responsibility to protect individually identifiable health information and the system components that such data resides in under HIPAA, the HITECH Act, the security and privacy regulations implementing HIPAA and HITECH Act, including without limitation, the policies and procedures and documentation requirements set forth in 45 CFR 164.308, 164.310, 164.312 and 164.316, as may be amended from time to time, other federal and state laws protecting confidentiality of health information, and professional ethics.

The law requires us to ensure the confidentiality, integrity, and availability of electronic PHI that Business Associate creates, receives, maintains, or transmits. Business Associate takes the privacy of electronic PHI seriously and expects its employees and subcontractors to do the same. All workforce members, including officers and employees, of Business Associate **must** adhere to these Policies and Procedures. Violations of any of these Policies and Procedures are grounds for disciplinary action up to and including termination of employment and other sanctions in accordance with Business Associate's HIPAA Sanctions Policy and personnel rules and regulations.

If you have any questions regarding security of electronic PHI, please contact Security Official.

## **SECURITY AWARENESS AND TRAINING**

To assist in compliance with these Security Policies and Procedures, Business Associate employees and others who are considered part of Business Associate's "workforce," including management, will be trained to understand, implement, and become aware of these Security Policies and Procedures and the Security Rule. Security Official is responsible for conducting the training, or delegating the training to an appropriately qualified employee or consultant. The training will be conducted for each person within a reasonable time after he or she becomes a member of Business Associate's workforce, and periodically for all workforce members at least once every twelve (12) months thereafter. Personnel directly involved in the design, deployment, maintenance and security of Business Associate's information technology infrastructure will be given security specific training to enable them to develop the expertise necessary to maintain that infrastructure in a manner consistent with these Security Policies and Procedures. Each member of Business Associate's workforce whose functions are affected by a material change in these Policies or Procedures will be trained within a reasonable period of time after the material change becomes effective. Business Associate will also train all members of its workforce on all Policies and Procedures implemented in connection with the Final Rule, as necessary and appropriate for the members of the workforce to carry out their functions



within Business Associate, within ten (10) business days of the Effective Date of these Policies and Procedures. Business Associate must document that the training has been provided.

## **POLICIES AND PROCEDURES**

**General Security Standards.** As a business associate, Business Associate must ensure the confidentiality, integrity, and availability of all electronic PHI it creates, receives, maintains, or transmits. Business Associate is responsible for protecting against any reasonably anticipated threats or hazards to the security or integrity of all electronic PHI, as well as protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted. Business Associate will review and modify these Policies and Procedures and the security measures implemented under the Security Rule as needed to continue provision of reasonable and appropriate protection of electronic PHI, and update documentation of such security measures in accordance with the Privacy Rule. To make certain that the standards set forth in the Security Rule are met, Business Associate must ensure compliance with the Security Rule by its workforce. If you have any questions regarding the security of electronic PHI or these Security Policies and Procedures, please contact Business Associate's Security Official.

**Security Official.** Business Associate must designate a Security Official who will be responsible for Business Associate's maintenance of and adherence to these Security Policies and Procedures, as well as developing and implementing these Security Policies and Procedures to ensure the confidentiality, integrity, and availability of the electronic PHI that Business Associate creates, receives, maintains, or transmits. Security Official will be responsible for developing and implementing a documented risk assessment procedure, taking into consideration existing models for risk assessment. Security Official may delegate any of these responsibilities to another member of Business Associate's workforce, and will oversee the work of that person. Security Official will work with technical staff and, where appropriate, with "outside" experts to determine and implement effective security and risk assessment measures. Security Official and others involved may recommend actions to be taken by Business Associate to ensure that reasonable and appropriate measures are in place to safeguard electronic PHI.

Jeffrey Hubbard is designated as Business Associate's Security Official and contact person regarding all PHI security matters.

**Access.** Only those persons or software programs that have been granted access rights will be allowed to access electronic PHI.

**Workforce Members' Access.** Security Official will assign unique user identification names and/or numbers and passwords to Business Associate workforce members to ensure that all workforce members that are authorized to access electronic PHI have the appropriate access to electronic PHI, and to prevent those workforce members who do not have authorization from obtaining access to electronic PHI. Other authentication processes may be used as deemed appropriate.

**Audit Controls.** Security Official will track and examine activity on information systems that contain or use electronic PHI.

**Business Associate Workforce Members.** Business Associate workforce members are authorized to have access to the minimum amount of electronic PHI necessary to perform their duties, and shall not access electronic PHI for purposes unrelated to the performance or inconsistent with their duties. All workforce members are subject to existing personnel screening policies, are required to follow Business Associate's HIPAA Security Policies and Procedures, and are required to report to Security Official any actual, suspected, or potential security incidents or breach of these Security Policies and Procedures that might affect the security of Business Associate's computer network or the





confidentiality, availability or integrity of electronic PHI. Security Official will determine whether the allegedly improper use or disclosure violates Business Associate's Security Policies and Procedures or the Security Rule. If you are unsure whether you are permitted to view electronic PHI for a particular purpose, contact Security Official.

Computer screens and workstations. Business Associate workforce members must ensure that electronic PHI is not readily visible from their workstations. When workforce members leave their workstations because of other duties or during non-work periods, they must close all programs that display electronic PHI and/or log off the workstation, and place all non-electronic PHI in locked drawers. Computer screens at workstations should not be visible to non-workforce members. All Business Associate workstations that can access electronic PHI will require username and passwords to restrict access only to authorized users.

E-Mail Communications. Electronic PHI should not be sent by e-mail or other electronic transmission unless it conforms to the appropriate encryption standards. If you are unsure whether the transmission conforms to the appropriate encryption standard, please contact Security Official. The e-mail system and all messages generated or handled by e-mail, including backup copies, are property of Business Associate. E-mail users have no right to privacy in their use of the computer system, including e-mail. Business Associate may monitor the content and usage of the computer system, including, e-mail, at any time and for any reason. E-mail users should restrict use of the e-mail system to proper business purposes. Any personal e-mail use should be avoided and may result in removal, demotion, suspension, or termination in some circumstances.

Fax Communications. Electronic PHI should not be faxed on or to a machine that is known to be accessible by the general public. Indicate the confidential nature of the fax on the cover sheet and request that any erroneous recipient destroy or return the fax. Confirm correctness of fax numbers periodically. Use your best efforts to ensure that an unintended recipient does not receive a confidential fax. When possible, contact any unintended fax recipient and request the return or destruction of the fax.

Portable Electronic Data. Employees, subcontractors, and others using portable data media, including, CD-ROMs, USB Drives, smart phones, tablets, portable computers or other electronic data media may not download, maintain, or transmit confidential patient or other information without the written authorization of Security Official, who must also retain a copy of such authorization.

Facility Access. Business Associate will limit physical access to its electronic information systems and the facility or facilities in which they are housed only to those who have the proper authorization by way of key, access code, or other reasonable methods.

Business Associates. Only subcontractors that have signed a business associate agreement consistent with the provisions of HIPAA and the Final Rule may access electronic PHI to the extent necessary to perform functions, services or activities for, or on behalf of, Business Associate. Please refer to our HIPAA Privacy Policies and Procedures for additional requirements related to subcontractors and business associate agreements with subcontractors.

Sanctions. Business Associate will sanction any employee or non-employee that uses or discloses electronic PHI in violation of Business Associate's Security Policies and Procedures or in violation of HIPAA. Business Associate will also sanction any subcontractor uses or discloses electronic PHI in violation of its business associate agreement, these Security Policies and Procedures or in violation of HIPAA. A violation will result in an appropriate reprimand, including but not limited to, oral and written warnings, removal, demotion, suspension, financial penalties, or termination for employees, or termination of business relationship for non-employees and subcontractors.



Termination of Access Privileges. Security Official must be immediately notified when a member of Business Associate's workforce has been separated from Business Associate due to retirement, resignation, termination or leave of absence. If there is an advance notice of a termination, Security Official must be timely informed prior to the effective date of termination. Security Official will limit and/or disable the separating individual's access to Business Associate's computer network and electronic PHI. Appropriate steps to prevent the former employee or other workforce member from gaining access to electronic PHI may include such actions as changing locks, removal from access lists, removal of user accounts and/or passwords, retrieval of keys, etc.

Risk Assessment and Analysis. Security Official will conduct risk assessments to identify threats to the security of Business Associate's computer network and the confidentiality, availability, and integrity of electronic PHI. The components of the risk assessment include physical and logical security mechanisms developed, implemented, maintained, and updated following a documented risk assessment process. Risk assessments will be made periodically to enable Security Official to make informed decisions about measures to be used to safeguard Business Associate's computer network and electronic PHI, and to reduce risks and vulnerabilities to a reasonable and appropriate level, based on accurate and current information. Business Associate's decisions about the design, deployment, maintenance, administration and growth of the information technology infrastructure will be guided by current security risk assessments.

System Activity Review. Security Official, or its designee, will periodically review records of information system activity such as audit logs, access reports, and security incident tracking reports.

Emergency, Disaster Recovery Plan. Security Official will ensure that Business Associate's workforce, subcontractors, and others authorized to access Business Associate's electronic PHI, will be able to access electronic PHI without unacceptable delay in the event of an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Business Associate's computer network. Security Official will be responsible for developing and periodically testing a disaster recovery plan, identifying sources for most recent backup copies of data, and establishing procedures to restore lost data. Security Official will review the disaster recovery plan, test the procedures described in the plan, and revise the plan as needed.

Data Backup. All electronic PHI will be properly copied and stored so that in the event that original documents, electronic records, or prodigies of electronic records are destroyed, they can be recreated as necessary. In the event of a disaster, whether natural or man-made, Business Associate must be able to reproduce all electronic PHI created, maintained and stored on its computer network.

Media Re-Use and Disposal. Security Official, or its designee, will ensure that upon receipt or final disposition of electronic PHI, and/or the hardware or electronic media on which it is stored such as for example, copiers, personal computers and servers, no electronic PHI can be accessed by unauthorized persons. Security Official will ensure that all electronic PHI is removed from electronic media before the media are made available for re-use. No electronic PHI may be altered, copied, destroyed, or removed from the premises without first notifying Security Official.

Availability. The documentation of these Security Policies and Procedures will be made available to Security Official and to those persons responsible for implementing the Security Policies and Procedures to which the documentation pertains.

Evaluation and Maintenance. Security Official will be responsible for periodically evaluating all technical and non-technical documents and records of these Security Policies and Procedures, and updating them as needed in response to environmental or operational changes affecting the security of



electronic PHI, in order to maintain reasonable and appropriate protection of electronic PHI, and to ensure that they meet the requirements of the Security Rule.

Record Retention. All documents and records received, sent, or created by Business Associate will be documented and retained by Business Associate in writing or electronic form for six (6) years from the date the document was sent, received, created or the date it was last in effect, whichever is later. Documents and records of Business Associate relating to Business Associate's activities (i.e., indicating who has been trained, what training occurred, and the date of training, sanctions, etc.) will be maintained by Business Associate for six (6) years following the date the documents or records were created, sent or received, or the date it was last in effect, whichever is later

#### **MITIGATION OF BREACH OF SECURITY OF PHI**

Every employee, independent contractor, agent and business associate must agree in writing to protect the security of any electronic PHI to which they are exposed. Once an actual, suspected, or potential breach of these HIPAA Security Policies and Procedures is reported to Security Official, Security Official will determine whether that improper use or disclosure could harm the patient whose electronic PHI was improperly used or disclosed. Security Official will mitigate the harm to the extent practicable, and take steps to secure against similar future breaches. Security Official will identify and isolate suspicious activity and contain, and recover from, network damage resulting from any security incident. All security incidents of which Business Associate becomes aware and their outcomes must be documented and reported to the applicable Covered Entity as soon as reasonably possible after discovery. Refer to our Breach Notification Rule Policies and Procedures for a determination if a reportable Breach occurred.

## Smartphones

### HIPAA Security Policy & Guidelines

Four criteria must be met to ensure PJ&A data and email are secure on a smartphone, and apply regardless of whether they are PJ&A provided or personally-owned:

1. The phone must have password protection
2. Data on the phone must be encrypted
3. It must limit the number of messages stored on the device
4. It must have the ability for data to be remotely purged if the device is lost or stolen.

Personally-owned Smartphones used to access, store, transmit or receive PJ&A data (typically email messages) must also meet these security standards. Please verify encryption and purge capabilities with your service provider and set up a password and email limits in compliance with PJ&A policy.

If you would like to know if your phone is encrypted, here's how:

iPhone – 3GS or newer models have been secured if a password is required prior to use.

#### Blackberry Devices (newer models with 5.x firmware)

1. From the Home screen of the BlackBerry smartphone, click Options.
2. Click Security Options.
3. Click Encryption.
4. Encryption is enabled

#### Older Blackberry Devices (with firmware prior to 5.x)

1. From the Home screen of the BlackBerry smartphone, click Options.
2. Click Security Options.
3. Click General Settings.
4. Content Protection is enabled.

#### Droid Devices

Please verify encryption and purge capabilities with your service provider and set up a password and email limits in compliance with PJ&A policy.

Devices other than those listed above won't meet the requirements and should not be used to access, store, receive or transmit PJ&A data and emails.

**Agreement on Use of USB Flash Drive**

Whereas, Perry Johnson & Associates, Inc. (PJ&A) has entrusted to the undersigned certain corporate USB flash drive(s),

And whereas, said USB flash drive(s) is (are) to be used exclusively for PJ&A business,

And whereas, the undersigned acknowledges and agrees to use said USB flash drive(s) shall remain, in perpetuity, the exclusive, confidential proprietary property of PJ&A,

The undersigned hereby acknowledges and agrees to the use said USB flash drive(s) with due care and diligence.

Each USB flash drive(s) will not contain any ePHI data. All data will be encrypted using an on-the-fly encryption tool. On the fly encryption means all files saved will be automatically encrypted. In the event of a lost, stolen or misplaced USB flash drive(s), the undersigned will notify PJ&A management immediately.

The undersigned further acknowledges and agrees that upon termination of employment with PJ&A, the undersigned shall immediately account for and return said USB flash drive(s) to PJ&A. Failure by the undersigned to return said USB flash drive(s) to PJ&A will result in legal action for its (their) repossession, at the undersigned's exposure.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

User:

Serial Number:

\_\_\_\_\_  
Witness

\_\_\_\_\_  
Accepted for Perry Johnson &  
Associates, Inc. by



## Data Security Incident Response Procedures

Revised: March 1, 2017



## Table of Contents

Incident Response Plan .....	3
Incident Response Team .....	3
Incident Response Team Members .....	3
Incident Response Team Roles and Responsibilities.....	3
Incident Response Team Notification.....	4
Types of Incidents.....	4
Breach of Personal Information - Overview .....	5
Definitions of a Security Incident .....	5
Requirements .....	5
Custodian (Owner) Responsibilities .....	5
When Notification Is Required .....	5
Incident Response .....	6
IT Security Officer.....	6
Notification Steps.....	8
Process Steps.....	8
Network Services .....	8
PJ&A Communications .....	8
Privacy Officer.....	8
Health Insurance Portability and Accountability Act of 1996 (HIPAA).....	9



## Incident Response Plan

An Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the organization. The Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

## Incident Response Team

An Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications. The Incident Response Team's mission is to prevent ePHI exposure, a serious loss of profits, public confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The IT Security Officer will coordinate these investigations.

## Incident Response Team Members

Each of the following areas will have a primary and most an alternate member:

1. PJ&A IT Security Officer (SEC)
2. PJ&A Privacy Officer (IPO)
3. Operations (OPS)
4. Network Services (NET)
5. Web Applications (WEB)
6. PJ&A Communications Dept (COM)
7. Helpdesk (HLP)

## Incident Response Team Roles and Responsibilities

### IT Security Officer (SEC)

- Determines the nature and scope of the incident
- Contacts qualified information security specialists for advice as needed
- Contacts members of the Incident Response Team Determines which Incident Response Team members play an active role in the investigation
- Provides proper training on incident handling
- Escalates to executive management as appropriate
- Contacts auxiliary departments as appropriate
- Monitors progress of the investigation
- Ensures evidence gathering, chain of custody, and preservation is appropriate
- Prepares a written summary of the incident and corrective action taken

### Privacy Officer (IPO)

- Coordinates activities with the IT Security Officer





Documents the types of personal information that may have been breached  
Provides guidance throughout the investigation on issues relating to privacy of customer and employee personal information  
Assists PJ&A Communications in developing appropriate communication to impacted parties  
Assesses the need to change privacy policies, procedures, and/or practices as a result of the breach

#### Operations (OPS)

Ensures all service packs and patches are current on mission-critical computers  
Ensures backups are in place for all critical systems  
Examines system logs of critical systems for unusual activity  
Notifies IT Security Officer of incidents and /or the need to activate computer incident response team

#### Network Services (NET)

Analyzes network traffic for signs of denial of service, distributed denial of service, or other external attacks  
Runs tracing tools such as sniffers, Transmission Control Protocol (TCP) port monitors, and event loggers  
Looks for signs of a firewall breach  
Takes action necessary to block traffic from suspected intruder

#### Web Applications (WEB)

Monitors web applications and services for signs of attack  
Reviews audit logs of mission-critical servers for signs of suspicious activity  
Contacts the IT Security Officer with any information relating to a suspected breach  
Collects pertinent information regarding the incident

#### PJ&A Communications Dept (COM)

Coordinates all public disclosures required by law or at the direction of PJ&A Administration.

#### Helpdesk (HLP)

Perform testing and mitigation on systems and/or dispatch technicians for testing and mitigation

## Incident Response Team Notification

The Security Officer will be the central point of contact for reporting computer incidents or intrusions. All computer security incidents must be reported to the IT Security Officer. A preliminary analysis of the incident will take place by the SEC and that will determine whether Incident Response Team activation is appropriate.

## Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Compromised Systems
- Excessive Port Scans / Denial of Service / Distributed Denial of Service
- Firewall Breach
- Virus Outbreak / Malware
- Breach of Personal Information ( see appendix X for additional procedures )



## Breach of Personal Information - Overview

For our purposes, personal information is defined as an individual's first name or first initial and last name, in combination with any of the following data, such as:

- Social Security number
- Driver's license number or Identification Card number
- Home address or e-mail address
- Medical or health information
- Date of birth

Note: that the data disclosed in an incident may be governed by multiple laws each having their own specific definition. The above list is illustrative but not presented as comprehensive or specific to a particular law or regulation.

## Definitions of a Security Incident

PJ&A uses the definition per HIPAA. A security incident means the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with system operations in an information system. Response and reporting implementation requirements include identifying and responding to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

## Requirements

Custodians (owners) must identify and document all systems and processes that store or utilize personal information of individuals. Documentation must contain system name, device name, file name, location and system administrator (primary and secondary contacts for each). The IT Security Officer must maintain the contact list of system administrators.

All authorized users who access or utilize personal information on individuals should be identified and documented by the respective custodians. Documentation must contain user name, department, functional role, device name (i.e., workstation or server), file name, location, and system administrator (primary and secondary contacts).

## Custodian (Owner) Responsibilities

Custodians (owners) responsible for personal information play an active role in the discovery and reporting of any breach or suspected breach of information on an individual. In addition, they will serve as a liaison between PJ&A and any third party involved with a privacy breach affecting the organization's data.

All custodians must report any suspected or confirmed disclosure of personal information to the IT Security Officer immediately upon discovery. This includes notification received from any third party service providers or other business partners with whom PJ&A shares personal information on individuals. The IT Security Officer will notify the Privacy Officer and custodians whenever a breach or suspected breach of personal information on individuals affects their business area.

The IT Security Officer will determine whether the breach or suspected breach is serious enough to warrant full incident response plan activation (See "Incident Response" section.) The custodian will assist in acquiring information, preserving evidence, and providing additional resources as deemed necessary by the CPO, IT Security Officer, Legal or other Incident Response Team members throughout the investigation.

## When Notification Is Required

Incidents may require notification to individuals under contractual commitments or applicable laws and regulations. The IT Security officer, Privacy Officer, Office of General Counsel and PJ&A Communications department together with the custodians are responsible for identifying the parties to whom notification is required and advise those parties appropriately.



## Incident Response

Incident Response Team members must keep accurate notes of all actions taken, by whom, and the exact time and date. Each person involved in the investigation must record his or her own actions.

### IT Security Officer

Contacts	Office Phone	Cell Phone	E-Mail
Phil Buzzette	(800) 803-6330	313-585-1691	<a href="mailto:pbuzzette@pjview.com">pbuzzette@pjview.com</a>

Alternate: TBD

1. Performs a preliminary analysis of the facts and assess the situation to determine the nature and scope of the incident.
2. Informs the legal department and the Privacy Officer if a possible privacy breach has been reported and provides them an overview of the situation.
3. Contacts the individual who reported the problem.
4. Identifies the systems and type(s) of information affected and determines whether the incident could be a breach, or suspected breach of personal information about an individual. Every breach may not require participation of all Incident Response Team members (e.g., if the breach was a result of hard copy disposal or theft, the investigation may not require the involvement of system administrators, the firewall administrator, and other technical support staff).
5. Reviews the preliminary details with the Legal Department and the Chief Privacy Office.
6. If a privacy breach affecting personal information is confirmed, Incident Response Team activation is warranted. Contact the IT support team and advise them to update the Incident Request with "Incident Response Team Activation – Critical Security Problem".
7. Notify the Communications Department of the details of the investigation and breach. Keep them updated on key findings as the investigation proceeds.
8. The IT Security Officer is responsible for documenting all details of an incident and facilitating communication to executive management and other auxiliary members as needed.
9. Contact all appropriate database and system administrators to assist in the investigation effort. Direct and coordinate all activities involved with Incident Response Team members in determining the details of the breach.
10. Contact appropriate Incident Response Team members.
11. Identify and contact the appropriate Custodian affected by the breach. In coordination with the Office of General Counsel, Privacy Officer and Custodian, determine additional notification requirements (e.g., Human Resources, external parties).
12. If the breach occurred at a third party location, determine if a legal contract exists. Work with the Office of General Counsel, Privacy Officer and Custodian to review contract terms and determine next course of action.
13. Work with the appropriate parties to determine the extent of the potential breach. Identify data stored and compromised on all test, development and production systems and the number of individuals at risk.



14. If personal information is involved, determine the type of personal information that is at risk, including but not limited to:

Name, Address, Social Security Number, Account number, Cardholder name, Cardholder address, Medical and Health Information

15. If personal information is involved, have the Custodian determine who might be affected. Coordinate next steps with the Office of General Counsel, Information Privacy Office and Public Relations (e.g., individual notification procedures).

16. Determine if an intruder has exported, or deleted any personal information data.

17. Determine where and how the breach occurred.

Identify the source of compromise, and the timeframe involved.  
Review the network to identify all compromised or affected systems. Consider e-commerce third party connections, the internal corporate network, test and production environments, virtual private networks, and modem connections. Look at appropriate system and audit logs for each type of system affected.

Document all internet protocol (IP) addresses, operating systems, domain name system names and other pertinent system information.

18. Take measures to contain and control the incident to prevent further unauthorized access to or use of personal information on individuals, including shutting down particular applications or third party connections, reconfiguring firewalls, changing computer access codes, and modifying physical access controls.

Change all applicable passwords for IDs that have access to personal information, including system processes and authorized users. If it is determined that an authorized user's account was compromised and used by the intruder, disable the account.

Do not access or alter the compromised system.

Do not turn off the compromised machine. Isolate the system from the network (i.e., unplug cable).

Change the wireless network Service Set Identifier (SSID) on the access point (AP) and other authorized devices that may be using the corporate wireless network.

19. Monitor systems and the network for signs of continued intruder access.

20. Preserve all system and audit logs and evidence for law enforcement and potential criminal investigations. Ensure that the format and platform used is suitable for review and analysis by a court of law if needed. Document all actions taken, by whom, and the exact time and date. Each employee involved in the investigation must record his or her own actions. Record all forensic tools used in the investigation.

21. If an internal user (authorized or unauthorized employee, contractor, consultant, etc.) was responsible for the breach, contact the appropriate Human Resource Manager for disciplinary action and possible termination. In the case of contractors, temporaries, or other third-party personnel, ensure discontinuance of the user's service agreement with the UTSHC.

Custodian Contacts	Office Phone	Email
Primary: Jim Nowak	(800) 803-6330	<a href="mailto:jinowak@pjats.com">jinowak@pjats.com</a>
Bryan Newby	(800) 803-6330	<a href="mailto:bnewby@pjats.com">bnewby@pjats.com</a>

List Maintained by SEC



Alternate: Various

**Notification Steps**

1. If the IT Customer Database group or Custodians hear of or identifies a privacy breach or data disclosure, contact the SEC.
2. The Custodians will assist the IT Security Officer as needed in the investigation.

**Process Steps**

1. Monitor access to customer database files to identify and alert any attempts to gain unauthorized access. Review appropriate system and audit logs to see if there were access failures prior to or just following the suspected breach. Other log data should provide information on who touched what file and when. If applicable, review security logs on any non-host device involved (e.g., user workstation).
2. Identify individuals whose information may have been compromised. An assumption could be "all" if an entire table or file was compromised.
3. Secure all files and/or tables that have been the subject of unauthorized access or use to prevent further access.
4. Upon request from the IT SECURITY OFFICER, provide a list of affected individuals, including all available contact information (i.e., address, telephone number, email address, etc.).

**Network Services**

Contacts	Office Phone	Cell Phone	E-Mail
Scott Bogart	(248) 358-3388	(586) 354-4244	<a href="mailto:sbogart@pjview.com">sbogart@pjview.com</a>

1. When notified by the IT Security Officer that the privacy breach Incident Response Plan is activated, provide assistance as determined by the details of the potential breach.
2. Review firewall logs for correlating evidence of unauthorized access.
3. Implement firewall rules as needed to close any exposures identified during the investigation.

**PJ&A Communications**

Contacts	Office Phone	Cell Phone	E-Mail
Brittany Larson	5140	(248) 275-8488	<a href="mailto:blarson@pjats.com">blarson@pjats.com</a>

**Ongoing:**

1. Monitor consumer privacy issues and practices of other institutions.
2. Monitor consumer privacy breaches of other institutions and how they respond.
3. Keep generic/situational talking points current.

**When Privacy Breach Occurs:**

1. After confirmation that a breach of personal information about individuals has occurred, notify the Public Relations Director.
2. Coordinate with the CPO and Legal on the timing, content and method of notification. Prepare and issue press release or statement, if needed.

**Privacy Officer**

Contacts	Office Phone	Cell Phone	E-Mail
Brittany Larson	5140	(248) 275-8488	<a href="mailto:blarson@pjats.com">blarson@pjats.com</a>

1. Monitor consumer privacy issues and practices of other institutions.
2. Assist in investigating breaches of data privacy.



## Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The primary focus of HIPAA was to improve the health insurance accessibility to people changing employers or leaving the workforce. It also addressed issues relating to electronic transmission of health-related data in Title II, Subtitle F of the Act entitled "Administrative Simplification". The administrative simplification provisions include four key areas:

- National standards for electronic transmission
- Unique health identifiers for providers, employers, health plans and individuals
- Security Standards
- Privacy Standards

The HIPAA Security Standards require a covered entity to implement policies and procedures to ensure:

- The confidentiality, integrity, and availability of all electronic protected health information
- Protect against any reasonably anticipated threats or hazards to the security of such information
- Protect against any reasonably anticipated uses or disclosures that are not permitted

Within this context, HIPAA requires a covered entity to implement policies and procedures to address security incidents. A security incident means the attempted or successful unauthorized access, use disclosure, modification, or destruction of information or interference with system operations in an information system. Response and reporting implementation requirements include identifying and responding to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.

The HIPAA security standards were effective on April 21, 2003. The compliance date for covered entities is by April 21, 2005 and April 21, 2006 for small health plans. The HIPAA privacy and security standards were significantly enhanced by the HITECH Act of 2009, which includes a breach notification provision. Note that this provision would apply to electronic, written or verbal breaches.

Under these new provisions, a breach is defined as the acquisition, access, use or disclosure of protected health information in a manner not permitted under the Privacy Rule and which poses a significant risk of financial, reputational, or other harm to the individual. As there are many details and exceptions to be considered to determine if a breach requires notification, these procedures apply:

- (1) All suspected breaches must be reported immediately to the IT Security Officer or Privacy Officer.
- (2) The IT Security Officer, together with a response team designated for that incident, will promptly investigate the facts and circumstances, perform and document the required risk analysis and report findings to PJ&A Administration.

Breach notifications are required without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. The content of a notification, in plain language, will include:

- (1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
- (2) A description of the types of unsecured protected health information what were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
- (3) Any steps individuals should take to protect themselves from potential harm resulting from the breach;
- (4) A brief description of what PJ&A is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- (5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, Web site, or postal address.

If the breach requires notification, then PJ&A will provide notice by:



- (1) Written notice by first-class mail to last known address of subject person, or
- (2) If subject person has agreed to receive electronic notice, the notice may be sent by electronic mail.
- (3) If subject person is deceased, the written notice will be sent to the last known address of the listed next of kin.

If PJ&A does not have sufficient contact information or if written notices are returned as undeliverable, substitute notification by electronic mail or telephone call will be done. If PJ&A does not have contact information or has out-of-date contact information for the next of kin, substitute notification for deceased persons will not be done.

If PJ&A has insufficient or out-of-date contact information for 10 or more individuals, then one of these substitute notifications will be done:

- (1) A conspicuous posting of notice on PJ&A home page for 90 days, or
- (2) Notification in major print or broadcast media in geographic areas where individuals affected by the breach are likely to reside.
- (3) Additionally, PJ&A will provide a toll-free number for 90 days, where an individual can learn whether the individual's unsecured PHI may be included in the breach.

In situations deemed to be urgent by PJ&A because of possible imminent misuse of unsecured PHI, PJ&A may notify by telephone or other means in addition to other notices.

In the event the breach involves more than 500 individuals, PJ&A will:

- (1) Send notification to major statewide media within 60 days, and
- (2) Notify the Secretary of the U. S. Department of Health and Human Services.

The IT Security Officer will maintain a breach notification log that documents breaches during the current calendar year and will submit that log within 60 days after the end of each calendar year to the Secretary of the U. S. Department of Health and Human Services.

## Client Reference Form

### Offeror Information

Company Name (Offeror): Perry Johnson & Associates, Inc.	Company (Offeror) Address: 1489 W. Warm Springs STE 110 Henderson, NV 89014
Name of Project: Transcription Services	

### Client Information

Organization Name (Client): <i>North Kansas City Hospital</i>	Organization Address: <i>2800 Clay Edwards Drive, North KS City, MO, 64116</i>
Person Providing the Reference: <i>Norma Knipp</i>	Title: <i>Director, HIM</i>
Phone Number: <i>816-691-1590</i>	Email address: <i>norma.knipp@nkch.org</i>
Reference <u>Signature</u> & Date: <i>Norma Knipp 3-16-17</i>	

The person providing the reference, as identified above, must provide the following information. This person must be a responsible party of the organization for which the work was performed. This person should have comprehensive knowledge about the project and the company's (Offeror) role and responsibilities within the project.

**1. Briefly describe the services provided by the company identified above.**

*Medical Transcription - All Hospital Physician Dictation is transcribed (excluding Path + XRay); Code Dx from H&P for EMR DX List.*

**2. Rate each of the following concerning this company's performance using the ratings below:**

- S - Strongly Agree/Very Positive
- A - Agree/Positive
- N - Neutral
- D - Disagree/ Negative
- F - Failed

Rating

- S A. This company ensured the project deliverables were completed on time and within the agreed budget.
- S B. This company provided the appropriate resources to the project.
- S C. This company was knowledgeable in providing the services.
- S D. The business relationship with this company was positive and cooperative, versus negative and adversarial.
- S E. This company provided open, timely communications, and was responsive to our needs and requirements.
- S F. I would choose to work with this company again.

**Additional Comments:**

*I am happy to speak with you to answer any further questions.*

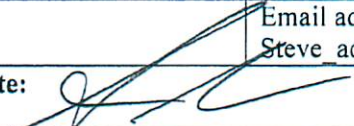


# Client Reference Form

## Offeror Information

Company Name (Offeror): Perry Johnson & Associates, Inc.	Company (Offeror) Address: 1489 W. Warm Springs STE 110 Henderson, NV 89014
Name of Project: Transcription Services	

## Client Information

Organization Name (Client): Concentra Health Services, Inc.	Organization Address: 5080 Spectrum Drive STE 1200W, Addison, TX 75001
Person Providing the Reference: Steve Adams	Title: Purchasing Specialist
Phone Number: 972-364-8069	Email address: Steve_adams@concentra.com
Reference <u>Signature</u> & Date:  3/16/17	

The person providing the reference, as identified above, must provide the following information. This person must be a responsible party of the organization for which the work was performed. This person should have comprehensive knowledge about the project and the company's (Offeror) role and responsibilities within the project.

**1. Briefly describe the services provided by the company identified above.**

PJ&A currently provides transcription services for our specialists segment. These services include supporting our provider templates and integration of the finished files into our EMR system.

**2. Rate each of the following concerning this company's performance using the ratings below:**

- S – Strongly Agree/Very Positive
- A – Agree/Positive
- N – Neutral
- D – Disagree/ Negative
- F – Failed

Rating

- S    A. This company ensured the project deliverables were completed on time and within the agreed budget.
- S    B. This company provided the appropriate resources to the project.
- S    C. This company was knowledgeable in providing the services.
- S    D. The business relationship with this company was positive and cooperative, versus negative and adversarial.
- S    E. This company provided open, timely communications, and was responsive to our needs and requirements.
- S    F. I would choose to work with this company again.

Additional Comments:

PJ&A offers exceptional value, consistently high quality and best in class customer service/support.

## Client Reference Form

### Offeror Information

Company Name (Offeror): Perry Johnson & Associates, Inc.	Company (Offeror) Address: 1489 W. Warm Springs STE 110 Henderson, NV 89014
Name of Project: Transcription Services	

### Client Information

Organization Name (Client): Commonwealth of Kentucky/Workforce /OET	Organization Address: 275 E Main St, 2WF Frankfort KY 40621
Person Providing the Reference: Kathy Norton	Title: Office Procedures Coordinator
Phone Number: 502-782-3303	Email address: kathya.norton@ky.gov
Reference <u>Signature</u> & Date: <i>Kathy Norton 3-17-17</i>	

The person providing the reference, as identified above, must provide the following information. This person must be a responsible party of the organization for which the work was performed. This person should have comprehensive knowledge about the project and the company's (Offeror) role and responsibilities within the project.

**1. Briefly describe the services provided by the company identified above.**

Transcribes disputed unemployment insurance hearings filed to Circuit Court.

---

**2. Rate each of the following concerning this company's performance using the ratings below:**

- S – Strongly Agree/Very Positive
- A – Agree/Positive
- N – Neutral
- D – Disagree/ Negative
- F – Failed

Rating

- A. This company ensured the project deliverables were completed on time and within the agreed budget.
- B. This company provided the appropriate resources to the project.
- C. This company was knowledgeable in providing the services.
- D. The business relationship with this company was positive and cooperative, versus negative and adversarial.
- E. This company provided open, timely communications, and was responsive to our needs and requirements.
- F. I would choose to work with this company again.

Additional Comments:

---



---



# CERTIFICATE OF LIABILITY INSURANCE

PERRY-2 OP ID: JM1

DATE (MM/DD/YYYY)  
03/16/2017

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

**IMPORTANT:** If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

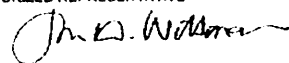
<b>PRODUCER</b> Cranbrook General Underwriters 21 East Long Lake Road #100 Bloomfield Hills, MI 48304 Cranbrook Insurance	<b>CONTACT NAME:</b> PHONE (A/C, No, Ext): 248-335-0000 FAX (A/C, No): 248-335-9850 E-MAIL ADDRESS:													
	<table border="1"> <tr> <th>INSURER(S) AFFORDING COVERAGE</th> <th>NAIC #</th> </tr> <tr> <td>INSURER A : CNA Insurance Companies</td> <td></td> </tr> <tr> <td>INSURER B : Axis Insurance Company</td> <td></td> </tr> <tr> <td>INSURER C :</td> <td></td> </tr> <tr> <td>INSURER D :</td> <td></td> </tr> <tr> <td>INSURER E :</td> <td></td> </tr> <tr> <td>INSURER F :</td> <td></td> </tr> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A : CNA Insurance Companies		INSURER B : Axis Insurance Company		INSURER C :		INSURER D :		INSURER E :		INSURER F :
INSURER(S) AFFORDING COVERAGE	NAIC #													
INSURER A : CNA Insurance Companies														
INSURER B : Axis Insurance Company														
INSURER C :														
INSURER D :														
INSURER E :														
INSURER F :														
<b>INSURED</b> Perry Johnson & Associates 755 W. Big Beaver Rd. #1300 Troy, MI 48084														

**COVERAGES**                      **CERTIFICATE NUMBER:**                      **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR  GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC <input type="checkbox"/> OTHER:			P2075660683	12/01/2016	12/01/2017	EACH OCCURRENCE \$ 1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$ 300,000 MED EXP (Any one person) \$ 5,000 PERSONAL & ADV INJURY \$ 1,000,000 GENERAL AGGREGATE \$ 2,000,000 PRODUCTS - COMPOP AGG \$ 2,000,000 \$
A	<b>AUTOMOBILE LIABILITY</b> <input type="checkbox"/> ANY AUTO <input type="checkbox"/> ALL OWNED AUTOS <input checked="" type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS			P2075660733	12/01/2016	12/01/2017	COMBINED SINGLE LIMIT (Ea accident) \$ 1,000,000 BODILY INJURY (Per person) \$ BODILY INJURY (Per accident) \$ PROPERTY DAMAGE (Per accident) \$ \$
A	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input checked="" type="checkbox"/> RETENTION \$ 10,000			P2075660828	12/01/2016	12/01/2017	EACH OCCURRENCE \$ 10,000,000 AGGREGATE \$ 10,000,000 \$ PER STATUTE    OTH-ER
A	<b>WORKERS COMPENSATION AND EMPLOYERS' LIABILITY</b> <input type="checkbox"/> ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory In NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N	N/A	WC277764734	12/01/2016	12/01/2017	E.L. EACH ACCIDENT \$ 1,000,000 E.L. DISEASE - EA EMPLOYEE \$ 1,000,000 E.L. DISEASE - POLICY LIMIT \$ 1,000,000
B	<b>Professional Liab</b> E&O			MCN-0000430016001	08/31/2016	08/31/2017	Limit 8,000,000

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

<b>CERTIFICATE HOLDER</b> COMMHEO	<b>CANCELLATION</b> SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.  AUTHORIZED REPRESENTATIVE 
--------------------------------------	--

© 1988-2014 ACORD CORPORATION. All rights reserved.