PROSHRED SECURITY

INFORMATION DESTRUCTION AT YOUR DOOR

Overview

for

SAN DIEGO ARMA

By: Todd M Hoover

WHO ARE WE?

PROSHRED® Security

PROSHRED® Security

WHAT DO WE DO?

PROSHRED® Security

- Secure document retention equipment
  - Bins, Executive Consoles & PDCs
  - Fully compliant with all laws and regulations
- Confidential and Secure Service Process
  - Hand's off approach
  - Uniformed and ID'd Customer Service Professionals with extensive criminal background checks, drug screening, and fully insured & bonded employees
- Shredded material can not be reconstructed
  - Meets requirements of 5/8 inch by 2 inch
  - Combined with other client's destroyed documents prior to recycling
  - A Certification of Destruction provided after each service visit

PRIVACY AND INFORMATION MANAGEMENT LEGISLATION:

- Fair and Accurate Credit Transactions Act (FACTA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLBA)
- Identity Theft Penalty Enhancement Act (ITPE)
- The Economic Espionage Act (EEA)
- State Legislation

DOCUMENT DESTRUCTION AT YOUR DOOR

- ISO 9001:2008 certified
- Certified, uniformed and bonded
- Ensures legislation compliance
- Certificate of Destruction
- Trusted business partner

CERTIFIED PROCESS

PROSHRED® Security

NSF ISR

Certificate of Registration

This certifies that the Quality Management System of

Proshred San Diego

7377 Convoy Court
San Diego, California, 92111, United States

has been assessed by NSF-ISR and found to be in conformance to the following standard(s):

ISO 9001:2015

Scope of Registration:
Provision of on-site information security and destruction

ANAB ACCREDITED ISO/IEC 17021 MANAGEMENT SYSTEMS CERTIFICATION BODY

IAF MEMBER OF MULTILATERAL RECOGNITION ARRANGEMENT

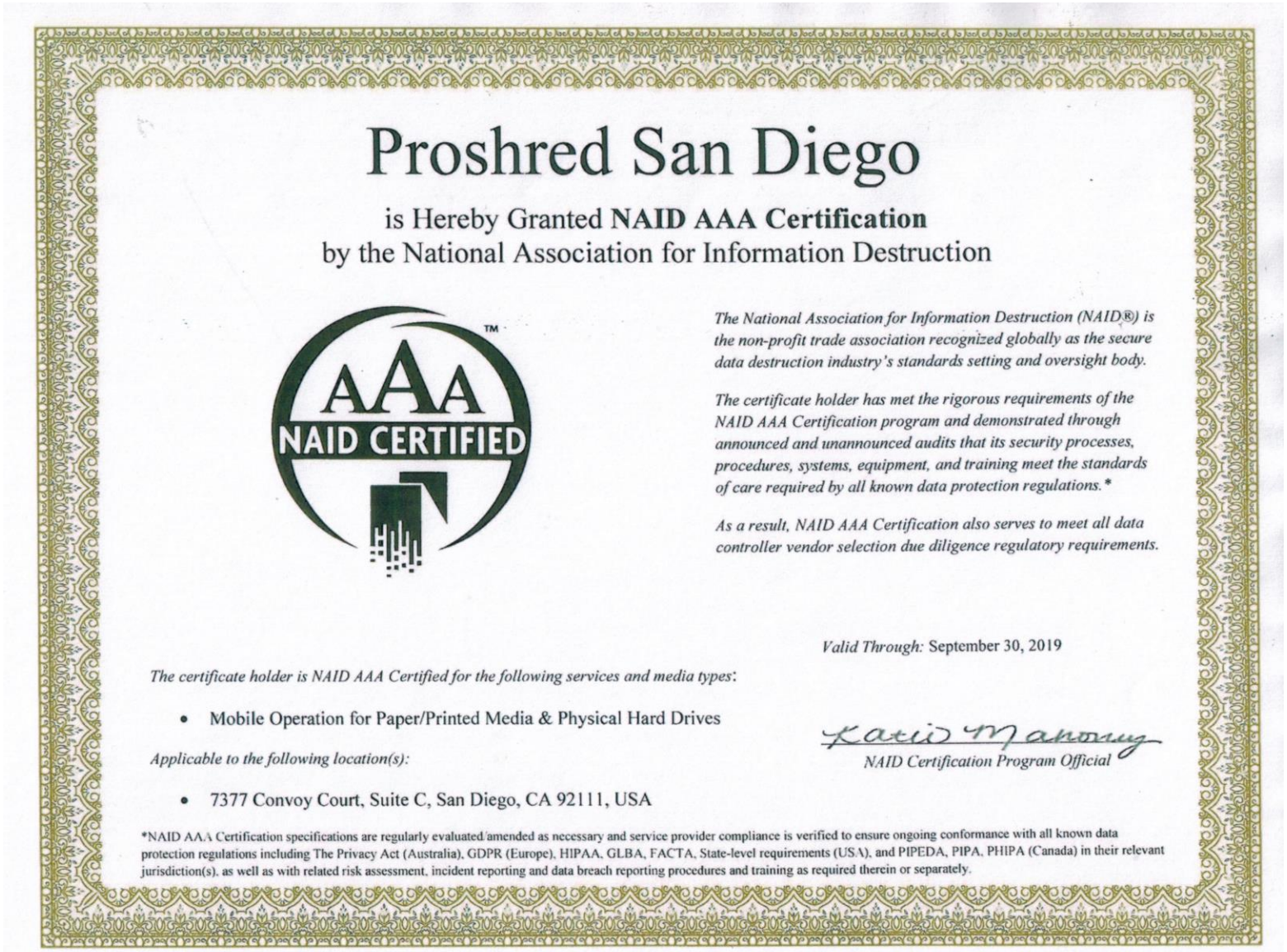
Certificate Number:	6H321-IS14-C0074096
Certificate Issue Date:	18-JUN-2018
Registration Date:	01-JUN-2017
Expiration Date *:	31-MAY-2020

Carl Blazik,
Director, Technical Operations &
Business Units, NSF-ISR, Ltd.

NSF International Strategic Registrations
789 North Dixboro Road, Ann Arbor, Michigan 48105 | (888) NSF-9000 | www.nsf-isr.org

Authorized Registration and /or Accreditation Marks. This certificate is property of NSF-ISR and must be returned upon request.
*Company is audited for conformance at regular intervals. To verify registrations call (888) NSF-9000 or visit our web site at www.nsf-isr.org

PROSHRED® Security



Proshred San Diego

is Hereby Granted **NAID AAA Certification**
by the National Association for Information Destruction

AAA NAID CERTIFIED

The National Association for Information Destruction (NAID®) is the non-profit trade association recognized globally as the secure data destruction industry's standards setting and oversight body.

*The certificate holder has met the rigorous requirements of the NAID AAA Certification program and demonstrated through announced and unannounced audits that its security processes, procedures, systems, equipment, and training meet the standards of care required by all known data protection regulations.**

As a result, NAID AAA Certification also serves to meet all data controller vendor selection due diligence regulatory requirements.

Valid Through: September 30, 2019

The certificate holder is NAID AAA Certified for the following services and media types:

- Mobile Operation for Paper/Printed Media & Physical Hard Drives

NAID Certification Program Official

Applicable to the following location(s):

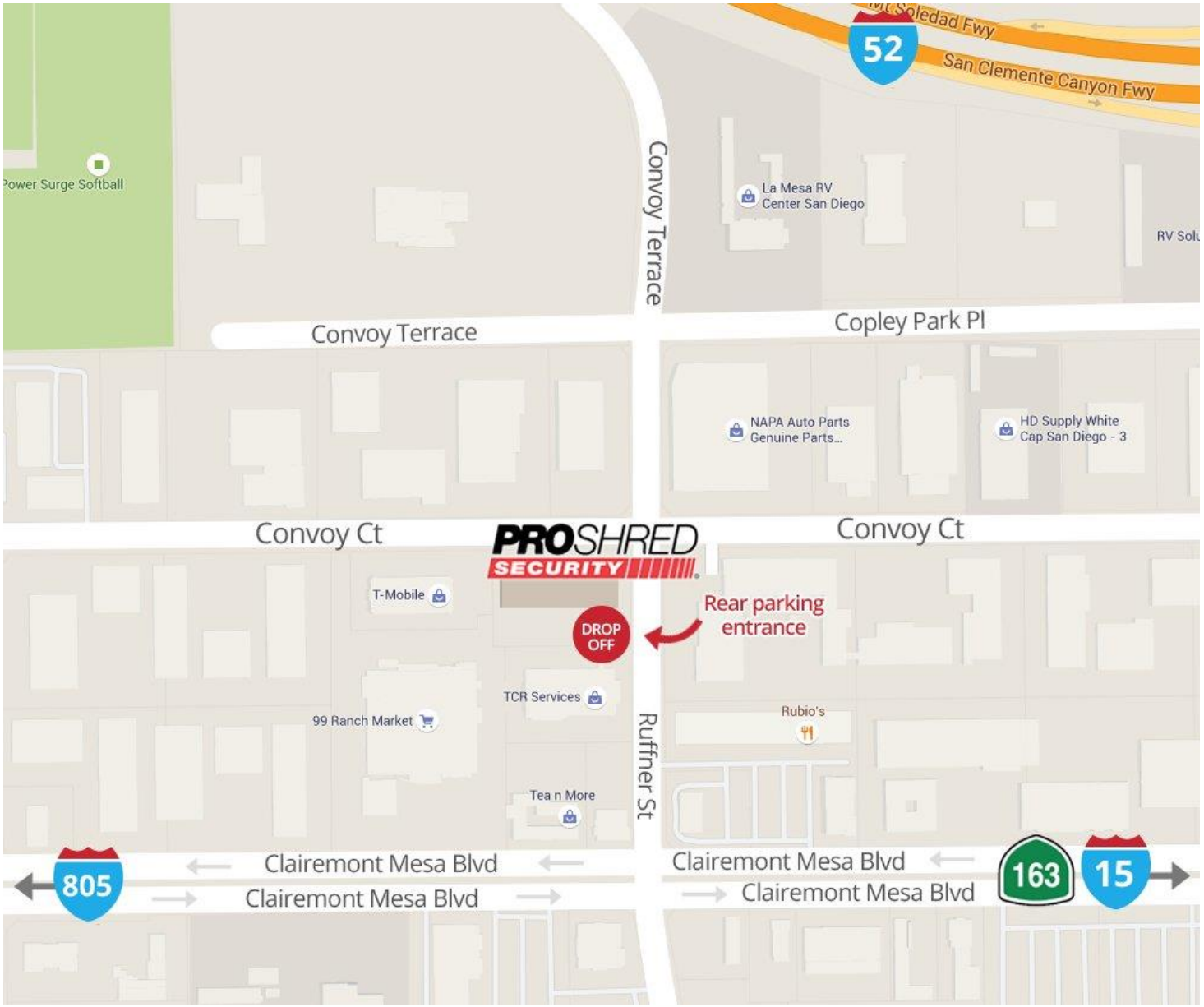
- 7377 Convoy Court, Suite C, San Diego, CA 92111, USA

*NAID AAA Certification specifications are regularly evaluated/amended as necessary and service provider compliance is verified to ensure ongoing conformance with all known data protection regulations including The Privacy Act (Australia), GDPR (Europe), HIPAA, GLBA, FACTA, State-level requirements (USA), and PIPEDA, PIPA, PHIPA (Canada) in their relevant jurisdiction(s), as well as with related risk assessment, incident reporting and data breach reporting procedures and training as required therein or separately.

SCHEDULED SHREDDING

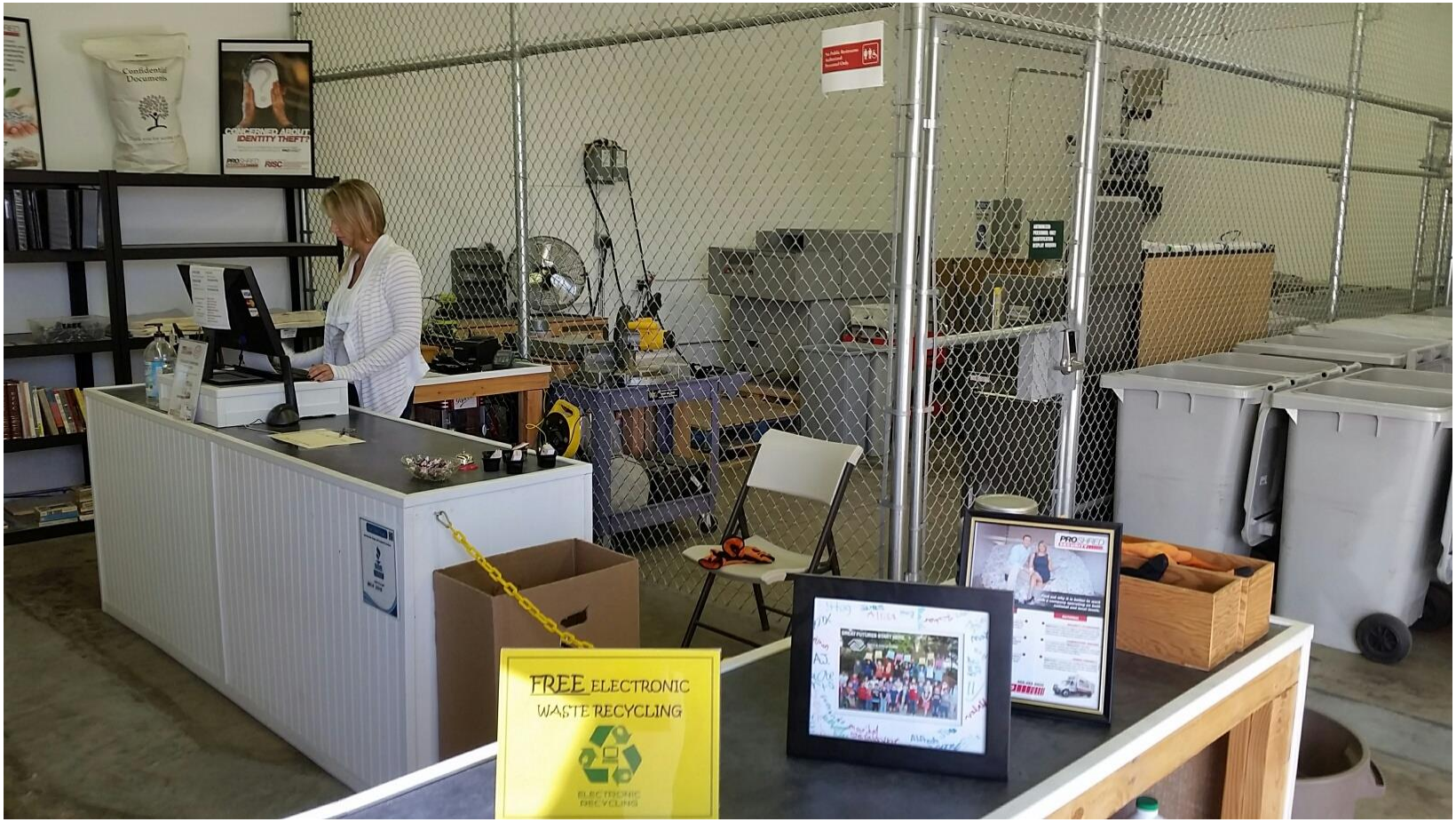
PURGE SHREDDING

PROSHRED® Security



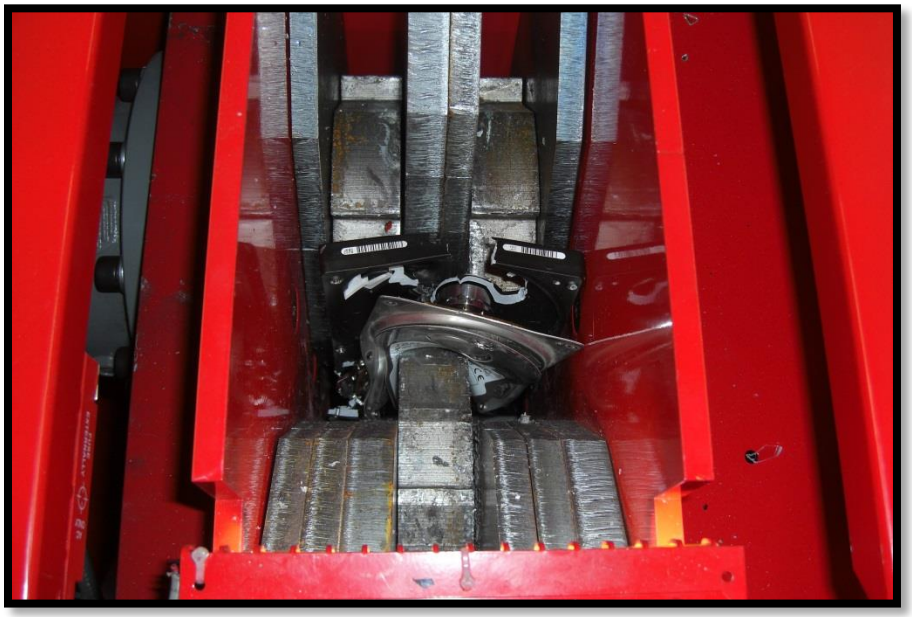
PROSHRED® Security

WITNESSED SHREDDING



WHAT ARE THESE?

COMPUTER HARD DRIVE SHREDDING



COMPUTER RECYCLING

PROSHRED® Security

SHRED CANCER
NATIONWIDE EVENT

AMERICAN INSTITUTE for CANCER RESEARCH®

IS RECYCLING SECURE?

ARE THESE BINS IN YOUR OFFICE?

WHO EMPTIES THEM, WHERE ARE THEY EMPTIED?

PROSHRED® Security

HOW WOULD YOU FEEL IF THESE WERE YOUR COMPANIES DOCUMENTS ?

SAN DIEGO RECYCLING CENTER

DUMPSTER DIVING IS A BUSINESS

LEADING METHOD USED IN OBTAINING PERSONAL INFORMATION

STREET VALUE

$1 to $6 – Stolen Credit Card

$14 to $18 – Identity (US Bank Account, Credit Card, DOB & Government ID)

$50 – Stolen Medical Identity

IS YOUR BUSINESS SECURE?

THE MAJORITY OF SECURITY BREACHES

ARE CAUSED BY

?

EMPLOYEE NEGLIGENCE

EMPLOYEE ERROR

MALICIOUS INTENT

97% OF BREACHES ARE AVOIDABLE WITH SIMPLY OR INTERMEDIATE CONTROLS

95% OF BREACHES OCCUR IN SMALL BUSINESSES OF 100 EMPLOYEES OR LESS

HAVE YOU INVESTED MONEY IN :

- EXTRA LOCKS ON DOORS
- CARD OR FOB CODED DOORS
- SECURITY SYSTEMS
- MONITORED SECURITY SYSTEMS
- SECURITY CAMERAS
- MULTIPLE LINES OF INSURANCE

HOW MANY OF YOU IN THIS ROOM HAVE A WRITTEN POLICY THAT EXPLAINS TO YOUR EMPLOYEES HOW TO HANDLE, STORE AND DISPOSE OF CONFIDENTIAL INFORMATION?

WHY?

85% OF SMALL BUSINESS OWNERS BELIEVE A DATA BREACH IS UNLIKELY

PROSHRED® Security

Wave House, San Diego, CA:

A former employee allegedly stole hundreds of applications and contracts while employed between May 2010 and January 2012. He is accused of making at least $40,000 in online purchases and pleaded not guilty to 17 counts of identity theft and one count each of grand theft, false personation, and a drug charge. He faces 15 years and eight months in prison if convicted.

Millimaki Eggert, LLP, San Diego, CA:

The office burglary of two password-protected laptops resulted in the exposure of sensitive client information. Names, Social Security numbers, and addresses may have been involved.

MILLIMAKI
▲ EGGERT LLP
CERTIFIED PUBLIC ACCOUNTANTS

[Name]
[Address]
[City, State Zip]

Dear Client:

We are writing to notify you of an incident that may affect the security of your personal information.

On April 27, 2013, an unknown individual(s) burglarized Millimaki Eggert's San Diego, California office and stole, among other things, two password-protected laptops containing sensitive information. We reported the theft to local law enforcement, and law enforcement's investigation into this incident is ongoing. We commenced an internal investigation into the incident to determine what data was stored on each laptop at the time of the theft. We retained privacy and data security legal counsel to assist with its investigation of, and response to, this incident. Although this investigation is ongoing, we determined that your Name, Address, Social Security Number, Bank Account Number and Date of Birth were stored in a password-protected software program on one of the laptops at the time of the theft.

PROSHRED® Security

Security Self-Assessment

Are you aware of privacy laws that relates to your business?	Yes □ No □
Who in your office is responsible for maintaining compliance?	
Who is trained for an information breach?	
Have your employees been trained on privacy legislation?	Yes □ No □
Are you aware of the penalties for failing to comply?	Yes □ No □
Does your office shred confidential documents?	Yes □ No □
What are you currently shredding?	Yes □ No □
a. HR documents	Yes □ No □
a. R&D files	Yes □ No □
a. Sales records	Yes □ No □
a. Legal files	Yes □ No □
a. Leases/ contracts	Yes □ No □
a. Medical Records	Yes □ No □
a. Purchasing records	Yes □ No □
a. Tapes	Yes □ No □
a. X-Rays	Yes □ No □
a. Disks/ hard drives	Yes □ No □
a. Everything	Yes □ No □
Does your organization have a policy in place to address the storage and destruction of confidential data? If so,	
a. Who is accountable for policing it?	
a. Is there a process for storage devices: discs drives, etc.?	Yes □ No □
a. Who is responsible for shredding documents?	

Who decides what is confidential and non-confidential?	
Are documents saved in open, unsecured areas of the office?	Yes □ No □
If documents are shredded, how is shredded material disposed?	
Would you worry if any trash or recycling went public?	Yes □ No □
Do visitors walk through the office unescorted?	Yes □ No □
Do you separate confidential and non-confidential information?	Yes □ No □
Do any employees work remotely?	Yes □ No □
Are documents stored offsite?	Yes □ No □
Does your organization archive using imaging, scanning, etc.?	Yes □ No □
Do you have signage regarding information-security?	Yes □ No □
Do all departments have access to containers?	Yes □ No □
Do you do semi-annual process reviews with your shredding contractor to ensure your process addresses current risk levels?	Yes □ No □
Is your shredding contractor certified by ISO for quality and satisfaction standards, and by NAID AAA for compliance?	Yes □ No □
Can your current provider train on document security risks?	Yes □ No □
Are confidential documents shredded onsite or offsite?	On-Site □ Off-site □
Can you demonstrate that you have taken reasonable actions to protect private information?	Yes □ No □
On a scale of 1 to 10, how comfortable are you that your information-security processes are compliant and sufficient?	1 2 3 4 5 6 7 8 9 10

SAMPLE TEMPLATE

[COMPANY NAME]

INFORMATION DESTRUCTION INSTRUCTION POLICY

1.0 Introduction and Overview

1.1 The Information Destruction Policy

It is the policy of [COMPANY NAME] to 1) protect the Personal Information of our clients and employees, 2) comply with state and federal regulations to protect/destroy such information when discarded, and 3) protect Competition-Sensitive Information. This document implements the official Information Destruction Policy of (COMPANY NAME) and is intended to provide direction to all employees regarding acceptable methods for destroying discarded information in order to protect our firm, its clients and employees.

Compliance with the policy and with the requirements herein when discarding or destroying information owned or maintained by (COMPANY NAME) is considered a condition of employment.

Failure to adhere to the requirements within this Information Destruction Instruction Manual could result in disciplinary action, dismissal, civil proceedings, regulatory penalties, and/or legal prosecution.

1.2 Policy Development, Implementation and Oversight

1.2.1 Policy Development

The **Management Committee** is responsible for the development and amendments to the organization's Information Destruction Policy. The policy shall be reviewed annually, or at anytime that there is substantive change in regulatory requirements, or under any circumstance that may otherwise provide cause for such a review.

1.2.2 Policy Approval

The **General Manager, upon advice from the Legal Council,** is responsible for the final approval of the Information Destruction Policy or any modifications made to it.

1.2.3 Orientation & Training

The **Office Manager, serving as the Compliance Officer,** is responsible for implementation and documentation of the orientation of employees to the Information Destruction Policy. This training may involve the participation of outside contractors hired to provide information management or destruction services.

1.2.4 Contracting/Purchasing

The **Office Manager** is responsible for the contracting of any third party (Approved Service Provider) to provide information destruction services.

1.2.5 Compliance Auditing/Review

The **Office Manager** is responsible for auditing employee compliance with the Information Destruction Policy on a daily basis, as well as documenting and retaining a record of violations of the policy.

1.3 Employee Orientation/Training

1.3.1 Orientation/Training

Upon hiring, and whenever updated, all employees shall 1) be properly oriented on the Practice's information destruction procedures, 2) be issued a copy of the Information Destruction Instruction Manual (IDIM) and 3) execute the appropriate acknowledgement prior to handling ANY information.

1.3.2 Acknowledgement

Upon completion of initial and ongoing orientation, employees shall sign the *Information Destruction Program Awareness Acknowledgement* verifying their understanding of, and their agreement to comply with, the requisite policies and procedures contained in the IDIM.

1.4 Information Destruction Policy Directory

Employees should direct all questions regarding compliance with the Information Destruction Policy to the **Office Manager**.

Employees are required to inform the **Office Manager** if at any point they become aware of a potential risk of unauthorized access to patient information or any violation of the IDIM.

In the event that the **Office Manager** is unavailable or is unresponsive, employees should direct questions or report threats and violation to **[_____ at (include contact information)].**

The organization will not engage in or tolerate any discrimination, retribution, punishment or persecution of any employee who exposes any potential data breach risk or violation to the Information Destruction Policy or the IDIM.

2.0 Information Destruction Procedures

All discarded Information-Bearing Media will be destroyed prior to disposal. The Practice relies on an Approved Service Provider, duly contracted by the Office Manager (only) for all media destruction.

2.1 Paper Media

Paper Media refers to all types of paper business communications bearing information, including but not limited to forms, notes, memos, messages, correspondence, transaction records and reports.

2.1.1 Authorization for Destruction of Paper Media

2.1.1.1 Paper Media (Incidental Records)

No approvals or authorizations are required for the destruction of Paper Media that is NOT subject to the organization's current Records Retention Schedule or otherwise a part of, or integral to, a patient's medical record.

2.1.1.2 Paper Media (Retained/Controlled)

Employees shall NOT destroy or otherwise discard any Paper Media that could be construed as being subject to the organization's current Records Retention Schedule or otherwise be a part of, or integral to, a patient's medical record without written authorization directly from the **Office Manager**.

If there is any question as to whether or not Paper Media is subject to the organization's current Records Retention Schedule or otherwise a part of a patient's medical record, the employee should seek instruction from the **Office Manager**.

2.1.2 Securing Paper Media Prior to Destruction

Incidental Paper Media intended for disposal/destruction, should be collected in a designated Deskside Collection Container at the employee's workstation. At minimum, all employees will deposit the contents of the Deskside Collection Container into the Centralized Secure Collection Containers at the conclusion of each shift prior to leaving for the day.

2.2 Other Media Disposal

Other than Incidental Paper Media, employees are prohibited from discarding any other type of Information-Bearing Media, including but not limited to Magnetic Tape &/or Optical Media (CD/DVD), PDAs/Mobile Phones, Computers, Hard Drives, Stored Records, or Medical Equipment.

In the event an employee has the need to dispose of any Information-Bearing Media other than Incidental Paper Media, the Office Manager will authorize and arrange for its proper destruction.

3.0 Qualifications and Selection of an Approved Service Provider

(COMPANY NAME) relies on a properly contracted Approved Service Provider for destruction services. Only the **Office Manager** has the authority to select and contract with an Approved Service Provider.

4.0 Policy Compliance

4.2 Auditing Internal Compliance

The **Office Manager** shall be responsible to audit compliance with the Information Destruction Policy and the IDIM on a daily basis.

4.3 Litigation Hold/Stop Destruction Order

In certain circumstances, it may be necessary to stop the destruction of records related to a specific subject. These include litigation, reasonable expectation of litigation, and internal or regulatory audits. There are potentially very serious negative consequences to the organization for destroying information or records subject to these circumstances.

In the event of such circumstances arising, the **Office Manager** will issue a *Stop Destruction Order* to each departmental supervisor with specific instructions.

PROSHRED® Security

- ***"Every business, whether large or small, must take reasonable and appropriate measures to protect sensitive consumer information, from acquisition to disposal. This agency will continue to prosecute companies that fail to fulfill their legal responsibility to protect personal information."***

Deborah Platt Majoras, Chairman, FTC
December 18, 2007

PROSHRED® Security

At Proshred Security of San Diego our goal is to exceed your expectations in every aspect of service and quality; this is the cornerstone of our business both locally and nationally!