Security made easy.

Recommendations for addressing security vulnerabilities in network printing, scanning and faxing.

NUANCE

Table of contents

Introduction

This white paper provides information on security vulnerabilities associated with networked multifunction devices (MFDs) and nine specific recommendations on how to address these threats. Here are the nine recommendations.

The cost and prevalence of data breaches
The Ponemon Institute defines a data breach as an event in which an individual's name plus a medical record and/or a financial record or debit card is potentially put at risk – either in electronic or paper format.

In May 2014, the Ponemon Institute and IBM released their ninth annual benchmark study on the cost of data breach incidents, *2014 Cost of Data Breach Study: Global Analysis*[1]. Their research concluded the following points:

– The average organizational cost of a data breach is $5.4 million

– The average "cost per record" of a data breach is $201

– Both malicious attacks and negligence were responsible for data breaches[1]

$5.4M
Avg. organizational cost of a data breach

Unfortunately, data breach incidents are a common occurrence, and are on the rise. In its April 2014 report, *Information Security: Federal Agencies Need to Enhance Responses to Data Breaches,* GAO stated that the number of data breach incidents in federal agencies had doubled between 2009 and 2013, to 25,566 per year[2]. The U.S. Department of Health and Human Services (HHS) reports that more than 26 million individuals have been impacted by data breaches since 2009[3].

25,566
Number of data breach incidents in U.S. federal agencies in 2013

The cause of data breaches are avoidable.
83% of respondents in the Healthcare Information and Management Systems Society's *6th Annual Security Survey* (published in February 2014)[4] said the risks that concerned them most were human-related factors such as employees losing devices, unintentionally disclosing information or actively circumventing or interfering with security access controls. In line with the reported incidence of theft, loss and unauthorized access, 83% of respondents had little to no confidence they could detect all loss or theft of patient data.

Here is one example of the financial impact: in 2011, a security breach within TRICARE, the U.S. Department of Defense (DOD) healthcare program, impacted 4.9 million individuals and resulted in a class action lawsuit of $4.9 billion dollars[5].

In the United Kingdom, the Information Commissioner's Office (ICO) show a increase in data breaches as a result of human error. Examining reported incidents between April and June 2013, and the same period for 2014, healthcare organizations top this list with 91 reported breaches increasing to 183—a staggering 101% increase. Accordingly, this continued upward trend has seen total fines issues by the ICO for violations to the data protection act since 2010 in excess of £6.7m[6].

£6.7m +
Total fines issues by the ICO for violations to the data protection act since 2010

During the first three months of 2014, one-quarter of reported data breaches were caused by the accidental loss or destruction of personal data. This is up from 15% for the second half of 2013. Of these, 43% involved confidential information being disclosed in error, primarily through emailing, faxing or posting data to an incorrect recipient[6].

Public Sector and healthcare, primarily NHS, organizations have experienced the greatest number of data breaches between April to June 2013 and April to June 2014, with Public Sector organizations responsible for £4.5m of this. With a 101% rise in breaches in the period from 91 to 183, healthcare organizations top the list for the number reported, followed by local government and education organizations. Central government also experienced a growth of over one-third (38%)[7].

1 2014 Cost of Data Breach Study: Global, Ponemon Institute & IBM, May 2014
2 http://gao.gov/assets/670/662227.pdf
3 http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
4 Healthcare Information and Management Systems Society's 6th Annual Security Survey, February 2014
5 Proofpoint HIPAA Breach Report: An Analysis of HITECH Breach Notifications and Settlements, Q1 2013
6 Information Commissioners Office, December 2014 Statistics
7 Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005 -2014, Center for Media, Data and Society School of Public Policy, Central European University

Convenience, not security, continues to be key when information is being shared with third parties, regardless of the risks. In support of this, only 7% of breaches for the period occurred as a result of technical failings. The remaining 93% were due to human error, poor processes and systems in place, and lack of care when handling data. In fact, to date no fines have been issued due to technical failings exposing confidential data, whereas a total £5.1m has been issued for mistakes made when handling sensitive information like:[7]

– Information being emailed to the incorrect recipient

– Information being sent to the wrong fax number

– Information mailed to the wrong address

– Loss of unencrypted devices

– Paperwork left in decommissioned buildings, on public transport or in the street

Due to strict legislation, the United Kingdom has an enormous number of data breach cases, both paper-based and digital ones. A large portion of these data breaches are a result of carelessness, either on the part of the owners or handlers of personal records. Most cases involve administrative errors or mismanagement, such as not wiping hard drives of old computers offered for re-sale.

Medical records are often treated with extra care, but there are still dramatic cases of data breaches involving confidential medical information. In London, a private clinic decided to contract another company to computerize the paper records they kept on their patients, which contained confidential details on the patients' conditions, names, home addresses and dates of birth. However, after scanning the documents this company sub-contracted other types of work on the files—such as compiling them into a database—to a company in India.

The records were offered for sale there by the firm's local employees, primarily to insurance companies or marketing executives for health products. Hundreds of thousands of personal medical records of UK patients have been outsourced to Indian companies this way, even though under the United Kingdom Data Protection Act it is illegal to send such documents outside the European Union—unless appropriate security is guaranteed.[7]

The Ireland Department of Social and Family Affairs has had several data breaches: the department has lost at least 400,000 records between 1985 and 2014. Some of these incidents involved stolen laptop(s), while others were insider abuse cases. Usually the department lost personal data with sensitive social welfare information, such as social security numbers and other personal records.[7]

Multifunction devices pose a threat.
In its report *Copier Data Security: A Guide for Businesses,* the U.S. Federal Trade Commission (FTC) makes a succinct statement: "Digital copiers are computers". As such, the report goes on to recommend that organizations should incorporate these devices into their information security plans. Digital copiers, also known as multifunction devices (office machines that have the ability to print, scan, copy and fax), have hard drives, embedded firmware, and the ability to communicate with other systems on the network.

7 Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005 -2014, Center for Media, Data and Society School of Public Policy, Central European University

They are susceptible to the same security vulnerabilities that a computer is. Therefore, without the proper security measures in place, the MFD poses a significant risk of sensitive information exposure. The challenge for compliance officers and IT directors is that there are too many information touch points in generating, using and sharing PII. Many of these involve organization's growing use of networked MFDs that copy, print, scan, fax and email.

To further enforce the security threat, acting under provisions of HITECH, the Department of Health and Human Services Office of Civil Rights issued new rules in 2013 that enhance patients' privacy protections, expand individuals' rights to their health information and strengthen the government's ability to enforce the law.

One new development from these rules is that a security risk assessment tool prepared by ONC mentions copiers 15 times as being workstations where PHI (Protected Health Information) must be protected with administrative, physical and technical safeguards that authenticate users, control access to workflows, encrypt data handled on the device and maintain an audit trail of all activity.

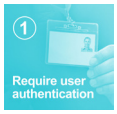
To prevent damaging data breaches, an organization must control and protect both the physical and electronic access points on their MFDs. The following section outlines 10 specific recommendations that organizations must consider to enable a more secure MFD, based on common scenarios that exist in most environments.

Nuance Document Government Solutions (NDGS) consist of a mature Commercial Off-The-Shelf (COTS) product suite consisting of capture, print management and mobile software applications. As a single integrated package, these applications provide a centrally-managed secure MFD capture and print solution.

Implementing a secure multifunction device environment.

Every time a document or form is copied, scanned, printed, faxed or emailed—on either an analog fax machine, digital multifunction device (MFD) or mobile phone or tablet—Personally identifiable information (PII) can be accidentally exposed or intentionally compromised. Paper output can be particularly difficult to track and control, and is not completely eliminated by electronic processes.

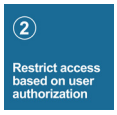
Nuance, a leading provider of secure information capture and output management solutions, has developed a software platform that many government organizations use today to secure their MFD environment. Nuance Document Government Solutions (NDGS) consist of a mature Commercial Off-The-Shelf (COTS) product suite consisting of capture, print management and mobile software applications. As a single integrated package, these applications provide a centrally-managed secure MFD capture & print solution.



Recommendation 1: Require user authentication for auditing purposes.
Authentication enables the auditing, reporting and tracking of user activity as well as various other security features. There is no MFD more unsecure than one that allows anonymous usage, such devices are susceptible to various forms of abuse and can make tracing the source of a data breach or leak virtually impossible.

As a general rule, some form of authentication is recommended over none. Whether via direct Active Directory logon or through a common access card such as Military CAC or PIV, it is crucial to restrict MFD usage through authentication, allowing only authorized staff to access specific devices, network applications and resources.

NDGS support various forms of authentication however single sign on capability via CAC / PIV card using two factor authentication is the preferred method. As alternatives, both Windows NTLM and Active Directory are supported. In the cases where the user environment doesn't allow for those forms of authentication, the solution also supports HID and proximity based technologies and custom authentication via simpler methods such as the use of a PIN.



Recommendation 2: Restrict access based on user authorization.
The MFD must support the restriction of features and capabilities of an authenticated user based on *group membership*. This is crucial from a central management security perspective and enables the MFD to restrict access to functions per security group membership basis.

Network authentication is seamlessly integrated with the document workflow and to ensure optimal auditing and security, documents containing sensitive information are captured and routed to various destinations such as email, folders, fax and line of business applications. Once users are authenticated, the solution also controls what they can and cannot do. It enables or restricts email or faxing and prohibits documents with sensitive information from being printed, faxed or emailed.

The ability to restrict workflows based on active directory group membership allows the solution to granulize access. Just because a user has authenticated into the system, doesn't mean they should have access to every function. This capability ensures that users only have access to those resources on the network that they normally do. Just as a user might not have access to a particular network share as defined by an ACL, they would not be able to scan a document to that location either. Likewise, if a user does not have access to a particular library in SharePoint™, the solution denies access to that library.

NDGS increase employee acceptance and reduce the need for them to find workarounds that bypass security measures. Consider the common action of scanning a document and emailing it to oneself as a simple way to work with it electronically. In a non-compliant workflow, a worker might authenticate at the MFD, select scan as a function and enter their own email address as the destination. Besides requiring upwards of 30 keystrokes, this process is not compliant if the document or sending device are identified by a generic descriptor—BrandNamePrinterScan001.pdf, for example—or the action is not captured in an audit log.

NDGS can make this activity as easy as tap and go. A user walks up to the device, signs in by tapping their proximity card against the reader and then chooses scan to my email from a list of pre-defined and pre-authorized workflows displayed on the MFD's control panel. It's a faster, simpler, error-free process and—with the activity audited as to user, device, action, email address, date and time and document metadata.

Recommendation 3: Centrally audit all network activity.
Auditing allows the MFD to store tracking information in a database. In the event of a data breach, this capability will allow you to easily track down which device was the source of the breach, tell you who the authenticated user was and where the data was sent. By enabling auditing, NDGS records all metadata passed through the system. Auditing enables you to track down a specific event, such a scan or print by a specific user. You can also produce reports that provide an overview of scanning activity by device or department. You can track as little or as much as

Network authentication is seamlessly integrated with the document workflow and to ensure optimal auditing and security, documents containing sensitive information are captured and routed to various destinations such as email, folders, fax and line of business applications.

you want. The solution can store all tracking data via SQL database, including the warehousing of all printed and scanned images by retention period.

Compliance security standards require most businesses to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. By building an audit trail of all copy, print, scan, email and fax activity at every networked MFD, including paths to document images, using the right kind of advanced capture and output solution will bring use of these devices into compliance.

Just as important, reviewing the audit log helps organization's to identify a breach, take prompt corrective action, issue the necessary notifications and avoid the cost of fines. In the case of healthcare for example, correcting a violation within 30 days of acquiring "actual or constructive" knowledge of it provides an "affirmative defense" and immunity against HIPAA's civil monetary penalties.

Recommendation 4: Encrypt data to/from MFDs. Modern MFD's often contain hard drives which are used to cache scanned document images and printed documents. As a result, all non-volatile memory media used to cache data on the device should employ a method of data erasure to protect data in accordance with NIST Special Publication 800-88 in the United States.

The Cryptographic Module Validation Program (CMVP) is operated jointly by the NIST's Computer Security Division and the Communications Security Establishment (CSE) of the Government of Canada. The use of validated cryptographic modules is required by the U.S. Government for all unclassified uses of cryptography. The Government of Canada also recommends the use of FIPS 140 validated cryptographic modules in unclassified applications of its departments.

The Communications Electronics Security Group (CESG) is the branch of Government Communications Headquarters (GCHQ) that works to secure the communications and information systems of the government and critical parts of the U.K. national infrastructure. CESG provides the CESG Assisted Products Service or CAPS. CAPS enables products to be cryptographically verified by CESG to U.K. Government cryptographic standards and formally approved for use by the U.K. Government and other appropriate organizations.

In Australia, the Defense Signals Directorate (DSD) has the responsibility for cryptography.

FIPS PUB 140-2 Compliance
Nuance Document Government Solutions (NDGS) meet the security requirements for cryptographic modules defined by Federal Information Processing Standard (FIPS) Publication 140-2 (FIPS PUB 140-2) by leveraging specific accredited encryption methods for both data in motion (DIM) and data at rest (DAR). Where SSL and disk encryption are mentioned in this paper, it is with respect to the utilization of (at minimum) a FIPS PUB 140-2 certified cryptographic algorithm.

Data in Motion: Data in Motion applies to communication between multi-function devices (MFDs) and the NDGS. Data in Motion is transferred over SSL with up to 2048-bit encryption. Supported MFDs can utilize FIPS 140-2 accredited Open SSL FIPS Object Modules, including AES (Certs. #1884, #2116, #2234, #2342, #2394 and #2484) and RSA (Certs. #960, #1086, #1145, #1205, #1237 and #1273). Reference, NIST, Cert #1747

Compliance security standards require most businesses to implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. By building an audit trail of all copy, print, scan, email and fax activity at every networked MFD, including paths to document images, using the right kind of advanced capture and output solution will bring use of these devices into compliance.

Data at Rest: Data at Rest applies to jobs held in the solution's print queue and scan jobs held in the solution's temporary working files. Encryption is enabled directly on the Windows Operating System (OS) and not within the Nuance software application. Data at rest is stored using up to dual layer data encryption utilizing two Windows operating system (OS) encryption methods: Windows Encrypting File System (EFS) (NT File System) and BitLocker Drive Full-volume Encryption (Whole Disk). Both methods rely on FIPS 140-2 validated cryptographic libraries. Reference: NIST, Cert #1054

5 Only release print jobs to authorized personnel

Recommendation 5: Only release print jobs to authorized personnel.
In order to avoid exposing documents with PII when printed, secure printing requires that users authenticate at the device before documents are released. The device must print only those documents that are associated with the authenticated user, and the print job must not be stored on the device prior to printing. Documents should be stored on the print server in a pending queue prior to printing where a FIPS PUB 140-2 cryptographic algorithm is utilized to protect the data at rest. During printing, the Internet Printing Protocol (IPP) should be used to transmit print jobs in an encrypted state.

There is a high cost associated with handling sensitive data exposure and security breaches. A Department of Veterans Affairs (VA) Office of Inspector General (OIG) in April recorded a common incident that could have been prevented with pull printing:

VA OIG reported approximately 8,000 such breaches in calendar year 2013. The VA calculated a cost of $37.50 per individual veteran affected, to cover notification, one year of credit monitoring services and identify theft insurance, and other legal expenses.[9]

In addition to the improved security, regulatory compliance can be supported through the implementation of pull printing. For U.S. federal agencies, integrating a pull printing capability with government-issued Common Access Cards (CAC) or Personal Identification Verification (PIV) cards, supports compliance with Homeland Security Presidential Directive 12 (HSPD-12), by requiring two-factor authentication to access network data (in this case a print stream).[10]

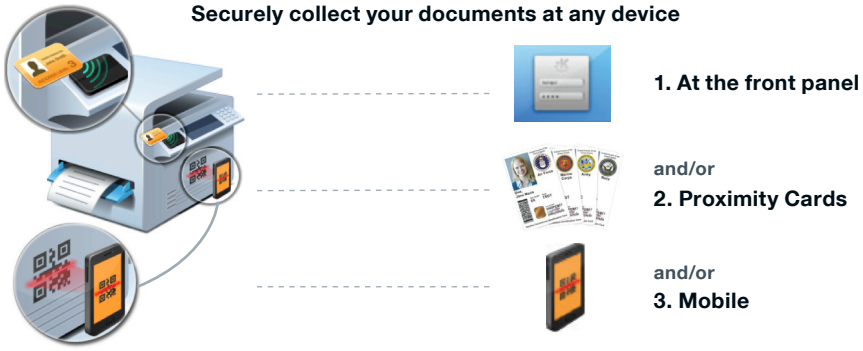
Sample Common Access Cards

"**Incident Summary**—
The Privacy Officer (PO) found a patient appointment list in the patient computer lab of the Mental Health Building. The list was printed by My HealtheVet (MHV) staff. While assisting a Veteran with MHV enrollment, the staff member forgot the appointment list in the computer lab. There were 55 patient names on the list. The patient appointment list included the appointment date and time, clinic name, and the patients' last name. The PO removed the appointment list and secured it."[8]

8 "Monthly Report to Congress of Data Incidents", U.S. Department of Veterans Affairs, Office of Information Security, Risk Management and Incident Response Team, April 2013
9 "Courier Services for the Fort Harrison VA Medical Center and surrounding clinics", VA259-14-R-0082, March 2010
10 Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors

Nuance Document Government Solutions provide a secure, server-based pull printing capability that enables users to submit print jobs from both Windows and mainframe applications. The solution holds the users' queues on a server, as a result users are able to release their print job from any integrated networked MFD/printer. The solution also supports an integrated single sign-on with CAC and PIV cards. Workers can even use a mobile device to activate "touch free" release of the document.

Through the solution's authentication process, the provider does not allow access to a print device until after a user's credentials have been verified. Once users are authenticated, the solution controls what users can and cannot do.



Recommendation 6: Implement rules-based printing. Secure access begins with user identification at the device (**authentication**) and then control as to what each user can or can't do (**authorization**). To mitigate the risk of documents containing PII from getting into the wrong hands, rule-based printing requires a user to be physically present (e.g., enter a PIC/PIN, swipe a proximity or smart card) to initiate a print job. Not only does this enhance security and prevent unauthorized users from accessing printed PII, but it also reduces the number of print jobs not retrieved, thereby also reducing consumable resource utilization and printing costs.

NDGS integrates print security with organizations' existing access control solutions. The solution can restrict access to devices by role, applications, time, etc. NDGS control and track what documents each user can access and securely distribute ensuring PII is controlled before it is ever gets to its intended destination. Through the solution's authentication process, the provider does not allow access to a print device until after a user's credentials have been verified. Once users are authenticated, the solution controls what users can and cannot do.

It enables or restricts scan to email or faxing, permits or places limitations on color printing, and prohibits documents sensitive information from being printed, faxed or emailed.

Recommendation 7: Enforce trusted network destinations. Nuance Document Government Solutions (NDGS) allows MFD's to validate metadata entered by users. For example, a Veterans Affairs hospital may enforce the validation of phone numbers entered at the MFD in order to prevent faxing to untrusted numbers. A government Office of Inspector General may require that email addresses

be validated so that documents scanned at an MFD cannot be delivered to non-government email addresses.

Scan-to-email example: Your security environment may not allow scanning certain types of content to email. For all other cases, the following is recommended.

– Consider validating all email addresses. For example, set the solution to allow only the sending of emails to addresses in Active Directory or the GAL. Alternatively, consider validating the email address domain, so that emails can only be sent within your organization, and so that they never leave your network.

– Consider workflows which send email only to specific addresses, such as a trusted destination, or the authenticated user's own inbox.

Recommendation 8: Monitor and control PII activity.
Nuance Document Government Solutions (NDGS) automatically enforce security policies by filtering outbound communications and intercepting documents, to proactively prevent PII from leaving the organization and render misdirected or intercepted information unreadable to unauthorized users. Simultaneous monitoring and auditing of sensitive information in documents ensures PII is controlled before it ever gets to its intended destination.

Recommendation 9: Implement network faxing.
Many organizations still perform a significant amount of faxing as a normal consequence of their day to day operations in respective industries. Commonly this involves faxing documents, even those with PII, over unsecured lines. As a result the following should be strongly considered.

– Eliminate direct analog faxing by adopting a centralized fax server solution, particularly one that retains a copy of the outbound fax via configurable retention period.

– Consider validating fax numbers against a white list in NDGS. If this is unfeasible due to the need for ad-hoc faxing, consider validating fax numbers by regular expression to ensure that only area codes within your state or region are used. At a minimum, consider blocking international faxes either at the panel of the device with NDGS or via fax server backend.

Additional Recommendation: Standardize and integrate network scanning.
The scanning of a file to a network folder is the most common, and unfortunately, usually the type of workflow that is left most unsecure. For this reason, it is important to standardize and integrate network scanning.

– Avoid allowing users to scan to a general folder. Not only can these folders become a cluttered dumping ground for various types of materials, they also expose everyone's work to each other.

– Use NDGS to route documents to the following locations instead
  - The authenticated user's home directory
  - A network share protected by ACL
    - Verify permissions for the authenticated user

Nuance Document Government Solutions (NDGS) automatically enforce security policies by filtering outbound communications and intercepting documents, to proactively prevent PII from leaving the organization and render misdirected or intercepted information unreadable to unauthorized users.

– Consider a secured SharePoint library instead, such as an authenticated user's "My Site". Integrate network devices with document management systems. Document managements systems come in a variety of flavors, but they tend to be the most secure destinations to scan into. They often support the consumption of content via SSL web service, and allow for impersonation of an authenticated user so that a service account does not have to serve as a proxy.

- Use NDGS to impersonate the user. This ensures that the user's view of the DMS is their own. This is important because document management systems can have complex ACL permission models that are independent of Active Directory.
- Always use SSL when transmitting documents to your DMS of choice, and ensure that data at rest is protected.

Conclusion

To prevent damaging data breaches, an organization must control and protect both the physical and electronic access points on their MFDs. The monetary penalties, settlements and costs for failing to secure PII are increasing and there are simply too many touch points that create risk in sharing PII, most of these involving the technologies that organizations are counting on to run their business—especially smart devices that copy, print, scan, fax and email.

NDGS enable the compliant exchange of PII by adding a layer of security and control to paper-based and electronic processes. Transparently applying automated security techniques that cannot be circumvented, NDGS authenticates users, controls access to workflows, encrypts data, validates network destinations, monitors and controls all documents containing PII and builds and maintains an audit trail of all user activity. As a result, NDGS minimizes the manual work and decisions that invite human error, mitigates the risk of non-compliance and helps companies avoid the fines, reputation damage and other costs of compliance breaches.

Thousands of organizations nationwide already depend on Nuance to help secure data at rest, data in motion and data in use. Beyond meeting institutions' requirements today, Nuance will continue to evolve, keeping pace as threats, vulnerabilities, breaches and the best practices for responding to them change in the future.

Appendix A: Glossary of Terms

Glossary of Terms	
FIPS PUB 140-2	The Federal Information Processing Standard (FIPS 140) is published by the National Institute of Standards and Technology (NIST) and is publically accessible here. It defines the standard that all Federal organizations must conform to when cryptographic algorithms are used to protect sensitive data.
FIPS PUB 201-1	Commonly known as the Homeland Security Presidential Directive 12 (HSPD-12), the Federal Information Processing Standard (FIPS 201) is published by the National Institute of Standards and Technology (NIST). FIPS PUB 201-1 and FIPS PUB 201 PIV II encompass the requirements needed to meet HSPD-12 compliance and are publically accessible here and here respectively.
DoD M 5200.01 VOL 1-4	Authorized under DoD Directive 5143.01, the Department of Defense Manual 5200.01 is composed of four volumes which define the guidelines for the protection of classified and unclassified information and is accessible via Defense Technical Information Center (DTIC) website here: VOL, 1, 2, 3, 4.
Distributed Capture	A function of the NDGS platform that allows documents to be captured from virtually any source be it a folder, inbound email, web or internet based submission (HTTPS, SFTP, etc.), desktop client, multifunction devices and any twain compatible desktop scanner.
Distributed Processing	A function of the NDGS platform which is akin to the core concepts of distributed computing. Enables the delegation, control and parallel processing across multiple local server CPU resources and across multiple NDGS servers
Distributed Delivery	A function of the NDGS platform that allows documents to be routed to virtually any target, be it a network folder, outbound email, web or internet based transmission (HTTPS, SFTP, etc.), database, document management system or custom built repository.
Virtual Print Queue	A function of the NDGS platform that emulates a standard Windows™ Server based print queue with the special ability to hold a print stream and all associated user metadata until a time at which it is released for printing on commanded, via trigger or by defined business rule.

Appendix B: Nuance Product Certifications

Authority to Operate and Certificates of Net Worthiness

The U.S. Army Network Enterprise Technology Command (NETCOM) has awarded an enterprise level *Certificate of Net Worthiness* (CoN) for the NDGS platform

Cert #	CoN Type	Expiration
201315936	Enterprise	8/9/2016

In addition, entities within the Department of Defense have granted the NDGS platform an *Authority to Operate* (ATO) to include:

Entity	Program	Network / Program Scope
U.S. Navy	Enterprise Scan-to-File	NMCI
U.S. Marine Corps	Enterprise Scan-to-File	NMCI
U.S. Military Health System (MHS)	HAIMS Information System	DHIMS
Office of the Assistant Secretary of Defense Health Affairs (OASD HA)	HAIMS Information System	DHIMS

Research:

Monthly Report to Congress of Data Incidents", U.S. Department of Veterans Affairs, Office of Information Security, Risk Management and Incident Response Team, April 2013

Courier Services for the Fort Harrison VA Medical Center and surrounding clinics, VA259-14-R-0082, March 2010

Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors

2014 Cost of Data Breach Study: Global, Ponemon Institute & IBM, May 2014

Healthcare Information and Management Systems Society's 6th Annual Security Survey, February 2014

http://gao.gov/assets/670/662227.pdf

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

http://www.inforisktoday.com/tricare-breach-affects-49-million-a-4105/op-11

http://www.forbes.com/sites/ciocentral/2013/02/07/the-hidden-it-security-threat-multifunction-printers/

http://www.pcworld.com/article/239456/a_hidden_security_threat_beware_the_office_multifunction_printer.html

About Nuance Communications, Inc.
Nuance Communications is reinventing the relationship between people and technology. Through its voice and language offerings, the company is creating a more human conversation with the many systems, devices, electronics, apps and services around us. Every day, millions of people and thousands of businesses experience Nuance through intelligent systems that can listen, understand, learn and adapt to your life and your work. For more information, please visit nuance.com.

NDI-6 SecurityMadeEasy-WP MAR 2015