Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

Cybersecurity for Local Churches

Training Tuesday Webinar

November 17, 2026

Agenda

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

- Featured Speaker: Rob Jett, Technology Services Manager
  - Cybersecurity Survival Guide
- Notes from National Church Group
  - Cybersecurity Insurance Considerations
- FAMLI Paid Leave Program
  - Updates and Pending Actions

TRAINING TUESDAY · CHURCH CYBERSECURITY

Cyber fraud is reaching our connection

New England Conference, August 5, 2026

$1.6M stolen

Criminals posing as bank representatives created a false sense of crisis, got into online banking, and tried 40 wires, each just under the $50k limit. 32 went through to accounts in 25 countries. About $250k recovered so far.

$3.05B

lost to business email compromise in 2025, the #2 cybercrime by dollars; wire transfers are the main path

70% +

of churches have been targeted by a cyberattack; most losses come from email fraud and stolen logins

+ 26%

rise in reported U.S. cybercrime losses from 2024 to 2025, to $20.9B

Sources: UM News (Aug. 26, 2026, updated Sept. 23); FBI IC3 2025 Internet Crime Report; APS, State of Church Payroll Security 2026

FINANCE & ADMINISTRATION
General Council on Finance and Administration
THE UNITED METHODIST CHURCH

A Survival Guide for a Cybersecurity Journey

THE CHECKLIST

One practice per slide, with practical explanations for United Methodist Church administrators.

Part 1 of the cybersecurity survival guide can be found here.

How to Use This Guide

Treat each slide as one conversation, one decision, and one next step.

UMC INFORMATION TECHNOLOGY SUPPORT

1

Read

Understand the practice in plain language.

2

Discuss

Identify who owns the decision and who needs to participate.

3

Act

Complete the practical actions listed on the slide.

4

Record

Document the decision so it survives staff transitions.

The checklist is designed to become a repeatable ministry process, not a one-time project.

01

Critical Systems Inventory Documented

Know which systems ministry depends on and who is responsible for each one.



You cannot protect what you have not documented.

FOUNDATION

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Create one reliable inventory of every critical system used by the church or conference.

WHY IT MATTERS

If essential knowledge exists only in one person's memory, the ministry may lose access, miss a renewal, or struggle to recover when that person is unavailable.

WHAT TO DO NOW

- List email, giving, accounting, church management, website, livestream, member database, and cloud storage systems.
- Record the account owner, hosting location, renewal date, support contact, and recovery information.
- Assign someone to keep the inventory current.

02

Administrative Access Reviewed

Every elevated permission should have a clear ministry purpose.



Access should follow responsibility, not convenience.

ACCESS CONTROL

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Review administrative privileges and confirm why each person needs the level of access assigned.

WHY IT MATTERS

Unused accounts and excessive permissions increase risk. Documented access decisions improve accountability and make future reviews easier.

WHAT TO DO NOW

- Ask, “Why does this person need access?” for every administrator.
- Remove unused accounts and permissions that no longer match a ministry role.
- Document who approved access and the reason it was granted.

03 MFA Enabled and Password Plan Established

Protect accounts with consistent authentication and recovery practices.



A password is stronger when it is unique and backed by MFA.

ACCOUNT SECURITY

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Use strong, unique passwords, multi-factor authentication, and a consistent plan for account ownership and recovery.

WHY IT MATTERS

Shared or personally owned ministry accounts can create continuity problems during staff transitions. Reliable recovery information keeps church leadership in control.

WHAT TO DO NOW

- Enable multi-factor authentication wherever it is available.
- Use a password manager for shared ministry accounts.
- Avoid personal email addresses for church-owned services.
- Keep recovery information accessible to authorized leadership.

04 Access Guidelines Defined

Give staff the minimum access needed.



Access should be specific, understood, and reviewed.

VOLUNTEERS

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Set clear rules for the permissions, acceptable use, confidentiality, and data protection expectations.

WHY IT MATTERS

Ongoing process that ensures that only authorized people can access specific systems, data, applications, or physical locations.

WHAT TO DO NOW

- Provide only the permissions required for the current role (reviewed with every transition).
- Explain acceptable use, confidentiality, and data handling expectations.
- Review accounts regularly (quarterly).
- Remove access when responsibilities change.

05

Device Security Standards Documented

Protect church information on both church-owned and personal devices.



Ministry data deserves protection wherever it is used.

DEVICE SECURITY

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Document minimum security expectations for every device used to conduct ministry work.

WHY IT MATTERS

UMC organizations often operate in mixed-device environments. Clear standards reduce ambiguity and make protection consistent across UMC-owned and personal equipment.

WHAT TO DO NOW

- Keep UMC-owned devices updated, protected by antivirus, advanced threat detection and secured with screen locks.
- Set expectations for passwords and software updates on personal devices used for ministry.
- Define how organizational information may be stored, accessed, and shared.

06

Files Stored in Approved Locations

Keep sensitive records in managed storage with appropriate access and backup.



Good record management protects trust.

DATA PROTECTION

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Store ministry records in approved cloud platforms rather than personal drives or unmanaged storage locations.

WHY IT MATTERS

Employee and financial records deserve special care. Managed storage supports restricted access, retention, and dependable backup.

WHAT TO DO NOW

- Move important records to approved only authorized locations.
- Limit sensitive information to authorized individuals.
- Establish retention guidelines.
- Confirm that backups are performed regularly.

07

Website and Domain Ownership Verified

Protect the organization's digital front door and communication channels.



The ministry should control its domain, website, and email.

DIGITAL PRESENCE

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Confirm that leaders can access and recover the website, domain registration, and communication platforms.

WHY IT MATTERS

Losing control of a domain or communication account can significantly disrupt ministry. Shared institutional knowledge makes recovery possible.

WHAT TO DO NOW

- Ensure more than one trusted leader knows how to access domain and website management.
- Protect email communication platforms with multi-factor authentication.
- Review public staff directories, forms and contact methods to reduce spam and fraud.

08

Financial Platform Access Review

Apply heightened scrutiny to giving, banking, accounting, and payment systems.



Financial access is a stewardship responsibility.

FINANCIAL CONTROL

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Review everyone who can access giving platforms, banking systems, accounting software, and payment processing services.

WHY IT MATTERS

Financial systems are frequent targets for cybercriminals. Separating responsibilities reduces the chance that one person controls every part of a transaction.

WHAT TO DO NOW

- Verify that each person’s access is current and appropriate.
- Separate financial responsibilities whenever possible.
- Remove access promptly when a role changes.
- Schedule periodic access reviews.

09

Offboarding Checklist Created

Remove access and transfer ministry information when someone leaves.



Departure should trigger a documented process.

TRANSITIONS

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Use a consistent checklist whenever a staff member leaves a ministry role.

WHY IT MATTERS

Delayed offboarding can lead to unauthorized access, missing files, and confusion about ownership. Prompt action protects continuity and ministry information.

WHAT TO DO NOW

- Disable accounts promptly.
- Collect organization-owned equipment.
- Transfer files and account ownership.
- Update shared passwords.
- Remove system permissions.

10

Onboarding Checklist Created

Help new staff and volunteers begin ministry safely.



Good security habits should begin on day one.

ONBOARDING

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Provide accounts, security expectations, authentication, and awareness training through a documented process.

WHY IT MATTERS

A consistent start helps new team members understand both the technology they use and their responsibility to protect ministry information.

WHAT TO DO NOW

- Provide accounts through an approved process.
- Explain organizational procedures and acceptable-use expectations.
- Enable multi-factor authentication.
- Offer new hire security awareness training.

11

Security Review Schedule Established

Make cybersecurity a routine part of ministry operations.



Small, regular reviews prevent larger problems.

GOVERNANCE

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Set a quarterly or semiannual schedule for reviewing accounts, permissions, devices, vendors, and critical systems.

WHY IT MATTERS

Routine reviews identify changes and small issues before they become major problems. Documented findings also make follow-through visible.

WHAT TO DO NOW

- Choose a quarterly or semiannual review rhythm.
- Document findings and unresolved issues.
- Assign owners and due dates to action items.
- Track completion before the next review.

12

Trusted Support Resources Identified

Know who to contact before a technology or security problem occurs.



Asking for help is responsible stewardship.

SUPPORT

UMC INFORMATION TECHNOLOGY SUPPORT

WHAT THIS MEANS

Identify trusted technology partners, denominational resources, security professionals, or managed service providers that can assist the ministry.

WHY IT MATTERS

No organization is expected to solve every technology challenge alone. A known support path improves response when suspicious activity or difficult changes occur.

WHAT TO DO NOW

- Record trusted contacts and how to reach them.
- Ask for help when implementing new systems.
- Seek assistance when responding to suspicious activity.
- Document an Incident Response Plan.

The Goal: Prepared, Repeatable Stewardship

Document systems. Manage access thoughtfully. Create processes that continue through staff transitions.

1. Start with one practice
2. Assign an owner
3. Document the decision
4. Set the next review date

A secure church is not a perfect church. It is a prepared church.

CYBER SECURITY INSURANCE

NOTES FROM NATIONAL CHURCH GROUP

NCG
Nonprofit Community Group

Protecting Church Funds & Ministry

Cyber insurance considerations for United Methodist congregations

Cybercrime is a financial and operational exposure

Ransomware, compromised email, stolen personal information and fraudulent payment instructions can disrupt ministry and strain church resources.

Insurance is one part of a broader strategy

Review cyber and crime insurance alongside strong payment controls, employee awareness, multifactor authentication and tested backups.

The key question

Would the church's current policies respond to the specific incident—and at what limit?

When a Contractor Payment Is Redirected

Illustrative wire transfer fraud scenario

1 A convincing request

A treasurer receives an email appearing to come from a contractor requesting that the next building-project payment go to a new bank account.

2 The payment is sent

The church transfers $75,000 before discovering the bank account change was fraudulent.

3 The coverage question

Does the policy address social engineering, invoice manipulation or funds transfer fraud? A voluntary transfer may be treated differently from an unauthorized transfer.

Cyber vs. Crime: Review Both

Coverage names alone do not determine whether a loss is insured

Cyber liability

May address ransomware, breach response, forensic investigation, system restoration, interruption and privacy liability; some policies also cover financial fraud.

Crime / social engineering coverage

May address computer fraud, funds transfer fraud or deceptive payment instructions. Confirm affirmative coverage for authorized payments induced by fraud.

Standalone vs. package endorsement

Compare scope, response resources, sublimits, deductibles, exclusions and verification conditions—not just the overall policy limit.

Practical Next Steps for Every Church

A short checklist for trustees, finance committees and staff

Prevent fraudulent transfers

Independently call a trusted number already on file to verify new or changed banking instructions; use dual approval and payment thresholds.

Review insurance before a loss

Ask your agent to examine cyber and crime policies together, especially social engineering, invoice manipulation, ransomware and separate sublimits.

Prepare for an incident

Know the bank's fraud contact and insurer's 24/7 reporting process. Preserve records, notify promptly and coordinate response vendors with the insurer.

MARYLAND FAMLI PAID LEAVE

UPDATE AND PENDING ACTIONS

FAMLI Timeline Revisited

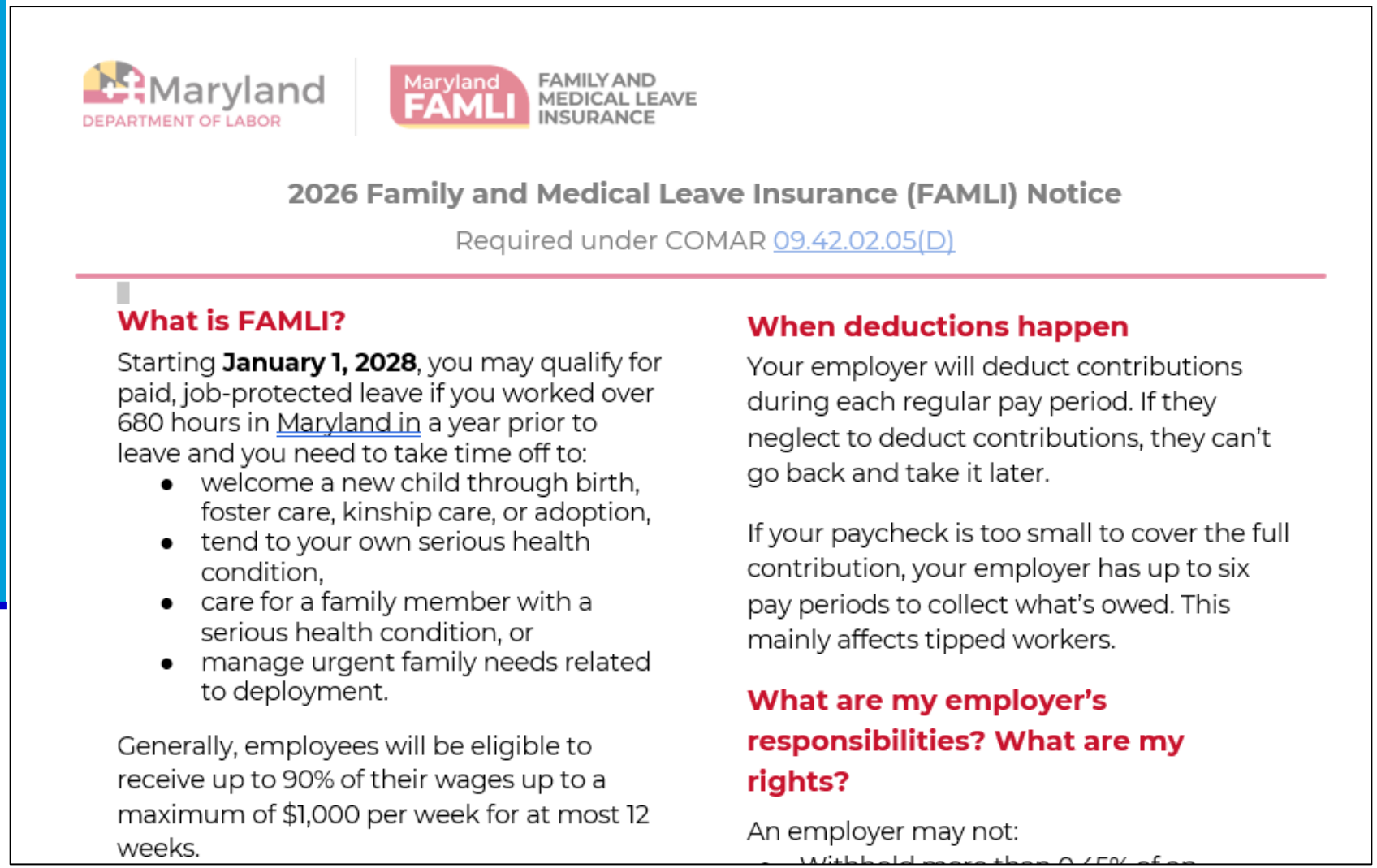
Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

- **We have learned since the last Training Tuesday that the November 15th deadline applied only to the registration for employers entering the Private Plan. This deadline has subsequently been extended to 11/20.**



Employee Notice – December 2026

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church



Maryland DEPARTMENT OF LABOR | Maryland FAMLI FAMILY AND MEDICAL LEAVE INSURANCE

2026 Family and Medical Leave Insurance (FAMLI) Notice

Required under COMAR 09.42.02.05(D)

What is FAMLI?

Starting **January 1, 2028**, you may qualify for paid, job-protected leave if you worked over 680 hours in Maryland in a year prior to leave and you need to take time off to:

- welcome a new child through birth, foster care, kinship care, or adoption,
- tend to your own serious health condition,
- care for a family member with a serious health condition, or
- manage urgent family needs related to deployment.

Generally, employees will be eligible to receive up to 90% of their wages up to a maximum of $1,000 per week for at most 12 weeks.

When deductions happen

Your employer will deduct contributions during each regular pay period. If they neglect to deduct contributions, they can't go back and take it later.

If your paycheck is too small to cover the full contribution, your employer has up to six pay periods to collect what's owed. This mainly affects tipped workers.

What are my employer's responsibilities? What are my rights?

An employer may not:

- Withhold more than 0.65% of an

- Employers are required to provide notice one pay period before payroll deductions begin on January 1, 2027.
- **Even if you plan to cover the employee's share of the contribution, you must still provide notice**.
- The employee notice template is found at the following link:

famli-2026-employee-notification-template.docx

Employee Notice – December 2026

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

How is FAMLI funded? What will I pay?

FAMLI is an insurance program funded by contributions made by both employers and employees. You may see a deduction of up to 0.45% from your pay starting January 1, 2027. Employers will then pay your contributions into a dedicated insurance fund administered by the State or to a regulated private insurance plan. Contributions begin in 2027 so that the FAMLI insurance fund will be ready to pay out benefits to employees in Maryland starting January 1, 2028.

From January 1, 2027 to December 31, 2027, your employer may deduct up to 0.45% from your wages up until you earn $192,300 in total wages.

Your employer will withhold **0.45%** of your wages from each paycheck.

employee's total pay; or

- Fail or refuse to pay contributions to FAMLI if they are in the State Plan;
- Discharge, demote, or otherwise discriminate or take adverse action against an employee for inquiring about the rights and responsibilities under the FAMLI law; expressing their intent to file a claim, complaint, or appeal; testifying in a proceeding under the FAMLI law; or filing a claim, taking FAMLI leave, or receiving FAMLI benefits when they become available in 2028.

If you believe your employer has violated the FAMLI law, you have a right to file a complaint. Contact FAMLI by phone at 410-525-4010 or by email at paid.leave@maryland.gov and request a complaint form to file a complaint.

Version 1.2 Updated November 5, 2026

Questions? Call 410-525-4010, email paid.leave@maryland.gov, visit paidleave.maryland.gov

- The employee notice will specify the percentage of wages withheld by the employer.

Your employer will withhold **0.45%** of your wages from each paycheck.

Clergy Housing Allowance

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

- We explained in September that it was unclear how the clergy housing allowance was being treated in the Maryland FAMLI Paid Leave. We still have not seen a clear definition provided to us by ADP.
- However, the QuickBooks default is setup to apply FAMLI Paid Leave contributions ONLY against the cash salary. It is not applied to the Box 14 wages like the clergy housing allowance.
- We are changing our guidance based on this observation and will continue to monitor other payroll services to confirm this guidance.

Clergy will contribute 0.45% based on the following wages:

- **Cash Salary**

Clergy will NOT contribute based on the following:

- **Housing Allowance is not eligible**
- **Imputed value of the parsonage is not eligible**
- **Retiree pension income is not eligible**

Note: Retired clergy who receive active pay from a Maryland church will also make FAMLI contributions on the active pay received. They will also be eligible for paid leave benefits if they exceed 680 hours worked in the four quarters before a submitted claim.

FAMLI Action Items

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

- **URGENT** Action Items
  - Register ASAP - EVERY Maryland Church – No exceptions
  - Provide FAMLI notices to their W-2 employees no later than the payroll prior to starting FAMLI payroll withholdings – **December 2026**
  - Include employer FAMLI contributions in the 2027 budgets, if 15 or more employees
  - Start employee payroll FAMLI deductions on **January 1, 2027**

- Future Action Items
  - Prepare for making Qtrly hour and wage reports NLT **April 30, 2027**
  - Prepare for notifications to employees about FAMLI claims process in **June 2027**

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

Please contact us with any questions:

Paul Eichelberger, Conference Treasurer
Chrisi Lockwood, Pen-Del Controller
Pier McPayten, BWC Controller

FAMLI@pdcbwc.org

Website for Additional Information

www.bwcumc.org/FAMLI

Thank You

APPENDIX

Employer Provided Insurance Plan (EPIP)

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

Self-Insured Plans

- **Large Employers:** Businesses with **50 or more employees** localized in Maryland can apply to self-insure their Equivalent Private Insurance Plan (EPIP).
- **Small Employer Exception:** Employers with **fewer than 50 employees** can only apply if they already had their own FAMLI-compliant private plan in place by **July 31, 2026.**

Commercial Plans

- **No Business Size Restrictions,** but many carriers will require a minimum of 10, 25, or 50 eligible employees
- **Plan Rollout:** Once the commercial insurance market opens and the state grants final approval to the specific policy, the carrier will begin administering and paying employee leave claims when benefits go live in **January 2028**.

Principal®

The Hartford

SHELTERPOINT
A Protective Company

AMERICAN FIDELITY
a different opinion



Timeline for Commercial and Self-Insured Plans

- **Declaration of Intent (DOI):** Employers planning to use a commercial plan must submit a signed DOI through the state portal between **September 1 and November 15, 2026**. This exempts the business from sending standard payroll tax contributions directly to the state in 2027.

- **Escrowing Contributions:** Beginning **January 1, 2027**, employers must still deduct the employee's portion of the FAMLI premium from payroll, but the funds must be held in an escrow account rather than paid to the state.

State Plan



Private Plan



Maryland DEPARTMENT OF LABOR | Maryland FAMLI FAMILY AND MEDICAL LEAVE INSURANCE

Family and Medical Leave Insurance (FAMLI)
Maryland Department of Labor
100 S. Charles Street, Tower I, Suite #10000
Baltimore, MD 21201-2725

Declaration of Intent
Proof of Private Plan Consultation

INSTRUCTIONS: The first page of this document is required to be submitted with an employer's Declaration of Intent and is to be completed solely by an insurance agent or other representative of an insurance company.

Attestation Statement

"I, _____
[printed name, insurance agent or other representative of an insurance company]

hereby attest that I met with _____ _____
[first name last name] [title]

from _____
[employer name]

on _____
[date]

and I explained all of the items contained in "Declaration of Intent - Private Plan Consultation Agenda."

Business Details

Business Address _____
Business Phone Number _____
Email Address _____

Signature

Signed this _____ day of _____, 2026
Signature _____
MD License # _____ (enter N/A if not applicable)

paidleave.maryland.gov

Wes Moore, Governor | Aruna Miller, Lt. Governor | Portia Wu, Secretary

Recommending the State Plan

Baltimore-Washington & Peninsula-Delaware Area
The United Methodist Church

Comparison Point	State Plan	Commercial Plan
Under-15 Employee Exemption	A small church will keep the under-15 employee exemption, avoiding premiums for exempt employees.	The church **will lose the exemption** and pay private insurance premiums for every employee.
Administrative Fees	No administrative application or renewal fees are charged under the State Plan.	The state will charge an **annual application and renewal fee** of $100 to $1,000, based on staff size.
Separation from Medical Decisions	Employees apply directly to the Maryland Department of Labor, which approves or denies claims and **keeps the church out of the medical review**.	The church may act as an intermediary between the insurer and employee, creating potentially awkward internal dynamics.
Coordination with Current Short-Term Disability Policy	**Most churches do not have a short-term disability policy**, Clergy CPP is a long-term disability policy that counts on salary continuation by the church for the first 90-days.	A broker may be able to "wrap" FAMLI into a strong existing disability policy, allowing staff to file one medical-absence claim.

It is recommended to stay in the State Plan through the first year of paid leave claims in 2028.

- There are known advantages in the state plan for most churches and there is currently a lack of information about the commercial plans.
- The primary downside of submitting a **Declaration of Intent (DOI)** in 2026 is that it locks your church into a strict, complex regulatory track with **zero room for operational delays or compliance errors** in 2027.
- FAMLI guidelines explicitly state that employers are allowed to exit the state pool and transition to a commercial plan in future years.