Personally Identifiable Information (PII)
and
Volunteer Examiners

by AA3RR

Introduction. As volunteer examiners, we collect several types of personal information from the people we serve. For purposes of this document, the terms "personal information" and "personally identifiable information or PII" are used interchangeably to refer to any information about an individual.

These people in most cases, willingly provide their personal information including their Social Security Numbers, phone numbers, e-mail addresses to complete strangers without question. They trust us without reservation just like we trusted those examiners who administered our license exams, whether it was a couple of strangers employed by the FCC or a group of strangers called volunteer examiners from a local amateur radio club. In either case we assumed these people were trustworthy and sharing our personal information with them would not put our most sensitive personal information at risk.

Unfortunately, we live in a time when more and more criminals are looking for more and more opportunities[1] to acquire our personal information for nefarious purposes and the number of opportunities and incidents is increasing. From 2006 through 2017, the number of identity theft complaints has increased on average, 160%[2]

Purpose. The purpose of this document is to promote awareness of our legal (and moral) obligations regarding the PII of the people we serve.

The remainder of this document is organized into the following sections:

[1] Secret Service Warning
[2] https://www.iii.org/graph-archive/96074

Section I
Definition of PII

1-1. The following data are examples of PII according to the National Institute of Standards and Technology (NIST).[3] The items in bold text are the examples of PII we usually see as Volunteer Examiners.

- **Full name** (if not common)
- Face (sometimes)
- **Home address**
- **Email address** (if private from an association/club membership, etc.)
- National identification number (e.g., **Social Security number in the U.S.**)
- Passport number
- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- **Telephone number**
- **Login name**[4], screen name, nickname, or handle

1-2. The following are potentially classified as PII, because they may be combined with other personal information to identify an individual.[5] An applicant's criminal record is limited to indicating whether or not they we ever convicted of a felony. We do not collect any details of any criminal activities.

- First or last name, if common
- Country, state, postcode or city of residence
- Age, especially if non-specific
- Gender or race
- Name of the school they attend or workplace
- Grades, salary, or job position
- **Criminal record**

1-3. Sensitive PII (SPII) is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

- SPII requires stricter handling guidelines because of the increased risk to an individual if the data is inappropriately accessed or compromised.
- Some categories of PII are sensitive as stand-alone data elements, including Social Security numbers (SSN) and driver's license or state identification numbers.[6]
- Combining sensitive PII with non-sensitive PII elevates the combination to Sensitive (e.g., Combining an applicant's Social Security number with their personal e-mail address, phone number, and/or criminal history.) [7]

[3] Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) Page 2-2
[4] An applicant's e-mail address can be their Login name for CORES
[5] https://en.wikipedia.org/wiki/Personally_identifiable_information
[6] DHS Handbook for Safeguarding Sensitive PII Page 5
[7] DHS Privacy Incident Handling Guidance – Page 4

Section II
Governance

2-1. What laws govern the protection of PII?

The privacy of an individual is a fundamental right that must be respected and protected. In order to protect the people we serve and ourselves, we must know, understand, and comply with all applicable federal, state and local laws regarding the collection, handling, storing, protecting, transmitting, and mailing of PII and the requirement to report lost, stolen or compromised PII that was in our possession.

a. Federal laws - The following congressional acts address requirements for the protection of personally identifiable information by federal agencies. Additionally, the Office of Management and Budget (OMB) also provides guidance to federal agencies regarding the protection of PII.

- the Privacy Act of 1974;
- the E-Government Act of 2002;
- the Federal Information Security Management Act of 2002;
- the Veterans Benefits, Health Care, and Information Technology Act of 2006; and
- the Health Insurance Portability and Accountability Act of 1996.

b. State laws - All states have security measures in place to protect data and systems.[8] These laws vary between the states and apply primarily to state agencies but can apply to businesses, including non-profit organizations.

c. The laws regarding PII and their applicability to volunteers are pretty vague at best or nonexistent at worst.

(1) The National Archives and Records Administration (NARA), like the Federal Communications Commission (FCC), is an independent agency of the United States.

(2) Unlike the FCC, NARA has a privacy policy that applies to all NARA employees, contractors, National Archives Foundation staff, Presidential Library Foundation staff, foundation funded employees, interns, ***volunteers***, detailees, or other individuals performing work for NARA.[9]

(3) According to Mr. Scot Stone, Deputy Chief, Mobility Division, Wireless Telecommunications Bureau, Federal Communications Commission:

> "*There are no specific FCC rules governing VEs' and VECs' handling of PII. I think that they just didn't consider such issues when the VEC system was created in 1983, and the rules haven't changed much since then. (When the Commission implemented the Universal Licensing System in 1998, it acknowledged that VECs would need the SSNs of applicants who didn't already have FRNs, but even then it did not enact any specific requirements for handling such information.*" [10]

[8] National Conference of State Legislatures

[9] https://www.archives.gov/files/foia/directives/nara1608.pdf

[10] E-mail exchange between Mr. Scot Stone and Robert Rose, 24 May 2017

(4) While there may be no FCC rules or requirements vis-à-vis handling PII as they pertain to VEs and VECs, there are no protections either.

2-2. What is our authority to collect PII?

a. In late 1982, the Goldwater-Wirth Bill was passed by Congress and signed into law by President Ronald Reagan. This bill, known as Public Law 97-259 [11], amended the Communications Act of 1934, permitting the FCC to accept the voluntary and uncompensated services of licensed radio amateurs to serve in preparing and administering examinations.

b. The Debt Collection Act of 1996 amended the Privacy Act of 1974 to require persons applying for a license from the Federal Communications Act to provide their Social Security Number to the FCC. [12]

c. FCC rules state that applicants must provide the administering VEs with all information required by the rules prior to the examination and the VEs may collect all necessary information in any manner of their choosing.[13] [14]

d. The information required to be provided by applicants/collected by VEs is found on the official application form for amateur radio amateur licenses - FCC 605 Main Form. [15] [16.]

e. In late 2001, the FCC mandated the use of the FCC Registration Number (FRN) as a means of "masking" an applicant's SSN.[17]

(1) Interestingly, the Amateur Radio service was excluded from this requirement for applicants applying for a new license. However, a licensee is required to provide their FRN when modifying, renewing, or updating their license or if changing their call sign systematically.

(2) Persons doing business with the FCC including applicants for an amateur radio license can register their SSN with the FCC (Through CORES) and receive an FCC Registration Number which is provided in lieu of their SSN.

(3) The FCC will convert an applicant's SSN to an FRN upon receipt of their amateur radio license application.

2-3. What is a Privacy Policy statement and is it required?

a. Basically, a privacy policy statement is a public notice that accurately discloses:

- What personal information is collected;
- Why personal information is collected;
- How it stores and protects the information;
- How the information is used;
- How personal information distributed and with whom;[18]

[11] Communications Amendments Act of 1982; PL 97-259

[12] Debt Collection Improvement act of 1996, PL 104-134. 31 U.S.C. §3701

[13] Electronic Code of Federal Regulations, Title 47, Part 97, §97.17(b)(1)

[14] Electronic Code of Federal Regulations, Title 47, Part 97, §97.21(a)(2)

[15] 605_main_form_september_2017_1.pdf

[16] Report and Order (FCC 98-234) WT Docket No. 98-20, September 7, 1998

[17] 47890 Federal Register/Vol. 66, No. 179/Friday, September 14, 2001/Rules and Regulations, Adoption of a Mandatory FCC Registration Number, Effective 3 Dec 2001

[18] http://www.swlaw.com/blog/data-security/2015/03/10/what-is-a-privacy-policy-part-1/

b. In practice, privacy policies are typically published on websites, usually via a hyper-link at the bottom of the webpage. Privacy policies can also disclose practices regarding personal information that is collected “off-line”, on hard-copy documents or audio and video records.[19]

c. There are no general federal or state laws that requires an organization to have a privacy policy in all circumstances. But there are several laws that require one in some circumstances. Not having a privacy policy when it is required by law is a potential compliance problem that can lead to liability.[20]

d. You are required to comply with applicable federal and states laws regarding a privacy policy.

e. When writing a privacy statement, keep in mind that the average U.S. adult reads at an 8th grade reading level. The majority of Fortune 500 privacy policies in a study require a reading comprehension level beyond that of the average U.S. adult. Remarkably, 82% of those privacy policies required a college-level reading ability.[21]

- Keep it simple
- Keep it accurate
- Keep it up-to-date

f. An example of a privacy policy statement is included at Appendix 1

[19] Ibid

[20] http://www.swlaw.com/blog/data-security/2015/03/12/why-you-need-a-privacy-policy-part-2-avoiding-three-common-fumbles/

[21] Ibid

Section III
Why does PII require Protection?

3-1. **Identity Theft/Fraud.**

a. Criminals use a victim's PII, to open new lines of credit, establish loans for cars or houses, open new utility accounts at a new address, and even apply for government benefits. Social Security numbers have long been considered the "Holy Grail" of PII. Having more of your information is helpful but not having the SSN just makes it more difficult to steal someone's identity.

(1) Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data [PII] in some way that involves fraud or deception, typically for economic gain.[22]

(2) Identity theft is a federal felony under U.S.C. Title 18 Part 1, Chapter 47, §1028.

b. According to the US Department of Justice (DOJ)'s most recent study, 17.6 million people in the US experience some form of identity theft each year. This includes activities such as fraudulent credit card transactions or personal information being used to open unauthorized accounts. The DOJ's study found that victims experienced a combined average loss of $1,343. In total, identity theft victims lost a whopping $15.4 billion in 2014.[23]

(1) The most common type of identity theft is the unauthorized misuse or attempted misuse of an existing account—experienced by 16.4 million persons.

(2) An estimated 8.6 million victims experienced the fraudulent use of a credit card, 8.1 million experienced the unauthorized or attempted use of existing bank accounts (checking, savings or other) and 1.5 million victims experienced other types of existing account theft, such as misuse or attempted misuse of an existing telephone, online or insurance account.

(3) Beyond money lost, identity theft can negatively impact credit scores. While credit card companies detect a majority of credit card fraud cases, the rest can go undetected for extended periods of time. A criminal's delinquent payments, cash loans, or even foreclosures slowly manifest into weakened credit scores. Victims often only discover the problem when they are denied for a loan or credit card application.

(4) Other findings include—

- The number of identity theft victims age 65 or older have increased.
- More females (9.2 million) were victims of identity theft than males.
- People in households with an annual income of $75,000 or more had the highest prevalence of identity theft (11 percent), compared to those in all other income brackets.

c. According to multiple studies[24] [25] the number of identity fraud victims increased by eight percent in the last year. Despite industry efforts, in 2017 the number of victims **increased by 1.3 million**, with the amount stolen rising to $16.8 billion.

[22] https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

[23] https://www.bjs.gov/content/pub/press/vit14pr.cfm

[24] https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

[25] https://www.identityforce.com/blog/how-much-time-does-identity-theft-recovery-take

(1) For the first time ever, Social Security numbers (35 percent) were compromised more than credit card numbers (30 percent) in breaches.

(2) Identity theft recovery takes an average of 6 months and 100 to 200 hours-worth of work. For those with limited time for phone calls, written correspondence, emails, police reports, follow-up replies and investigative work, those hours can stretch out over years.

(3) Those who were hit by identity theft as children are particularly vulnerable to longer identity theft recovery timeframes. Often, the damage isn’t detected until they’re older and applying for their first bank accounts or jobs.

Section IV
Protecting PII

"An ounce of prevention is worth a pound of cure."
— **Benjamin Franklin**

4-1. **How does identity theft happen?**

Knowing how identity theft is committed can help prevent it or minimize the chance of it happening to us or the people we serve.

a. Most cases of identity theft can be traced back to an insider such as an employee, family member or friend.[26]

b. Insiders have a significant advantage over external attackers. They are not only aware of their organization's policies, procedures, and technology; they are also aware of its vulnerabilities (for example, loosely enforced policies or exploitable flaws in networks). Insider incidents occur in all organizational sectors, often causing significant damage. These incidents include national security espionage; modifying or stealing confidential or sensitive information for personal gain...[27]

c. Almost 64 percent of the total stolen data records occurred in the United States, whose large population, concentration of major companies, and rate of technological adoption make it the prime target for thieves.[28] Identity theft techniques include the following:

- Data breaches
- Accidental disclosure[29] [30]
- "Dumpster diving"
- "Shoulder surfing"
- Hacking
- Telephone calls
- E-mail scams
- Theft

4-2. **What can we do to protect applicants' PII?**

- Comply with applicable federal and state laws.

- Whether or not there are specific legal requirements for volunteer examiners regarding PII that is entrusted to us, we have a moral obligation to protect that PII. In the absence of specific federal and state laws, use the best practices of industry and government.

  Two great reference documents are the National Institute of Standards and Technology's "*Guide to Protecting the Confidentiality of Personally Identifiable Information" (PII)*"[31] and the DHS Handbook for Safeguarding Sensitive PII [32]

[26] https://www.bankinfosecurity.com/interviews/id-theft-insider-access-no-1-threat-i-836
[27] https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21232
[28] https://blog.varonis.com/the-world-in-data-breaches/
[29] https://www.benefitspro.com/2017/08/07/accidental-data-breaches-remain-the-leading-cause/?slreturn=20180923175720
[30] https://intelligentid.com/graton-casino-pii-mistake-shows-accidental-side-insider-threat/
[31] Guide to Protecting the Confidentiality of Personally Identifiable Information
[32] DHS Handbook for Safeguarding Sensitive PII

- Understand which elements of PII we typically handle.
- Understand which PII requires protection and which does not.
- Understand our vulnerabilities
- Create procedures and policies for protecting PII
- Train your VEs
- Implement procedures/policies to protect PII

4-3. **The following are elements of PII we typically collect.** The bold examples are PII elements we are required to collect.

- **Name**
- **Social Security Number or FCC Registration Number**
- **Call sign (If applicable)**
- **Mailing address**
- **Felony question answer** – New licenses and modifications of existing licenses
- Phone number
- E-mail address

4-4. **Some PII elements require protection and others do not.**

a. Not all PII needs to be protected in the same way. In fact, some PII does not need to have its confidentiality protected at all.[33] The Privacy Act of 1974 authorizes agencies to disclose information about individuals under a "routine use." A routine use is defined as a disclosure of a record outside of the agency "*for a purpose which is compatible with the purpose for which it was collected*."[34]

A radio amateur's license information listed in the Universal Licensing System (ULS) is a good example. The FCC publishes the licensee's name, FCC Registration Number (FRN), call sign, mailing address and if they've been convicted of a felony in the ULS which is accessible by the public. Because this information is publicly accessible, it does not require protection.

Note: A licensee can request the FCC treat the details of their conviction as confidential, in which case the public cannot view that information. However, the fact that a licensee was convicted remains publicly viewable.

b. PII not viewable by the public must be protected until it becomes viewable.

c. Applicant social security numbers, phone numbers, and e-mail addresses **always require protection**.

d. VE Teams serve two types of applicants:

(1) Applicants for a new license. Typically, some or all of the PII we collect from these applicants is not in the "public domain". Therefore, the PII of applicants for a new license requires protection.

(2) Licensees. All or most of the PII we collect from these applicants is in the "public domain" and as a result, some of their PII is not subject to protection.

[33] Ibid Page ES-3
[34] 5 U.S.C. § 552a(a)(7), (b)(3).

4-5. **Understand your vulnerabilities**

a. Depending on several factors, we are probably susceptible to the following PII theft techniques and almost all of these can be mitigated or prevented. They are listed in the likelihood of their occurrence.

(1) **Accidental breaches.** These are probably our biggest vulnerability.

- Paper and digital documents with applicant's PII are left exposed/unprotected so other people can see the information.
- These can occur at the exam session location or at home.

(2) **Loss, mis-delivery, and theft.** These are very possible. The Postal Service processes and delivers about 493.4 million pieces of mail each day.[35] Presumably that includes First Class, Certified, Registered, and Priority mail, as well as packages and junk mail.

(a) First class mail is the type of mail service that is not normally tracked and therefore not a lot of data is available regarding lost or mis-delivered. Since First class mail is not normally trackable, it is logical that it is the type of mail service that experiences the most lost or mis-delivered mail.

(b) The Postal Service is very successful in delivering mail that is trackable (e.g., Certified, Priority, and Registered) and packages. Trackable mail is rarely lost or mis-delivered. Because it is trackable, it is recoverable and deliverable.

(c) Mail and packages are also subject to theft regardless of how it is mailed.

- A relatively small percentage of theft is internal to the Postal Service
- Other theft is external to the Postal Service (Thieves steal mail and packages from your porch or outside mail box)

(d) Some mail is undeliverable due to damage incurred during machine processing and invalid addresses. Invalid or missing return addresses prevents the mail from being returned.

(3) **E-mail scams** – This is a more likely vulnerability, especially if you don't use good security practices regarding your e-mail. Don't click on links in e-mails from people you don't know – don't make it easier for the criminals.

- Phishing scams.[36]
- Trojan horse.[37]
- Drive-by downloads.[38]

(4) **Hacking** – There is a relationship between hacking and e-mail scams. It's not very likely that someone will access your computer and troll through your files looking for goodies.

(5) **Shoulder surfing** – This occurs when someone stands behind the victim and uses their phone to photograph documents with PII or share the info over the phone to an accomplice.

(6) **Dumpster diving** - This is probably oldest method of identity theft. Documents with applicants' PII are tossed in the trash and the "diver" retrieves them.

[35] USPS
[36] https://www.webroot.com/us/en/resources/tips-articles/what-is-phishing
[37] https://www.webroot.com/us/en/resources/tips-articles/what-is-trojan-virus
[38] https://www.kaspersky.com/resource-center/definitions/drive-by-download

4.6. **What can you do to protect applicants' PII?**

a. **It's not that complicated.** Since we deal with different applicants whose PII protection requirements vary, the best course of action is to treat each applicant's paperwork as if it contained the most sensitive PII (e.g., yours).

b. Create and implement procedures and policies for protecting PII.

- "An ounce of prevention is worth a pound of cure."
- Protecting the PII of the people we serve is a full-time responsibility that begins the moment we receive it until we no longer possess it, regardless of its form (Paper or digital).

c. Comply with applicable federal and state law.

- Don't take shortcuts.
- Failure to comply could result in you being held liable

d. Review your workflow and identify real or potential vulnerabilities.

- From start to finish
- Not limited to your exam session
- Identify any real or potential vulnerabilities that could result in the unauthorized exposure of an applicant's PII, including an applicant's answer to the felony question.
- Implement procedures to eliminate any real or potential vulnerabilities.

e. Train your VEs.

(1) Focus attention on the procedures for handling and protecting PII.

(2) All persons who will be granted access to applicants' PII should receive appropriate training on handling and protecting PII.

(3) Depending on the roles and functions involving PII, important topics to address may include:

- The definition of PII
- Applicable privacy laws, regulations, and policies
- The importance of protecting PII
- Restrictions on data collection, storage, and use of PII
- Roles and responsibilities for using and protecting PII
- Appropriate disposal of PII
- Sanctions for misuse of PII
- Recognition of an incident involving the loss, theft and/or compromise of PII
- Retention of PII
- Roles and responsibilities in responding to PII-related incidents and reporting.

f. Keep in mind that an applicant's SSN is the most sensitive element of PII followed by their phone number and e-mail address. Treat the answer to the felony question as PII regardless of how it's answered.

- Provide instruction/assistance prior to exam sessions, as appropriate.
- Provide on-site capability to acquire an FRN prior to the start of the exam session, if possible.
- Assist applicants as required but respect and protect their privacy during the process.

g. Minimize the exposure of an applicant's sensitive PII (SPII) before, during, and following your exam session.

- Limit the number of VEs who will have access to an applicant's SPII.
- Never leave documents that contain SPII unattended on a desk, network printer, fax machine, or copier.
- Create and implement procedures (e.g., "safe distances") to prevent people from:
  - Eavesdropping when discussing PII/SPII with an applicant.
  - Viewing applicants' PII on forms and/or computer screens if using SessionManager.
    - Use cover sheets or folders when handling hard copy documents with SPII to prevent accidental exposure by prying eyes (e.g., "Shoulder surfing")
- Identify and announce "off limits" areas at your exam session.
- Maintain physical control/custody of session-related paperwork that contains PII when not in use.
  - At home - keep in a locked office, drawer, cabinet, desk, box, or safe.
  - While in transit - keep in a locked box or in the trunk of your vehicle.

h. If you use SessionManager on a personal or on a shared computer (e.g., a club's computer), prevent unauthorized access to the SessionManager application and its files.

- Use a password to access the application.
- Archive your previous exam sessions or delete them.
- Use a screen saver or sleep mode that requires a password to access SessionManager.
- Close the SessionManager application when not in use
- Implement methods/procedures to prevent unauthorized access to forms and documents that contain applicants' PII.
- Delete or archive your session files.
  - Archiving your session files encrypts them and they can be recalled if necessary.

I. Destroy all documents that contain applicants' PII but are not used.

- Do not put documents in the trash.
- Shred or burn unused documents that contain applicants' PII
  - Prevents dumpster divers from acquiring documents with PII.

j. Do not retain copies of documents with applicants' PII.

- You cannot legally or morally justify why you need to retain someone's PII, especially their SSN.
- Do not store copies of session paperwork containing applicants' PII on your computer.
  - Prevents loss of applicants' PII from hackers and e-mail scams.

k. Mail your session paperwork using a delivery service that provides the capability to track your package (e.g., USPS, UPS, FEDEX, etc.). The odds of losing the paperwork with regular First-Class mail are much higher.

Section V
Lost, stolen or compromised PII

5.1. **Privacy Incidents**

a. A privacy incident is described as the following:

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where…

(1) A person other than the authorized user accesses or potentially accesses [PII] or

(2) An authorized user accesses or potentially accesses [PII] for an unauthorized purpose.

The term encompasses both suspected and confirmed incidents involving PII, whether intentional or inadvertent, which raises a reasonable risk of harm.[39]

5.2. **What if you have a privacy incident?**

a. If you know or suspect that an applicant's PII that you collected was lost, stolen, and/or compromised, immediately report the incident in accordance with your state's laws.

b. In lieu of specific state laws do the following if an applicant's Social Security Number is lost, stolen, and/or compromised:

(1) File a report with local law enforcement so there is an official record of the incident and follow their instructions as appropriate. It may be necessary for each person whose SSN was involved to file a report as well.

(2) Report the loss of the materials to the applicable carrier (e.g., USPS, UPS, FEDEX, etc.)

(a) **United States Postal Service**
If after 7 business days, your mail or package hasn't arrived, submit a Missing Mail Search Request with the following information:

- Sender mailing address
- Recipient mailing address
- Size and type of container or envelope you used
- Identifying information such as your USPS Tracking number(s), the mailing date from your mailing receipt, or Click-N-Ship® label receipt
- Description of the contents
- Pictures that could help us recognize your item

(b) **United Parcel Service (UPS)**
e-Mail Notification
Phone - (800) 742-5877
Say "Tracking," then say your tracking number and listen for instructions.

(c) **Federal Express (FEDEX)**
File a claim
Phone - (800) 463-3339

[39] DHS Privacy Incident Handling Guidance

(3) **If you believe that an applicant's PII was compromised or stolen from your computer** you may notify the National Cybersecurity & Communications Integration Center (NCCIC).

a. **We are not required to report to US-CERT**, however, you can voluntarily report.[40]

b. For more information on federal incident reporting requirements, visit: https://www.us-cert.gov/incident-notification-guidelines.

(4) Notify each applicant by phone, e-mail or by certified mail, that their SSN, phone number, and/or e-mail address was possibly lost, stolen, and/or compromised including but not limited to the following:

a. The approximate date of the breach (e.g., Loss, theft, and/or compromise).

b. Any facts you can share

c. A brief description of the personal information included in the breach (e.g., SSN, Phone number, e-mail address).

d. Advise the applicant(s) whose SSN was possibly lost, stolen, and/or compromised, to contact the organizations listed below. A more detailed list of this information is included as a separate document at Appendix 2 and should be provided to each person whose SSN was involved.

- Equifax Information Services LLC
- Experian Information Solutions, Inc
- TransUnion LLC
- Federal Trade Commission
- Internal Revenue Service
- Social Security Administration
- Financial institutions

Note: Depending on the circumstances, this can be a challenging task. But you must make the effort.

Note: Publicly available information that is lawfully made available to the general public from federal, state or local government records (e.g., a licensee's information in the ULS) is not considered as compromised PII.

[40] E-mail exchange between Bob Rose and the National Cybersecurity & Communications Integration Center, 20 December 2018

Section VII
Our Liability

7.1. What can happen if an applicant's personal information we collected is lost, stolen, or compromised?

a. It's hard to say, but the following are possible, probable, or certain[41].

- People will ask the following:
  - How could this happen?
  - Why didn't the organization do what was necessary to protect against a breach?

- A law suit that might allege that you, your team, your club, your Regional Coordinator, the VEC chairman and/or the parent organization of the VEC (e.g., The Laurel Amateur Radio Club, Inc) were individually and/or collectively negligent in failing to protect the stakeholder's personal information, and that their loss was directly attributable to your individual and/or collective negligence.

- State and/or federal agencies could investigate and take action against any organization determined to be negligent in guarding personally identifiable information. The actions could include fines and penalties which can be substantial and are often on a per record basis.

7.2. How can we protect ourselves from liability?

a. Employ the best practices when it comes to protecting an applicant's PII. Refer to section IV, paragraph 4.6. These will minimize the chance that your applicants' PII will be lost, stolen, or compromised.

b. Purchase some form of liability insurance. This probably isn't necessary if you employ the best practices for protecting applicants' PII described in Section IV, paragraph 4.6.

[41] Data Privacy and Cyber Liability

Summary

We must comply with the applicable federal and state laws regarding the handling and protection of PII. It is your responsibility to know your state's laws regarding PII. In lieu of specific state laws or regulations integrate the procedures in Section IV, paragraph 4.6. into your team's normal procedures.

Protecting the PII of the people we serve is a full-time legal and moral responsibility that begins the moment we receive it regardless of its form (Paper or digital).

While we cannot totally prevent the loss or theft and resulting compromise of applicants' PII, we can take reasonable, common-sense steps to minimize the chances of it lost, stolen, or compromised.

Another option is to do nothing and hope that nothing bad happens if your applicant's PII is lost, stolen, or compromised. This option is described quite well below.

Appendix 1

Example of a Privacy Statement

Collecting, Sharing and Protecting Personal Information	
Why is data collected?	The Federal Communications Commission (FCC) requires specific personal data from an applicant in order to grant, modify and/or update an amateur radio license.
What data is required to be collected?	Your name, mailing address, Social Security Number (SSN) or FCC Registration Number (FRN) in lieu of the SSN, and call sign if applicable. Phone number and e-mail address can be optionally provided.
Is data shared?	Yes.
With whom is data shared?	Personal information is transmitted from the Volunteer Examiner team to a Regional Coordinator, the FCC, and the Chairman of the Laurel VEC.
How is data shared?	By e-mail, through an FCC website, and by “snail mail”.
How is data protected?	The session information including individual applications is encrypted and sent by e-mail. It is transmitted to the FCC via a secure website. The hard copy paperwork is mailed using a tracking capability. Data that is retained on the VE team’s computer is also encrypted.
Once a license is granted, your personal information (Except SSN, Phone, and e-mail) is posted in the FCC’s Universal Licensing System data base which is accessible to the general public and the right to privacy for that information is waived.	

Appendix 2

If your personal identification information was possibly lost, stolen, and/or compromised, contact the organizations listed below.

- **Equifax**
  - (800) 525-6285 (Option 6) or 800-685-1111
  - www.equifax.com/personal/

  Equifax Information Services LLC
  P.O. Box 740241
  Atlanta, GA 30374-0241

- **Experian**
  - (888) 397-3742 (Option 1 followed by Option 1, again)
  - www.experian.com

  Experian Information Solutions, Inc
  P.O. Box 2104
  Allen, TX 75013-0949

- **TransUnion**
  - (800) 680-7289 (Option 2) or (888) 909-8872
  - www.transunion.com

  TransUnion Fraud Victim Assistance
  P.O. Box 2000
  Chester, PA 19016

- **Federal Trade Commission (FTC)**
    - (877) 438-4338
    - www.identitytheft.gov
    - https://www.identitytheft.gov/?utm_source=takeaction

  Federal Trade Commission
  600 Pennsylvania Avenue, NW
  Washington, DC 20580

- **Internal Revenue Service (IRS)**
    - (800) 908-4490
    - https://www.irs.gov/identity-theft-fraud-scams

  If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

    - Respond immediately to any IRS notice; call the number provided.

    - Complete IRS Form 14039, Identity Theft Affidavit, if your e-filed return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.

    - If you previously contacted the IRS and did not have a resolution, contact them for specialized assistance at 1-800-908-4490. They have teams available to assist.

  Note: The IRS **DOES NOT** initiate contact with taxpayers by e-mail to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

- **Social Security Administration (SSA)**
    - (800) 269-0271 or (800) 772-1213
    - https://blog.ssa.gov/protecting-your-social-security-number-from-identity-theft/
    - You can speak to a Social Security representative between 7 a.m. and 7 p.m. Monday through Friday.
    - If you suspect someone’s using your Social Security number for work purposes, report the problem to them immediately by contacting the Federal Trade Commission.

- **Financial institutions** - Close any financial or credit accounts opened without your permission or tampered with by identity thieves.

- **Freeze your credit report**
    - Each of these companies offers you the option to freeze your report with them (subject to state laws) if you request it.
        - Equifax, (800) 685-1111 (Automated, Option 3) or (888) 298-0045 (Live)
        - Experian, (888) 397-3742 (Option 2 followed by Option 2)
        - TransUnion, (888) 909-8872