Sydney Pugh

University of Pennsylvania, Philadelphia, PA
Email: sydney.pugh@pennmedicine.upenn.edu | Web: https://sfpugh.github.io

EDUCATION

Ph.D. in Computer and Information Science 8/2019 – 8/2024
University of Pennsylvania, Philadelphia, PA
Dissertation: Weakly-Supervised Evaluation of Medical AI Systems
Co-Advisors: Prof. Insup Lee and Prof. James Weimer
Committee: Eric Eaton, Kevin Johnson, Miroslav Pajic (Duke University), Oleg Sokolsky (chair)

M.S.E. in Computer and Information Science 8/2019 – 5/2021
University of Pennsylvania, Philadelphia, PA
Co-Advisors: Prof. Insup Lee and Prof. James Weimer

B.S. in Applied Mathematics and Computer Science 8/2015 – 5/2019
Loyola University Maryland, Baltimore, MD
Co-Advisors: Prof. David Binkley and Prof. Lisa Oberbroeckling
Honors: Summa Cum Laude, Phi Beta Kappa, Pi Mu Epsilon, Upsilon Pi Epsilon

RESEARCH INTERESTS

Artificial Intelligence (AI) for Healthcare, Medical Cyber-Physical Systems (MCPS), Internet of Medical Things (IoMT), Programmatic Weak Supervision (or Data Programming)

RESEARCH EXPERIENCE

Postdoctoral Researcher 10/2024 – Present
Department of Biostatistics, Epidemiology, and Informatics
University of Pennsylvania, Philadelphia, PA
Advisor: Kevin Johnson

- Developing trustworthy and interpretable real-time, multimodal AI-based systems for the early detection of cognitive decline, Alzheimer's disease, and frailty for primary and emergency care settings.
- Leveraging large language models (LLMs) to automatically identify diagnostic indicators of cognitive decline in real patient clinic visit recordings.
- Collaborating with clinicians at the Hospital of the University of Pennsylvania to identify key issues related to cognitive decline and inform the design of AI-based solutions.
- Mentoring undergraduate, Master's, and PhD students in conducting research projects.

Doctoral Researcher 8/2019 – 8/2024
Department of Computer and Information Science
University of Pennsylvania, Philadelphia, PA
Co-Advisors: Insup Lee and James Weimer

- Developed weakly supervised performance evaluation methods for medical AI systems to address challenges arising from real-world medical evaluation data constraints.
- Designed a predictive model and identified patient phenotypes for assessing the respiratory support needs of infants with bronchopulmonary dysplasia (BPD) using features derived from time-series clinical monitoring data (e.g., vital signs).
- Collaborated with clinicians at the Children's Hospital of Philadelphia to develop and validate solutions aimed at reducing clinical alarm fatigue and optimizing respiratory support for infants with BPD.
- Contributed to research projects on in-hospital fall risk prediction and improving quality of patient-clinician interaction.
- Coordinated and led research group meetings for the NSF Smart and Connected Health project "Smart Alarms 2.0: Foundations for Caregiver-in-the-loop Suppression of Non-Informative Alarms".

Summer Undergraduate Research Fellowship 5/2018 – 8/2018, 5/2019 – 8/2019
National Institute of Standards and Technology (NIST), Gaithersburg, MD
Advisors: Richard Kuhn and Mohammad S. Raunak

- Developed a systematic testing methodology for discovering coding bugs in cryptographic algorithm implementations.
- Identified bugs in multiple algorithm implementations submitted to NIST's Lightweight Cryptography and Post-Quantum Cryptography standardization projects using our method.

Research Assistant 9/2017 – 5/2018
Department of Computer Science
Loyola University of Maryland, Baltimore, MD
Advisor: David Binkley

- Developed ATARI, an adaptive approach to association rule mining for software change impact analysis.

Hauber Summer Research Fellowship 5/2017 – 8/2017
Loyola University of Maryland, Baltimore, MD
Advisor: David Binkley

- Explored dynamic selection of software change history transactions for assessing software change impact analysis.

TEACHING INTERESTS

- **Artificial Intelligence for Healthcare**: Exploring strategies to design, implement, and validate AI-driven solutions for real-world research problems in healthcare (e.g., disease diagnosis). Covers complexities of working with clinical data and ethical implications.
- **MCPS and IoMT Security**: Covering security challenges, vulnerabilities (e.g., man-in-the-middle), and defenses (e.g., cryptography), with discussion of real-world case studies.

TEACHING EXPERIENCE

Guest Lecturer Fall 2022, Fall 2023
CIS 541: Embedded Software for Life-Critical Applications
Department of Computer and Information Science
University of Pennsylvania, Philadelphia, PA

- Delivered two lectures on Cyber-Physical Systems (CPS) and Internet of Things (IoT) security, covering attacks (e.g., man-in-the-middle, DDoS), defenses (e.g., cryptography), and real-world case studies.

Teaching Assistant Fall 2020, Spring 2022
CIS 541: Embedded Software for Life-Critical Applications
Department of Computer and Information Science
University of Pennsylvania, Philadelphia, PA

- *Spring 2022*: Designed and implemented a module on Cyber-Physical Systems (CPS) and Internet of Things (IoT) security, which involved delivering two lectures and integrating a security component into the course final project. Conducted weekly office hours and collaborated in course grading.
- *Fall 2020*: Conducted weekly office hours and graded assignments, exams, and the course final project.

Volunteer Classroom Assistant Fall 2018 – Spring 2019
Guilford Elementary/Middle School, Baltimore, MD

- Tutored middle school students in mathematics through individual and small group sessions.

Tutor Fall 2018 – Spring 2019
Department of Mathematics
Loyola University Maryland, Baltimore, MD

- Tutored fellow undergraduates in calculus, business calculus, and statistics.

HONORS AND AWARDS

Research

- **Penn AI × Science × Medicine Postdoctoral Fellows Program.** University of Pennsylvania, Philadelphia, PA. 2025.
- **Best Paper Award Finalist.** 15th ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS) for the paper "Curating Naturally Adversarial Datasets for Learning-Enabled Medical Cyber-Physical Systems". 2024.
- **1st Place Natural and Applied Science Division**. Undergraduate Student Research & Scholarship Colloquium at Loyola University Maryland, Baltimore, MD. 2018.

Student and Travel Funding

- **NSF Student Travel Award** to support travel to CPS-IoT Week in Hong Kong, China. 2024.
- **Eniac Fellowship**. University of Pennsylvania, Philadelphia, PA. 2019.
- **Abha Ahuja Scholarship**. North American Network Operators' Group (NANOG). 2019.
- **T. Rowe Price Scholarship**. Loyola University Maryland, Baltimore, MD. 2017.

PUBLICATIONS

Publication Summary: As of March 19, 2025, I have 16 total publications (9 in journals and highly selective conferences) with a total of 72 citations (as reported by Google Scholar).

JOURNAL ARTICLES

[J4] Sriharsha Mopidevi, Kuk Jang, Basam Alasaly, **Sydney Pugh**, Jean Park, Ashley Batugo, Sy Hwang, Eric Eaton, Danielle Mowery, and Kevin Johnson. "MedVidDeID: Protecting Privacy in Clinical Encounter Video Recordings." *Journal of Biomedical Informatics (JBI)*. 2025. (under review)
DOI: 10.2139/ssrn.5194782 (preprint)
Impact Factor: 5.62
Summary: This paper presents MedVidDeID, a modular pipeline for de-identifying audio-video healthcare data. The system uses a six-stage process that integrates open-source tools to handle transcript extraction, text and audio de-identification, and video obfuscation. In its most effective mode, Greedy Privacy Preservation (GPP), the pipeline achieved a 97.5% first-round de-identification success rate while reducing processing time by 64.2% compared to manual methods.

[J3] **Sydney Pugh**, Ivan Ruchkin, James Weimer, and Insup Lee. "Evaluating Robustness of Learning-Enabled Medical Cyber-Physical Systems with Naturally Adversarial Datasets." *ACM Transactions on Cyber-Physical Systems (TCPS)*. 2025.
DOI: 10.1145/3734695
Impact Factor: 3.65

Summary: This paper presents the Catfish tool for evaluating the robustness of learning-enabled medical cyber-physical systems (LE-MCPS) to naturally occurring adversarial examples. Extending a prior conference paper (C5), this work introduces two key improvements: (1) confidence intervals for weak label uncertainty to improve adversarial ordering, and (2) bootstrapping technique to handle ties in an adversarial ordering. Finally, a synthetic experiment validates the approach, showing that the proposed evaluation correctly distinguishes between robust and non-robust simulated LE-MCPS.

[J2] **Sydney Pugh**, Ivan Ruchkin, Christopher Bonafide, Sara DeMauro, Oleg Sokolsky, Insup Lee, and James Weimer. "Evaluating Alarm Classifiers with High-Confidence Data Programming." *ACM Transactions on Computing for Healthcare (HEALTH)*. 2022.
DOI: 10.1145/3549942
Impact Factor: 10.18
Summary: This paper presents a lightweight method for evaluating alarm classifiers in clinical settings without requiring perfect alarm labels. It utilizes probabilistic labels generated from data programming, a paradigm combining noisy labeling heuristics. By leveraging these labels, the method generates confidence bounds for sensitivity and specificity values, simulating evaluations with manual labeling.

[J1] Leon Moonen, David Binkley, and **Sydney Pugh**. "On Adaptive Change Recommendation." *Journal of Systems and Software (JSS)*. 2020.
DOI: 10.1016/J.JSS.2020.110550
Impact Factor: 5.88
Summary: The paper presents Atari, an adaptive approach for change impact mining in software systems. It improves efficiency by dynamically selecting relevant transactions for association rule mining, compared to state-of-the-art methods that typically use complete change histories.

PEER-REVIEWED CONFERENCE PAPERS

[C7] **Sydney Pugh**, Matthew Hill, Sy Hwang, Rachel Wu, Kuk Jang, Stacy L Iannone, Karen O'Connor, Kyra O'Brien, Eric Eaton, and Kevin Johnson. "WATCH-SS: A Trustworthy and Explainable Modular Framework for Detecting Cognitive Impairment from Spontaneous Speech." *Pacific Biocomputing Symposium (PSB)*. 2026. (under review)
DOI: 10.1101/2025.08.06.25333047 (preprint)
Summary: This paper presents the Warning Assessment and Alerting Tool for Cognitive Health from Spontaneous Speech (WATCH-SS). WATCH-SS is a modular framework that leverages several specialized detectors to identify linguistic and acoustic indicators of CI, which are then aggregated by a predictive model to produce a final classification. The framework achieves strong predictive performance, yielding an AUC of 0.80 on the DementiaBank ADReSS test dataset.

[C6] Jean Park[1], **Sydney Pugh**[1], Kaustubh Sridhar, Mengyu Liu, Navish Yarna, Ramneet Kaur, Souradeep Dutta, Elena Bernardis, Oleg Sokolsky, and Insup Lee. "Automating Weak Label Generation for Data Programming with Clinicians in the Loop." *IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE)*. 2024.
DOI: 10.1109/CHASE60773.2024.00013
Summary: This paper presents an algorithm to automate the generation of weak labels for high-dimensional medical data settings (*e.g.*, images, time-series) to apply data programming. The algorithm generates partitions centered around real prototypical data samples, with a clinician assigning labels to each prototype, thus inducing weak labels on the full dataset. The memory-induced sets of weak labels can then be used as input for data programming, effectively addressing the challenge of creating labeling functions for medical data.

[C5] **Sydney Pugh**, Ivan Ruchkin, James Weimer, and Insup Lee. "Curating Naturally Adversarial Datasets for Learning-Enabled Medical Cyber-Physical Systems." *ACM/IEEE 15th International Conference on Cyber-Physical Systems (ICCPS)*. 2024.
DOI: 10.1109/ICCPS61052.2024.00026
** Best Paper Award Finalist **
Acceptance Rate: 28%
Summary: This paper presents a method for evaluating the robustness of learning-enabled components (LECs) in medical cyber-physical systems (CPS) to naturally occurring adversarial examples. The method leverages probabilistic labels obtained from data programming to order unlabeled input data by their naturally adversarial severity, from which a sequence of datasets with increasing proportion and severity of adversarial examples is curated. On such a sequence, a robust model is expected to show decreasing accuracy with respect to the probabilistic labels due to weak labeling inaccuracies inherent in classifying adversarial examples.

[C4] Amanda Watson, Jean Park, **Sydney Pugh**, Oleg Sokolsky, James Weimer, and Insup Lee. "Medical Cyber-Physical Systems: IoMT Applications and Challenges." *56th Asilomar Conference on Signals, Systems, and Computers*. 2022.
DOI: 10.1109/IEEECONF56349.2022.10052004
Summary: This paper presents the challenges in developing medical cyber-physical systems and the internet of medical things (IoMT), some of our work in addressing them, and several open research issues.

[1] Equal contribution.

[C3] Pengyuan Lu, Xian Li, Sooyong Jang, Alexander Lee, **Sydney Pugh**, Amanda Watson, Ragnhildur I Bjarnadóttir, Robert Lucero, George Demiris, Ani Nenkova, James Weimer, and Insup Lee. "FRED: Fall Risk Evaluation Database Based on Electronic Health Record Data." *IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE).* 2021.
DOI: 10.1109/CHASE52844.2021.00030
Acceptance Rate: 41% (24 out of 58)
Summary: This paper presents a four-part database, FRED, for fall risk evaluation based on electronic health record data from MIMIC-III.

[C2] **Sydney Pugh**, Ivan Ruchkin, Christopher Bonafide, Sara DeMauro, Oleg Sokolsky, Insup Lee, and James Weimer. "High-Confidence Data Programming for Evaluating Suppression of Physiological Alarms." *IEEE/ACM Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE*). 2021.
DOI: 10.1109/CHASE52844.2021.00015
Acceptance Rate: 41% (24 out of 58)
Summary: This paper presents a lightweight method for evaluating alarm suppression without access to the true alarm labels. The method leverages data probabilistically labeled with high confidence via the data programming paradigm to estimate the sensitivity and specificity of a suppression mechanism and describes the likely outcomes of an observational study in the form of confidence bounds.

[C1] **Sydney Pugh**, David Binkley, and Leon Moonen. "The Case for Adaptive Change Recommendation." *IEEE 18th International Working Conference on Source Code Analysis and Manipulation (SCAM*). 2018.
DOI: 10.1109/SCAM.2018.00022
Acceptance Rate: 25% (16 out of 63)
Summary: This paper presents an adaptive approach to association rule mining, which dynamically selects relevant transactions, potentially considering as few as a single transaction. This contrasts with state-of-the-art approaches that typically analyze tens of thousands of transactions, offering a more efficient solution, particularly in domains like change impact analysis.

PEER-REVIEWED WORKSHOP PAPERS

[W3] Kuk Jang[2], Sameer Bhatti[2], **Sydney Pugh**[2], Chimezie Maduno, Sarang Sridhar, Sriharsha Mopidevi, Eric Eaton, and Kevin Johnson. "Towards a Real-time Clinical Agenda Setting System for Enhancing Clinical Interactions in Primary Care Visits." *AAAI Workshop on Large Language Models and Generative AI for Health (GenAI4Health).* 2025.

[2] Equal contribution.

Summary: This paper investigates the feasibility of using large language models (LLMs) to develop a real-time, AI-driven agenda-setting system for primary care visits. It evaluates the ability of LLMs to identify discussion topics and summarize clinically relevant details from a collection of simulated clinical visit recordings.

[W2] **Sydney Pugh**, Mohammad S. Raunak, Richard Kuhn, and Raghu Kacker. "Systematic Testing of Lightweight Cryptographic Implementations." *Lightweight Cryptography Workshops*. 2019.
Summary: This paper extends upon work from W1, applying a systematic testing approach to implementations of candidate cryptographic algorithms submitted to National Institute of Standards and Technology's (NIST) Lightweight Cryptography (LWC) Project. The results demonstrate the effectiveness of this approach in discovering several faults in the implementations.

[W1] **Sydney Pugh**, Mohammad S. Raunak, Richard Kuhn, and Raghu Kacker. "Systematic Testing of Post-Quantum Cryptographic Implementations using Metamorphic Testing." *IEEE/ACM 4th International Workshop on Metamorphic Testing (MET).* 2019.
DOI: 10.1109/MET.2019.00009
Summary: This paper presents a systematic testing approach based on metamorphic relations derived from cryptographic algorithm specifications for discovering code bugs in highly complex cryptographic algorithm implementations. Results demonstrate the effectiveness of this approach in discovering all known (at time of writing) faults in candidate algorithm implementations submitted to National Institute of Standards and Technology's (NIST) Post-Quantum Cryptography (PQC) Project.

ABSTRACTS

[A2] **Sydney Pugh**, Souradeep Dutta, Ramneet Kaur, Yahan Yang, Elena Bernardis, and Insup Lee. "Automated Labeling Function Generation using Distance Functions for Physiological Alarm Suppression." *ACM/IEEE 14th International Conference on Cyber-Physical Systems (ICCPS)*. 2023.
DOI: 10.1145/3576841.3589620
Summary: This abstract presents an automated approach for generating labeling functions using distance functions and a small, labeled dataset (*i.e.*, 50 or fewer samples) to streamline the application of data programming to medical time-series data. This work was presented as a poster at the conference.

[A1] **Sydney Pugh** and David Binkley. "Change Impact using Dynamic History Analysis." In *ACM 49th Technical Symposium on Computer Science Education (SIGCSE)*. 2018.
DOI: 10.1145/3159450.3162347
Summary: This abstract investigates the viability of dynamic selection of relevant transactions to improve efficiency of targeted association rule mining for effective change impact analysis. This work was presented as a poster at the symposium.

TECHNICAL SKILLS

- **Programming Languages**: Python, C/C++, Java, MATLAB, Bash/Zsh
- **Data & AI Tools**: PyTorch, TensorFlow, scikit-learn, Hugging Face transformers, MLFlow, Pandas, Numpy, SciPy, Matplotlib
- **Developer Tools and Environments**: Git/GitHub, Microsoft Azure Databricks, VSCode, HPC clusters, SLURM

SERVICE

Conference Organization

- IEEE/EMBS International Conference on Body Sensor Networks: Sensor and Systems for Digital Health **Technical Program Committee Member** (IEEE/EMBS BSN 2025)
- ACM/IEEE International Conference on Cyber-Physical Systems **Demo/Poster Program Committee Member** (ICCPS 2025)
- IEEE/ACM Conference on Connected Health: Applications Systems and Engineering **Journal-Track Co-Chair** for ACM Transactions on Computing for Healthcare (CHASE 2025)

Academic

- **Panelist** on the "Pursuing Graduate School in Computing" panel at the ACM Capital Region Celebration of Women in Computing (CAPWIC 2022).
- **Guest speaker** on graduate school in STEM for the Computer Science - Physics, and Mathematics Statistics (C-PaMS) Scholars program at Loyola University Maryland, Baltimore, MD. 10/2022, 11/2023.

Peer Reviewer

- IEEE/EMBS International Conference on Body Sensor Networks (BSN). 2025.
- ACM Transactions on Computing for Healthcare (HEALTH). 2020, 2021, 2024, 2025.
- IEEE Engineering in Medicine & Biology Conference (EMBC). 2023.

Sub Reviewer

- IEEE Open Journal of Engineering in Medicine and Biology (OJEMB). 2024.
- AAAI Conference on Artificial Intelligence. 2023.

Last Updated: August 12, 2025