



PRIVACY POLICY

VERSION 1.4



American Association of
Motor Vehicle Administrators

This document describes the approach taken by AAMVA with respect to personal privacy issues.

Privacy Policy

The American Association of Motor Vehicle Administrators (AAMVA) is a nonprofit organization, representing the state and provincial officials in the United States and Canada who administer and enforce motor vehicle laws.



Address 📍: AAMVA, Inc
4401 Wilson Boulevard
Suite 700
Arlington, Virginia 22203

Telephone 1-703-522-4200
☎️:

Fax 📠: 1-703-522-1553

Website 🌐: www.aamva.org

The American Association of Motor Vehicle Administrators (AAMVA) produced this document.

No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage or retrieval systems, for any purpose other than the intended use by AAMVA, without the express written permission of AAMVA.

© 2015 AAMVA. All rights reserved

Privacy Policy

Contents

1	Purpose	4
2	Scope & Limitations	4
2.1	Target Audience	4
2.2	Privacy Expectations	4
3	AAMVA Privacy Policy Statement	5
3.1	Statement of Policy	5
4	AAMVA Privacy Controls	6
4.1	Authority and Purpose (AP)	6
4.2	Accountability, Audit, and Risk Management (AR)	7
4.3	Data Quality and Integrity (DI)	9
4.4	Data Minimization and Retention (DM)	10
4.5	Individual Participation and Redress (IP)	11
4.6	Security (SE)	12
4.7	Transparency (TR)	13
4.8	Use Limitation (UL)	14
5	Responsible Party	15
6	Definitions	16
7	References	17
8	Revision History	17
9	Approval	19
10	Appendices	20
10.1	Appendix A: Security Controls for Protecting PII	20
10.2	Appendix B: Sources for AAMVA Privacy Controls	22
10.3	Appendix C: AAMVA’s Privacy Compliance	23
10.4	Appendix D: External Agreements	24

Privacy Policy

1 PURPOSE

This document establishes privacy principles to be followed in AAMVA; defines key terms and concepts; states requirements; and assigns accountability for governance, oversight, and compliance.

The objectives are to:

1. Protect individuals' privacy to a degree that is consistent with common sense, current laws and regulations, and best practices.
2. Protect AAMVA from the adverse consequences, such as loss of reputation and financial damage that could result from a privacy-related incident.

2 SCOPE & LIMITATIONS

2.1 TARGET AUDIENCE

This policy applies to all AAMVA employees, and users of AAMVA resources and information assets.

2.2 PRIVACY EXPECTATIONS

Users of AAMVA resources of the AAMVA network acknowledge that they have no expectation of privacy in any communications made or work conducted with such resources. AAMVA reserves the right to review, inspect, and monitor any and all use of the resources it provides and operates.

AAMVA respects the users' privacy and all monitoring activities are conducted in accordance with the *AAMVA Network and Computer Monitoring Policy*.

AAMVA will comply with the lawful orders of courts, such as subpoenas and search warrants. This compliance may include providing, when required, copies of system files, email and chat content or other information ordered by the court.

Information in transit (e.g., electronic communications) or at rest (e.g., saved as files) should never be considered private or confidential unless special measures are taken. Be mindful of the sensitivity of the information you are handling and understand the protections in place versus those required to safeguard this information. If in doubt, please consult with the security team within the Enterprise Architecture – Security department.

Privacy Policy

3 AAMVA PRIVACY POLICY STATEMENT

3.1 STATEMENT OF POLICY

AAMVA will protect the privacy of individuals in all aspects of AAMVA's enterprise – AAMVA networks, systems, business processes, and technology resources. This protection pertains to:

1. AAMVA personnel information collected and handled as part of AAMVA's human resource processes such as but not limited to:
 - Personnel Records
 - Payroll
 - Background Investigations
 - Data collected as part of Personnel Monitoring as defined in the *AAMVA Network and Computer Monitoring Policy*
2. Information obtained by AAMVA either directly from the individual or by a third party, such as a jurisdiction, including but not limited to:
 - netFORUM
 - Conferences and Membership
 - Public Web Site
3. Information processed by systems developed or operated by AAMVA in support of its business goals and mission, or on behalf of its clients including but not limited to:
 - Driver Systems (e.g., CDLIS)
 - Vehicle Systems (e.g., NMVTIS)
 - Verification Systems (e.g., DLDV)

Privacy Policy

4 AAMVA PRIVACY CONTROLS

AAMVA’s policy statement is addressed by implementing privacy controls which are defined below and organized by the following privacy families:

- Authority and Purpose (AP)
- Accountability, Audit, and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitation (UL)

Refer to [Appendix C](#) for a description of AAMVA’s privacy compliance and sources of the privacy controls described in this policy.

4.1 AUTHORITY AND PURPOSE (AP)

This family ensures identification of the legal basis that authorizes collection of PII or activity that impacts privacy. Additionally, the family includes controls to specify in privacy notices the purpose(s) for which the data is collected.

<i>Authority and Purpose (AP)</i>
Privacy Policy Statements:
AP-1: <i>Authority to Collect</i>
AAMVA determines and documents its legal authority to collect, use, maintain, and share PII, either generally or in support of a specific program or information system requirement.
AP-2: <i>Purpose Specification</i>
AAMVA describes in its privacy notices the purpose(s) for which PII is collected, used, maintained, and shared.

Privacy Policy

4.2 ACCOUNTABILITY, AUDIT, AND RISK MANAGEMENT (AR)

The privacy controls below enhance public confidence through governance, monitoring, risk management, and assessment. Implementing these controls demonstrates compliance with applicable privacy protection requirements and minimization of over risk to privacy.

<i>Accountability, Audit, and Risk Management (AR)</i>
Privacy Policy Statements:
AR-1: <i>Governance and Privacy Program</i>
AAMVA designates a member of the Senior Leadership Team accountable for maintaining this policy and for ensuring that AAMVA complies with measures that support AAMVA’s privacy protection principles and practices.
AAMVA managers are accountable for complying with the above principles and all applicable privacy protection requirements in their areas of responsibility.
State and Federal privacy laws and policies are monitored for changes that impact AAMVA’s privacy program.
AAMVA allocates sufficient resources to implement, operate, and support the AAMVA privacy program.
AAMVA implements applicable privacy controls, policies, and procedures.
AAMVA Security and Privacy plans, policies, and procedures are reviewed at least annually and updated as needed.
AR-2: <i>Privacy Impact and Risk Assessment</i>
AAMVA documents and implements risk management processes to assess privacy risk to individuals from the collection, sharing, storing, transmitting, use, and disposal of PII.
AAMVA assesses privacy issues affecting its network, systems, and other technology resources and infrastructure by completing Privacy Impact Assessments (PIAs) ¹ as pertinent early in the development process, and updating them as appropriate throughout the system development life cycle (SDLC).
AR-3: <i>Privacy Requirements for Contractors and Service Providers</i>
Roles, responsibilities, and access requirements for contractors and service providers are established.

¹ See AAMVA’s “Privacy Impact Assessment (PIA) Guideline” for the template and guidance in conducting a PIA.

Privacy Policy

<i>Accountability, Audit, and Risk Management (AR)</i>
Contracts include confidentiality protection requirements.
AR-4: <i>Privacy Monitoring and Auditing</i>
The Chief Information Security Officer determines if and when AAMVA’s use of PII shall be audited to demonstrate compliance and the effective implementation of privacy policy.
AR-5: <i>Privacy Awareness and Training</i>
AAMVA develops and implements privacy protection awareness and training to focus the attention of its employees on protecting PII and to change and/or reinforce desired behavior in regards to PII and privacy practices.
AAMVA provides training to all employees and contractors who use or handle PII.
Individuals who are granted access to PII will receive appropriate training so as to reduce the possibility that PII is inappropriately accessed, used, or disclosed.
AAMVA personnel certify (manually or electronically) their acceptance of AAMVA privacy requirements and responsibilities at least annually.
AAMVA reinforces through staff communications the seriousness of protecting PII.
AR-6: <i>Privacy Reporting</i>
As appropriate and needed, reports demonstrating AAMVA’s accountability and compliance with privacy laws and regulations are prepared and disseminated to governing bodies.
AR-7: <i>Privacy-Enhanced System Design and Development</i>
AAMVA information systems are designed to support privacy by automating privacy controls, as applicable.
AR-7: <i>Accounting of Disclosures</i>
As required, AAMVA documents and retains an accounting of disclosures of information under its control. Documentation includes: date, nature, purpose of each disclosure; and name and address of person / agency to which disclosure was made.
AAMVA documents, as necessary, the duration for which disclosures records must be kept, by developing data retention schedules or similar artifacts.

Privacy Policy

4.3 DATA QUALITY AND INTEGRITY (DI)

The following privacy controls enhance confidence that any PII collected and maintained is accurate, relevant, timely, and complete for the purpose for which it is to be used.

<i>Data Quality and Integrity (DI)</i>
Privacy Policy Statements:
DI-1: <i>Data Quality</i>
To the extent practicable, AAMVA ensures that PII directly collected from an individual or created is accurate, relevant, timely, and complete.
AAMVA collects PII directly from the individual to the greatest extent practicable.
AAMVA strives to check for and periodically corrects, as necessary, any inaccurate or outdated PII used by its programs or systems.
AAMVA utilizes controls to promote and maximize the quality and integrity of disseminated information.
DI-2: <i>Data Integrity and Data Integrity Board</i>
AAMVA documents processes to ensure the integrity of PII through existing security controls.
AAMVA, as applicable, ensures that it remains in compliance with provisions of the Privacy Act.

Privacy Policy

4.4 DATA MINIMIZATION AND RETENTION (DM)

Data minimization and retention controls assist organizations to collect, use, and retain only relevant PII necessary for the original purpose for which it was collected.

Data Minimization and Retention (DM)
Privacy Policy Statements:
DM-1: <i>Minimization of Personally Identifiable Information</i>
AAMVA limits collection and use of PII to only that which is essential and directly relevant to (a) meet AAMVA-authorized business purposes; and (b) accomplish the specific purpose(s) of its use.
Collection will be through lawful and fair methods and, where appropriate, with the knowledge and consent of the individual to whom the information pertains.
As part of its Risk Management Framework (RMF), AAMVA periodically reviews existing Privacy Impact Assessment (PIA) .
Where feasible and when technology allows, AAMVA uses anonymization and de-identification techniques to remove or obscure PII.
DM-2: <i>Data Retention and Disposal</i>
AAMVA retains PII only for as long as necessary to fulfill the specified purpose(s), or as required by law or AAMVA data retention policies.
Regardless of the method of storage, AAMVA’s disposal, destruction, erasure, and/or anonymization of PII complies with the approved record retention schedule and prevents loss, theft, misuse, or unauthorized access.
AAMVA promptly destroys PII that is no longer needed and ensures that retired or repurposed hardware is properly sanitized of all PII before disposal or reassignment.
DM-3: <i>Minimization of PII Used in Testing, Training, and Research</i>
AAMVA minimizes the use of PII for testing, training, and research with specific controls implemented to protect PII used for such purposes.

Privacy Policy

4.5 INDIVIDUAL PARTICIPATION AND REDRESS (IP)

Individual participation and redress controls assist in making individuals active participants in the decision-making process regarding the collection and use of their PII. Public confidence in an organization’s decision-making process based on the PII is enhanced when these controls are implemented that provide individuals with access to their PII and the ability to correct or amend their information as needed.

<i>Individual Participation and Redress (IP)</i>
Privacy Policy Statements:
IP-1: <i>Consent</i>
<p>In the event that AAMVA were to share or use PII data it directly collected for purposes different than its original intended use (e.g., HR benefits, payroll, etc.), AAMVA will seek the consent of the individuals, or the organizations, that provided the data.</p> <p>Monitoring of data, including PII, is defined in the AAMVA Network and Computer Monitoring Policy.</p>
IP-2: <i>Individual Access</i>
<p>AAMVA facilitates an individual’s ability to review and update the PII that it collects directly collects from such individuals. For information that AAMVA doesn’t collect directly, AAMVA makes reasonable efforts to assist individuals in understanding how their information may be accessed.</p>
IP-3: <i>Redress</i>
<p>AAMVA facilitates the capability for an individual to correct or redress their personal PII. In some cases, the process consists of assisting such individual with the relevant point of contact from the organization that provided AAMVA data.</p> <p>Where AAMVA owns the relationship, AAMVA facilitates the dissemination of corrected or amended PII to other parties.</p>
IP-4: <i>Complaint Management</i>
<p>Inquiries, complaints, concerns, or questions from individuals about AAMVA privacy policies should be directed to the AAMVA Chief Information Security Officer.</p>

Privacy Policy

4.6 SECURITY (SE)

The following privacy controls supplement the security controls and help to protect PII (in all formats) by using reasonable security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

Security (SE)
Privacy Policy Statements:
SE-1: <i>Inventory of Personally Identifiable Information</i>
AAMVA strives to create, maintain, and periodically update an inventory listing all programs and information systems that collect, use, maintain, or share PII.
AAMVA establishes information security requirements for all new and modified systems containing PII.
SE-2: <i>Privacy Incident Response</i>
AAMVA integrates procedures into its Incident Response plan that clearly define roles and responsibilities, effectively manage internal communication, and address the unique differences in handling incidents and breaches involving PII from that of non-PII incidents.
AAMVA procedures for notifying individuals or regulatory bodies about real or possible breaches of personal information aim to satisfy the most stringent notification standard of any jurisdiction for which AAMVA provides services or support.
AAMVA provides an organized and effective response to privacy incidents that considers the following: <ul style="list-style-type: none">• Compliance with data breach laws (e.g., state notification laws).• Potential for subjecting affected individuals to embarrassment, identity theft, or blackmail;• Greater harm to AAMVA’s reputation and reduction of public trust; and• Increased media attention

Privacy Policy

4.7 TRANSPARENCY (TR)

Transparency controls ensure that notice of information practices are provided to the public in addition to the privacy impact of the organization’s programs and activities.

<i>Transparency (TR)</i>
Privacy Policy Statements:
TR-1: <i>Privacy Notice</i>
For PII that AAMVA collects directly from individuals (e.g., employee PII), AAMVA documents ² the existence and nature of personal data under its control and the main purpose of its use.
Where AAMVA processes or stores data that originated from or remains primarily the responsibility of other entities (e.g., the jurisdictions), AAMVA is only responsible for documenting the nature and purpose of AAMVA systems and their data, and making that information available as appropriate.
TR-2: <i>System of Records Notices (SORN) and Privacy Act Statements</i>
AAMVA conforms to SORN as applicable.
TR-3: <i>Dissemination of Privacy Program Information</i>
AAMVA is open and transparent with respect to its collection, use, dissemination, and maintenance of PII.
AAMVA ensures that information about its privacy activities is accessible by pertinent parties.

² The form used to collect the information (e.g., health-care benefit enrollment form) is an acceptable vehicle to meet the documentation requirement as the reason for collection and use is clearly stated.

Privacy Policy

4.8 USE LIMITATION (UL)

Use Limitation privacy controls helps to ensure that the use of PII remains within scope.

<i>Use Limitation (UL)</i>
Privacy Policy Statements:
UL-1: <i>Internal Use</i>
AAMVA's use of PII remains consistent with the original and authorized purpose(s) for which the data is collected.
AAMVA limits access to PII to only those with an authorized and approved "need to know" and enforces the principles of "separation of duties" and "least privilege." ³
AAMVA minimizes the number of copies that are made of data containing PII.
AAMVA copies or extracts PII for development or support purposes only when the original purpose specifically include such usage ⁴ .
AAMVA limits the places where data with PII appears or is stored.
UL-2: <i>Information Sharing with Third Parties</i>
AAMVA only shares PII with third parties who are authorized to receive and access the information.
Sharing PII with third parties must be documented prior to the sharing and compatible with the purpose(s) for which the PII was originally collected.
Agreements document the sharing of PII with third parties.

³ See the [Appendix A](#) for specific security controls relevant to accessing PII. Also refer to the *AAMVA Information Security Policy Manual*.

⁴ This control is not intended to restrict essential and authorized access to PII in the course of direct operation and support of systems, or by help desk personnel.

Privacy Policy

5 RESPONSIBLE PARTY

Please direct all inquiries about this document, including requests for policy exceptions or content change to AAMVA IT Enterprise Architecture – Security.

Privacy Policy

6 DEFINITIONS

Term / Acronym	Definition
Anonymization	Technique by which previously identifiable information that has been de-identified and for which a code or other association for re-identification no longer exists.
Confidentiality	The importance of information as measured by its unauthorized exposure. Specifically for this policy, preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
De-Identification	Process by which records with PII have enough of the PII removed or obscured (i.e., masked or obfuscated) such that the remaining information does not identify an individual.
Integrity	The importance of information as measured by the loss of its trustworthiness. Specifically for this policy, guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Personally Identifiable Information (PII)	Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother’s maiden name, etc.)”
Privacy Impact Assessment (PIA)	An analysis of how information is handled (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy Policy

Term / Acronym	Definition
Security Controls	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

7 REFERENCES

Reference	Purpose
<i>AAMVA Information Security Policy Manual</i>	This policy manual defines AAMVA’s requirements for securely managing its information assets and associated resources in order to protect the confidentiality, integrity and availability of those information assets
“Privacy Impact Assessment (PIA) Guideline”	This document provides guidance on the applicability and completion of the Privacy Impact Assessment (PIA) at AAMVA.

8 REVISION HISTORY

Version #	Description of Revision	Date
1.0	Original document.	11/18/2010
1.1	<ul style="list-style-type: none"> • Modified definitions of “Confidentiality” and “Integrity” to align with those in other security policies • Revised “Applicability of Policy” • Changed Responsible Party to “AAMVA IT Enterprise Architecture – Security” • Revised format of “References” table. 	5/9/2011
1.2	<ul style="list-style-type: none"> • Policy updated to include the privacy controls from SP 800-53, Rev. 4, Appendix J. • References to Privacy Threshold Analysis (PTA) removed. • Definitions reviewed and edited. 	8/23/2013

Privacy Policy

Version #	Description of Revision	Date
	<ul style="list-style-type: none"> • Several sections, moved to Appendix • “Approval” section moved to the end of the document to accommodate e-signature. 	
1.2	Annual policy review – no changes required	12/22/2014
1.3	Policy reviewed and updated to align with current AAMVA privacy policy and to provide clarity. Changes include: <ul style="list-style-type: none"> • “Privacy Expectations” section added from “Acceptable Use Policy” • Sections 2.3 to 2.6 deleted • Section 3.1 text changed to clarify scope of protection of individual privacy • Selected policy statements in Section 4 added, changed, deleted for clarity 	07/29/2015
1.4	Minor edits throughout	04/15/2016


Privacy Policy

9 APPROVAL

This policy has been reviewed and approved by AAMVA IT Enterprise Architecture – Security.

Name: Pierre Y. Boyer

Title: CISO

Signature: 

Date: 4/15/16

Privacy Policy

10 APPENDICES

10.1 APPENDIX A: SECURITY CONTROLS FOR PROTECTING PII

AAMVA protects PII from misuse or unauthorized disclosure by utilizing the security controls described in the *AAMVA Information Security Policy Manual*.

The security controls listed below in Table 1 are identified as being of special relevance to PII in [NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information \(PII\)](#).

Note: The names of the Security Controls are updated to those listed in SP 800-53, Revision 4, April 2013.

Table 1 – Security Controls for Protecting Privacy of PII

Control Area	Security Control
Access Control (AC)	AC-3 - Access Enforcement AC-5 - Separation of Duties AC-6 - Least Privilege AC-17 - Remote Access AC-19 - Access Control for Mobile Devices AC-21 - Information Sharing
Audit and Accountability (AU)	AU-2 - Audit Events AU-6 - Audit Review, Analysis, and Reporting
Identification and Authentication (IA)	IA-2 - Identification and Authentication (Organizational Users)
Media Protection (MP)	MP-2 - Media Access MP-3 - Media Marking MP-4 - Media Storage MP-5 - Media Transport MP-6 - Media Sanitization

Privacy Policy

Control Area	Security Control
System and Communications Protection (SC)	SC-8 - Transmission Confidentiality and Integrity SC-9 - Transmission Confidentiality – Withdrawn; incorporated into SC-8 SC-28 - Protection of Information at Rest
System and Information Integrity (SI)	SI-4 - Information System Monitoring

Privacy Policy

10.2 APPENDIX B: SOURCES FOR AAMVA PRIVACY CONTROLS

AAMVA's privacy policy focuses on protecting [personally identifiable information \(PII\)](#) from loss of [confidentiality](#) and [integrity](#), and from misuse.

For the framework of this policy, AAMVA adopted the eight Fair Information Practice Principles (FIPPs) described in [DHS' "Privacy Policy Guidance Memorandum" \(Memorandum Number: 2008-01; December 29, 2008\)](#). These principles are:

- Accountability and Auditing
- Data Minimization
- Data Quality and Integrity
- Individual Participation
- Purpose Specification
- Security
- Transparency
- Use Limitation

NIST Special Publication (SP) 800-53, Revision 4, includes Appendix J, "Privacy Control Catalog". The privacy controls in Appendix J (and listed below) are based on the FIPPs which, in turn, embodies the principles in the Privacy Act of 1974. This appendix addresses privacy by:

- Structuring privacy controls, based on best practices, to help organizational compliance;
- Creating a link and relationship between privacy and security controls in order to enforce privacy and security requirements which may overlap in concept and in implementation;
- Illustrating the applicability of the NIST Risk Management Framework in selecting, implementing, assessing, and monitoring of privacy controls;
- Promoting closer interaction and cooperation between privacy and security officials within an organization.

The privacy controls listed in the following sections are key safeguards AAMVA employs to protect the privacy of individuals and their PII. This privacy information includes that which AAMVA collects, uses, maintains, shares, and ultimately disposes of, whether in paper or electronic form, through its programs, systems, and personnel.

Similar to the structure used in *AAMVA Information Security Policy Manual*, the following privacy controls are organized by privacy control family. The eight families align with the FIPPs.

Privacy Policy

10.3 APPENDIX C: AAMVA'S PRIVACY COMPLIANCE

AAMVA will enforce this policy in accordance with applicable state and Federal laws and regulations. Violations may result in disciplinary action up to termination of employment or contract, and/or civil and criminal prosecution.

Regulations of special relevance for AAMVA include:

- Privacy Act of 1974 - which sets forth a code of fair information practices for information systems associated with federal agencies,
- Federal Information Security Management Act (FISMA) – which defines a comprehensive framework for the protection of government information, operations, and resources against threats (both natural and man-made); and
- Driver Privacy Protection Act (DPPA)- which regulates how personal information collected by state motor vehicle agencies may be used.

Additionally, AAMVA adheres to specific state privacy laws and regulations as applicable.

AAMVA users should report areas of non-compliance and propose plans to close any gaps as quickly as possible, taking advantage of upcoming releases, major maintenance schedules, and contract renewal dates as opportunities to make the necessary adjustments without disrupting operations.

Questions and issues should be brought to the attention of the Chief Information Security Officer.

Privacy Policy

10.4 APPENDIX D: EXTERNAL AGREEMENTS

In situations where AAMVA handles or transports PII originally collected, stored, or processed by an external entity (e.g., a jurisdiction or federal agency), AAMVA should require documented agreements to ensure that the entity accepts appropriate responsibility, and is not dependent upon AAMVA, for any of the procedural or technical actions that are required by the Privacy Policy Principles or the Operational Safeguards.

At a minimum, these agreements will specify:

- Roles and responsibilities;
- Restrictions on further sharing of the information;
- Requirements for notification to each party in case of a breach; and
- Minimum security controls.

Technical requirements that are necessary may be included in Interconnection Security Agreements (ISA) or their equivalent.