

# Physical Safeguards Compliance

## Nonpublic Personal Information (NPI)

Federal law requires that dealerships and their employees safeguard consumers' non-public personal information. Nonpublic information (or "NPI") consists of any information a consumer provides on a credit application, any information learned about the consumer from a credit report, or any other information about the consumer that is not available to the general public. Physical safeguards are the most obvious type. This means keeping unauthorized persons physically away from documents or networks containing customers' NPI.



**Keep unauthorized persons away from NPI.**

## Locks

Locks are one example of a physical safeguard. Offices where NPI is available should be lockable, and locked when an authorized person is not present.



**Lock doors to offices containing NPI.**

A door lock might not be necessary, though, if all file cabinets and drawers where NPI is located are consistently locked. Having both locked doors and locked files cabinets would be better still, but might be more than necessary. Remember, the idea is to keep unauthorized people away from customer NPI, not make it impossible to get work done.



**Lock file cabinets containing NPI.**

## Logs

Locking files is a start but you also should keep a log (almost like a librarian) of who accesses customer files and when they are returned. An administrative assistant can do this and electronically enter the entries so that activity of particular users can be tracked. Review individual user activity and if you see a spike in someone's access to deal files or safeguarded information, investigate the situation promptly and find out why. It is not unusual for criminals to attempt to induce auto dealer employees to get customer information for them and a spike in accessing files might be a way to identify such activity.



**Log access to paper and electronic files.**

## Secure Areas

If the fax machine or copier used to transmit credit applications to lenders is accessible to the general public, moving it to the accounting office or an F&I office would be another simple physical safeguard.



**Keep fax/copier in the Secure Area.**

## Security Systems

Motion detection or other after-hours intrusion alarms would also be a proper physical safeguard.



**Use the motion detector/ alarm after hours.**

## Guards

Another physical safeguard would be a night watchman or guard service.



**Employ a watchman or after-hours security service.**

# Physical Safeguards Checklist

This checklist is intended to help you perform quick audits of your Physical Safeguards. It is not a comprehensive Risk Assessment and does not address the Technical and Administrative Safeguards that should also be in place as a part of your dealership's Safeguards Program. A full Risk Assessment should be conducted at least annually. This checklist can be used to address and review the Physical Safeguards at your dealership. Some questions may not be applicable if your business uses electronic rather than paper records.

## Are F&I offices lockable?

F&I offices should be kept locked when not occupied.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Is the business office lockable?

Offices and other areas where NPI is gathered, used, or stored should be kept locked when not occupied.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Are file cabinets in a lockable area?

All file cabinets and drawers where NPI is located should be consistently locked.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Are dealership computers/servers in a lockable area?

Computers/servers should be located in secure areas if possible.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Do customers have access to computer terminals?

If computers are located in areas accessible to unauthorized persons they should be password-protected, and lock after a set time. Never leave screens containing NPI open on an unattended device.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Are computers password-protected?

Computers must be password protected. If they contain NPI they must use Multifactor Authentication. Do not post passwords on post-it notes or elsewhere in writing where it may be seen by someone else.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Are computer terminals locked after a set time?

Lock screen settings should be set to a relatively short period of time particularly if the computer is located in an area customers can access.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Are janitorial services performed after hours?

Ensure janitorial staff do not have access to secure areas. NPI storage areas and computers should be locked. Consider performing janitorial services during business hours when they can be supervised.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Where are current records stored?

Answer: \_\_\_\_\_

Locked/secured?

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Where are long-term records stored?

Answer: \_\_\_\_\_

Locked/secured?

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## How are obsolete records destroyed?

Answer: \_\_\_\_\_

Certificate of destruction provided?

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------

## Are there any documents containing NPI left out in the open or in trash bins rather than shredder bins?

Do not leave deal jackets and papers containing NPI in plain sight and unprotected. Don't place documents containing NPI in trash bins or wastebaskets. If you see NPI in papers in waste baskets, pick up the papers and deposit into a shredder bin, or shred them yourself. Report the incident to your manager.

Yes	<input type="checkbox"/>	No	<input type="checkbox"/>
-----	--------------------------	----	--------------------------